

ROZPORZĄDZENIE
MINISTRA CYFRYZACJI¹⁾

z dnia 2020 r.

w sprawie profilu zaufanego i podpisu zaufanego

Na podstawie art. 20d ustawy z dnia 17 lutego 2005 r. o informatyzacji działalności podmiotów realizujących zadania publiczne (Dz.U. z 2020 r. poz. 346, 568 i 695) zarządza się, co następuje:

§ 1. Rozporządzenie określa warunki:

- 1) potwierdzania, przedłużania ważności, wykorzystywania i unieważniania profilu zaufanego, w tym:
 - a) okres ważności profilu zaufanego,
 - b) zbiór danych zawartych w profilu zaufanym,
 - 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 potwierdzenia, przedłużania ważności i unieważnienia profilu zaufanego,
 - g) warunki, które powinien spełniać punkt potwierdzający profil zaufany,
 - h) warunki organizacyjne i techniczne dla potwierdzenia profilu zaufanego oraz uwierzytelnień i autoryzacji przy nieodpłatnym wykorzystaniu środka identyfikacji elektronicznej stosowanego do uwierzytelniania w systemie teleinformatycznym banku krajowego lub innego przedsiębiorcy, zwanego dalej „podmiotem niepublicznym”,
 - i) sposób potwierdzania spełniania warunków, o których mowa w lit. h;

¹⁾ Minister Cyfryzacji kieruje działem administracji rządowej - informatyzacja, na podstawie § 1 ust. 2 rozporządzenia Prezesa Rady Ministrów z dnia 18 listopada 2019 r. w sprawie szczegółowego zakresu działania Ministra Cyfryzacji (Dz. U. poz. 2270).

2) składania podpisu zaufanego.

§ 2. Użyte w rozporządzeniu określenia oznaczają:

- 1) system, w którym wydawany jest profil zaufany - system teleinformatyczny, przy użyciu którego zapewniana jest obsługa publicznego systemu identyfikacji elektronicznej, w ramach którego wydawany jest profil zaufany;
- 2) identyfikator profilu zaufanego - unikatowy ciąg znaków alfanumerycznych jednoznacznie identyfikujących profil zaufany;
- 3) identyfikator użytkownika - unikatowy ciąg znaków alfanumerycznych jednoznacznie identyfikujących użytkownika systemu, w którym wydawany jest profil zaufany;
- 4) konto profilu zaufanego - konto osoby fizycznej, założone w systemie, w którym wydawany jest profil zaufany, umożliwiające wnioskowanie o potwierdzenie profilu zaufanego, używanie profilu zaufanego, przedłużanie ważności profilu zaufanego i unieważnianie profilu zaufanego, a także zmianę czynników uwierzytelniania;
- 5) konto nieużywane - konto profilu zaufanego, które nie było wykorzystywane przez użytkownika profilu zaufanego w okresie dłuższym niż 3 lata;
- 6) osoba wnioskująca - osobę fizyczną występującą z wnioskiem o potwierdzenie profilu zaufanego;
- 7) ustawa - ustawę z dnia 17 lutego 2005 r. o informatyzacji działalności podmiotów realizujących zadania publiczne;
- 8) punkt potwierdzający - punkt potwierdzający profil zaufany, o którym mowa w art. 20c ustawy;
- 9) rozporządzenie 910/2014 - rozporządzenie Parlamentu Europejskiego i Rady (UE) nr 910/2014 z dnia 23 lipca 2014 r. w sprawie identyfikacji elektronicznej i usług zaufania w odniesieniu do transakcji elektronicznych na rynku wewnętrznym oraz uchylające dyrektywę 1999/93/WE (Dz.Urz. UE L 257 z 28.08.2014, s. 73);
- 10) ePUAP - elektroniczną platformę usług administracji publicznej, w rozumieniu art. 3 pkt 13 ustawy;
- 11) minister - ministra właściwego do spraw informatyzacji;
- 12) tymczasowy profil zaufany – profil zaufany potwierdzany w sposób, o którym mowa w art. 20ca ustawy.

§ 3. 1. Osoba wnioskująca o potwierdzenie profilu zaufanego w punkcie potwierdzającym składa wniosek o potwierdzenie profilu zaufanego w postaci elektronicznej, wypełniając

formularz elektroniczny udostępniony w systemie, w którym wydawany jest profil zaufany. Formularz elektroniczny, o którym mowa w zdaniu pierwszym, może stanowić element udostępnionej w ePUAP usługi elektronicznej umożliwiającej założenie konta w tym systemie teleinformatycznym.

2. Jeżeli w terminie 14 dni od dnia złożenia wniosku, o którym mowa w ust. 1, nie dokonano potwierdzenia profilu zaufanego, wniosek ten jest usuwany z systemu, w którym wydawany jest profil zaufany.

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

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

3. Osoba wnioskująca potwierdza wolę posiadania profilu zaufanego, opatrując podpisem własnoręcznym wydruk wniosku, o którym mowa w § 3 ust. 1, sporządzony w punkcie potwierdzającym przez osobę upoważnioną do potwierdzenia profilu zaufanego.

4. Osoba upoważniona do potwierdzenia profilu zaufanego, po pozytywnej weryfikacji tożsamości osoby wnioskującej, potwierdza profil zaufany oraz odnotowuje na wydruku wniosku dokonanie potwierdzenia.

5. Osoba upoważniona do potwierdzenia profilu zaufanego dokonuje potwierdzenia, podpisując profil zaufany osoby wnioskującej:

- 1) podpisem zaufanym albo;
- 2) kwalifikowanym podpisem elektronicznym.

§ 5. Osoba wnioskująca o potwierdzenie tymczasowego profilu zaufanego składa wniosek o potwierdzenie tymczasowego profilu zaufanego w postaci elektronicznej, wypełniając formularz elektroniczny udostępniony w systemie, w którym wydawany jest profil zaufany.

§ 6. 1. W celu potwierdzenia tymczasowego profilu zaufanego, osoba upoważniona do potwierdzenia tymczasowego profilu zaufanego odnajduje w systemie, w którym wydawany jest profil zaufany, wniosek o potwierdzenie tymczasowego profilu zaufanego i weryfikuje przy użyciu tego systemu, czy:

- 1) imię (imiona), nazwisko i nr PESEL podane we wniosku są zgodne danymi zgromadzonymi w rejestrze PESEL, o którym mowa w ustawie z dnia 24 września 2010 r. o ewidencji ludności (Dz.U. z 2019 r. poz. 1397 i 2294 oraz z 2020 r. poz. 695) oraz

2) w Rejestrze Dowodów Osobistych, o którym mowa w ustawie z dnia 6 sierpnia 2010 r. o dowodach osobistych (Dz. U. z 2020 r. poz. 332, 695 i 875), znajduje się wizerunek wnioskodawcy o którym mowa w art.20ca ust. 5 pkt 1 lit. a.

2. Weryfikacja, o której mowa w ust. 1, może być wykonywana automatycznie przez system, w którym wydawany jest profil zaufany.

3. W przypadku stwierdzonej niezgodności weryfikowanych danych z rejestrem PESEL lub braku wizerunku wnioskodawcy w Rejestrze Dowodów Osobistych, wniosek odrzuca się z powodu niezgodności danych.

4. W przypadku stwierdzonej zgodności weryfikowanych danych z rejestrem PESEL i istnieniu wizerunku wnioskodawcy w Rejestrze Dowodów Osobistych, osoba upoważniona do potwierdzenia tymczasowego profilu zaufanego kontaktuje się z wnioskodawcą telefonicznie na numer telefonu podany we wniosku, podaje podczas rozmowy numer tego wniosku automatycznie nadany przez system, w którym wydawany jest profil zaufany i ustala sposób i termin transmisji audiowizualnej. Sposób i termin transmisji audiowizualnej osoba upoważniona do potwierdzenia tymczasowego profilu zaufanego potwierdza pocztą elektroniczną wysyłając stosowne zaproszenie na adres podany we wniosku o tymczasowy profil zaufany.

5. Osoba upoważniona do potwierdzania tymczasowego profilu zaufanego w trakcie transmisji audiowizualnej kolejno:

- 1) informuje wnioskodawcę, że transmisja jest nagrywana,
- 2) podaje numer wniosku,
- 3) zwraca się o okazanie dowodu osobistego lub paszportu w sposób umożliwiający weryfikację treści tego dokumentu oraz pokazanie twarzy w wystarczającym oświetleniu i w sposób minimalizujący możliwość pomyłek;
- 4) uzyskuje ustne oświadczenie wnioskodawcy, że:
 - a) dane zawarte we wniosku są prawdziwe i aktualne,
 - b) zapewni poufność danych, danych służących do używania profilu zaufanego,
 - c) nie udostępni konta profilu zaufanego osobom trzecim,
 - d) niezwłocznie unieważni profil zaufany w przypadku utraty częściowej lub całkowitej kontroli nad tym profilem.

6. Osoba upoważniona do potwierdzania tymczasowego profilu zaufanego może w trakcie transmisji audiowizualnej zażądać wykonania gestu, który ułatwi wykrycie działania

oprogramowania zakłócającego teletransmisję audiowizualną w sposób uniemożliwiający lub utrudniający potwierdzenie tożsamości wnioskodawcy.

7. W trakcie trwania transmisji audiowizualnej osoba upoważniona do potwierdzania tymczasowego profilu zaufanego przeprowadza procedurę wideoidentyfikacji wnioskodawcy, o której mowa w art. 20ca ust. 5 pkt 1 ustawy, pod warunkiem, że jakość transmisji pozwala na:

- 1) odczytanie danych zawartych w warstwie graficznej okazywanego dowodu osobistego albo paszportu wnioskodawcy;
- 2) porównanie wizerunku wnioskodawcy z wizerunkiem tego wnioskodawcy pobranym z Rejestru Dowodów Osobistych.

8. Osoba upoważniona do potwierdzania tymczasowego profilu zaufanego weryfikuje jakość sporządzonego nagrania, w szczególności czy można na jego podstawie odczytać dane zawarte w warstwie graficznej dowodu osobistego albo paszportu wnioskodawcy okazywanego podczas transmisji audiowizualnej oraz czy zarejestrowany został wizerunek wnioskodawcy, po czym dokonuje potwierdzenia, podpisując profil zaufany osoby wnioskującej:

- 1) podpisem zaufanym albo
- 2) kwalifikowanym podpisem elektronicznym.

9. Weryfikacja jakości nagrania może odbywać się automatycznie w systemie, w którym wydawany jest profil zaufany.

10. W przypadku wątpliwości odnośnie porównania wizerunku wnioskodawcy z wizerunkiem z Rejestru Dowodów Osobistych, osoba upoważniona do potwierdzenia tymczasowego profilu zaufanego może zweryfikować tożsamość wnioskodawcy przy wykorzystaniu dodatkowych danych dotyczących wnioskodawcy, których zgodność może zostać zweryfikowana z danymi zgromadzonymi w rejestrach publicznych lub w systemach teleinformatycznych, w szczególności zadając pytanie o dane:

- 1) zgromadzone w rejestrze publicznym możliwe do zweryfikowania przez osobę potwierdzającą bezpośrednio lub trybie przewidzianym dla dostępu do danego rejestru,
- 2) znajdujące się w dokumencie stanowiącym element akt sprawy podmiotu publicznego, który został doręczony wnioskodawcy.

11. W przypadku, o którym mowa w ust. 10, osoba upoważniona do potwierdzenia tymczasowego profilu zaufanego dokonuje potwierdzenia, po zweryfikowaniu dodatkowych

danych z właściwym rejestrem publicznym, lub pomiotem publicznym i udokumentowaniu tej czynności w aktach sprawy.

12. Po pozytywnym zweryfikowaniu danych, o których mowa w ust. 11, osoba potwierdzająca podpisuje profil zaufany osoby wnioskującej:

- 1) podpisem zaufanym albo
- 2) kwalifikowanym podpisem elektronicznym.

13. W przypadku braku możliwości uzyskania połączenia telefonicznego lub połączenia umożliwiającego transmisję audiowizualną z osobą wnioskującą, osoba upoważniona do potwierdzenia tymczasowego profilu zaufanego odnotowuje to w systemie, w którym wydawany jest profil zaufany, i odrzuca wniosek o potwierdzenie tymczasowego profilu zaufanego. Za brak możliwości uzyskania połączenia telefonicznego uznaje się spełnienie warunku dwukrotnego nieudanego połączenia z osobą wnioskującą w odstępie co najmniej jednego dnia. Za brak możliwości połączenia umożliwiającego transmisję audiowizualną uznaje się nieskuteczną próbę połączenia z wnioskodawcą w wyznaczonym terminie.

§ 7. Minister dostosuje, uwzględniając możliwości techniczne, proces potwierdzania tymczasowego profilu zaufanego, o którym mowa w § 6, do potrzeb osób mających szczególne potrzeby, takie jak niemożność zrozumiałego mówienia czy głuchota.

§ 8. 1. Osoba wnioskująca może samodzielnie dokonać potwierdzenia profilu zaufanego, odpowiednio:

- 1) składając wniosek o potwierdzenie profilu zaufanego w postaci elektronicznej, przy użyciu formularza elektronicznego udostępnionego w systemie, w którym wydawany jest profil zaufany, i opatrując ten wniosek kwalifikowanym podpisem elektronicznym;
- 2) identyfikując się i autoryzując czynność utworzenia i potwierdzenia profilu zaufanego w systemie teleinformatycznym podmiotu niepublicznego przy użyciu środka identyfikacji elektronicznej, o którym mowa w art. 20c ust. 8 ustawy;
- 3) identyfikując się i autoryzując czynność utworzenia i potwierdzenia profilu zaufanego przy użyciu profilu osobistego.

2. Profil zaufany potwierdzony w sposób, o którym mowa w ust. 1:

- 1) pkt 1 opatrzony jest kwalifikowanym podpisem elektronicznym wnioskodawcy;
- 2) pkt 2 i 3 opatrzony jest pieczęcią elektroniczną ministra.

3. W przypadku samodzielnego potwierdzenia profilu zaufanego:

- 1) dane identyfikujące osobę fizyczną, o których mowa w art. 20ad ust. 1 ustawy, ustalone są automatycznie, odpowiednio do metod, o których mowa w ust. 1, na podstawie: kwalifikowanego certyfikatu podpisu elektronicznego albo środka identyfikacji elektronicznej, przy użyciu którego dokonano uwierzytelnienia osoby wnioskującej;
- 2) dane, o których mowa w § 11 ust. 1 pkt 6-8, określane są przez osobę wnioskującą przy użyciu formularza elektronicznego udostępnionego odpowiednio w systemie, w którym wydawany jest profil zaufany, albo w systemie teleinformatycznym podmiotu niepublicznego, o którym mowa w ust. 1 pkt 2.

§ 9. 1. Zakres danych oraz oświadczenia wymagane we wniosku o potwierdzenie profilu zaufanego określa załącznik nr 1 do rozporządzenia.

2. Zakres danych wymagany we wniosku o potwierdzenie tymczasowego profilu zaufanego określa załącznik nr 2 do rozporządzenia.

§ 10. Osoba posiadająca ważny profil zaufany:

- 1) zapewnia poufność danych, które mogłyby być wykorzystane do identyfikacji i uwierzytelnienia w systemie teleinformatycznym przy użyciu profilu zaufanego lub złożenia podpisu zaufanego przez osoby trzecie;
- 2) niezwłocznie unieważnia profil zaufany w przypadku utraty częściowej lub całkowitej kontroli nad tym profilem.

§ 11. 1. Profil zaufany zawiera:

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

2. Raz nadany identyfikator użytkownika nie może być nadany ponownie.

3. W przypadku potwierdzenia profilu zaufanego:

- 1) w punkcie potwierdzającym - profil zaufany zawiera również oznaczenie punktu potwierdzającego oraz imię i nazwisko osoby upoważnionej do potwierdzania profilu zaufanego;
- 2) w sposób, o którym mowa w art. 20c ust. 1 pkt 2 ustawy - profil zaufany zawiera również wskazanie, że został potwierdzony przy wykorzystaniu kwalifikowanego podpisu elektronicznego;
- 3) w sposób, o którym mowa w art. 20c ust. 1 pkt 3 ustawy - profil zaufany zawiera również oznaczenie systemu teleinformatycznego podmiotu niepublicznego, w którym uwierzytelnianie dokonywane jest przy użyciu środka identyfikacji elektronicznej, który posłużył do potwierdzenia profilu zaufanego;
- 4) w sposób, o którym mowa w art. 20c ust. 1 pkt 4 ustawy - profil zaufany zawiera również wskazanie, że został potwierdzony przy wykorzystaniu profilu osobistego;
- 5) w sposób, o którym mowa w art. 20ca ust. 5 ustawy - profil zaufany zawiera również imię i nazwisko osoby upoważnionej do potwierdzania profilu zaufanego.

4. Uwierzytelnienie z wykorzystaniem profilu zaufanego dokonywane jest w sposób zapewniający średni poziom bezpieczeństwa, przy wykorzystaniu co najmniej dwóch czynników uwierzytelnienia należących do co najmniej dwóch różnych kategorii, o których mowa w przepisach wydanych na podstawie art. 8 ust. 3 rozporządzenia 910/2014, przy czym:

- 1) jeden czynnik stanowi:
 - a) identyfikator użytkownika i hasło do konta profilu zaufanego albo
 - b) inny czynnik uwierzytelniania wymagający od osoby podlegającej uwierzytelnieniu określonej, znanej tylko tej osobie wiedzy albo,
 - c) dane posiadacza profilu zaufanego zweryfikowane za pomocą kwalifikowanego certyfikatu podpisu elektronicznego;
- 2) drugi czynnik stanowi:
 - a) hasło jednorazowe przesyłane na wskazany przez użytkownika numer telefonu komórkowego albo
 - b) inny czynnik uwierzytelniania wymagający od posiadacza profilu zaufanego wykazania się posiadaniem ustalonej uprzednio rzeczy lub urządzenia niezbędnego dla wykorzystania tego czynnika.

5. Zamiast identyfikatora użytkownika, o którym mowa w ust. 4 pkt 1 lit. a, użytkownik może używać adresu poczty elektronicznej pod warunkiem, że w systemie, w którym wydawany jest profil zaufany z tym adresem poczty powiązany jest tylko jeden identyfikator.

6. Uwierzytelnienie przy użyciu profilu zaufanego może następować również:

- 1) z wykorzystaniem czynników uwierzytelniania, spełniających warunki określone w ust. 4, wykorzystywanych w ramach środka identyfikacji elektronicznej, o którym mowa w art. 20c ust. 8 ustawy, stosowanego do uwierzytelniania w systemie teleinformatycznym podmiotu niepublicznego;
- 2) wyłącznie przy wykorzystaniu tylko jednego czynnika uwierzytelniania, o którym mowa w ust. 4, jeżeli przepisy prawa regulujące usługę online dopuszczają możliwość uwierzytelnienia użytkownika tej usługi w sposób zapewniający niski poziom bezpieczeństwa, o którym mowa w art. 8 ust. 2 rozporządzenia 910/2014.

7. W przypadku usług online, wymagających uwierzytelnienia użytkownika profilem zaufanym, autoryzacje wymagane w tych usługach dokonywane są przy użyciu drugiego czynnika uwierzytelnienia, o którym mowa w ust. 4 pkt 2, z uwzględnieniem czynników uwierzytelniania, o których mowa w ust. 6 pkt 1, spełniających warunki określone w ust. 4 pkt 2.

8. Posiadacz profilu zaufanego może dokonać zmiany:

- 1) adresu poczty elektronicznej lub numeru telefonu komórkowego - samodzielnie w systemie, w którym wydawany jest profil zaufany, autoryzując tę czynność w sposób, o którym mowa w ust. 7, albo w punkcie potwierdzającym profil zaufany;
- 2) środka identyfikacji elektronicznej lub czynników uwierzytelniania, o których mowa w ust. 6 pkt 1 - samodzielnie w systemie podmiotu niepublicznego;
- 3) czynników uwierzytelniania - samodzielnie w systemie, w którym wydawany jest profil zaufany, albo w systemie teleinformatycznym podmiotu niepublicznego, o ile w systemie tym udostępniono taką możliwość.

9. Przepisów ust. 8 nie stosuje się dla tymczasowego profilu zaufanego jeżeli dokonana zmiana wiązałaby się z automatycznym przedłużeniem ważności profilu zaufanego.

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

11. Struktura danych profilu zaufanego oraz podpisu zaufanego udostępniane są przez ministra w Biuletynie Informacji Publicznej na stronie podmiotowej ministra.

12. W przypadku użytkownika ePUAP czynniki, o których mowa w ust. 4 pkt 1 lit. a, są tożsame z czynnikami służącymi do identyfikacji i uwierzytelniania tego użytkownika w ePUAP.

13. System, w którym wydawany jest profil zaufany wymaga stosowania hasła, o którym mowa w ust. 4 pkt 1 lit. a, które spełnia wymogi w zakresie stopnia złożoności oraz wymaganej częstotliwości zmian, ustalonych przez ministra.

§ 12. 1. Profil zaufany potwierdza się na okres trzech lat, a jego ważność może być przedłużona na taki sam okres.

2. Osoba posiadająca profil zaufany może dokonać przedłużenia jego ważności:

- 1) samodzielnie w systemie, w którym wydawany jest profil zaufany, potwierdzając tę czynność przy wykorzystaniu profilu zaufanego, profilu osobistego albo kwalifikowanego podpisu elektronicznego;
- 2) w punkcie potwierdzającym.

3. W systemie, w którym wydawany jest profil zaufany, gromadzone są dane odzwierciedlające historię kolejnych przedłużeń ważności profilu zaufanego obejmujące w szczególności czas i sposób przedłużenia.

4. Zakres danych oraz oświadczenia wymagane we wniosku o przedłużenie ważności profilu zaufanego określa załącznik nr 3 do rozporządzenia.

5. Przepisów ust. 1, 2 i 4 nie stosuje się dla tymczasowego profilu zaufanego.

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

- 1) okazania nieważnego dokumentu, o którym mowa w § 4 ust. 2 lub § 6 ust. 5 pkt 3, lub braku możliwości jednoznacznego potwierdzenia tożsamości osoby wnioskującej na podstawie okazanego dokumentu;
- 2) niezgodności imienia, imion lub nazwiska podanych w złożonym wniosku o potwierdzenie profilu zaufanego z danymi ustalonymi na podstawie okazanego przez wnioskodawcę dokumentu tożsamości;
- 3) niezgodności numeru PESEL podanego w złożonym wniosku o potwierdzenie profilu zaufanego z numerem PESEL ustalonym na podstawie okazanego przez wnioskodawcę dokumentu tożsamości;
- 4) niezgodności daty urodzenia ustalonej na podstawie pierwszych sześciu cyfr numeru PESEL podanego w złożonym wniosku o potwierdzenie profilu zaufanego z datą urodzenia ustaloną na podstawie okazanego przez wnioskodawcę dokumentu tożsamości - w przypadku gdy okazany dokument tożsamości nie zawiera numeru PESEL;

- 5) niewystarczającej jakości transmisji audiowizualnej albo nagrania tej transmisji, o których mowa w § 6 niepozwalającej na odczytanie danych z warstwy graficznej okazywanego dokumentu tożsamości;
- 6) wątpliwości odnośnie porównania wizerunku wnioskodawcy z wizerunkiem z Rejestru Dowodów Osobistych zarejestrowanego w trakcie transmisji audiowizualnej o której mowa w § 6 z wizerunkiem pobranym z Rejestru Dowodów Osobistych i brakiem możliwości potwierdzenia tożsamości osoby wnioskującej za pomocą dodatkowych danych, o których mowa w § 6 ust. 10;
- 7) braku możliwości pobrania wizerunku Rejestru Dowodów Osobistych - w przypadku potwierdzenia profilu zaufanego w ramach usługi, o której mowa w art. 20ca ustawy;
- 8) braku oświadczenia wnioskodawcy, o którym mowa w § 6 ust. 6 pkt 4;
- 9) niestosowania się wnioskodawcy do poleceń osoby upoważnionej do potwierdzenia tymczasowego profilu zaufanego, skutkującego brakiem możliwości zarejestrowania w trakcie transmisji audiowizualnej:
 - a) wizerunku wnioskodawcy, oraz dokonania porównania tego wizerunku w sposób o którym mowa w § 6 ust. 5 pkt 3, lub
 - b) danych zawartych w warstwie graficznej okazywanego dokumentu tożsamości.

2. Niedokonanie potwierdzenia profilu zaufanego w punkcie potwierdzającym osoba upoważniona do potwierdzenia profilu zaufanego odnotowuje na wydruku wniosku o potwierdzenie profilu zaufanego wraz z podaniem czasu i przyczyny niedokonania potwierdzenia.

3. Niedokonanie potwierdzenia tymczasowego profilu zaufanego osoba upoważniona do potwierdzenia profilu zaufanego odnotowuje w systemie, w którym wydawany jest profil zaufany, określając przyczynę niedokonania potwierdzenia.

4. Informacja o niedokonaniu potwierdzenia tymczasowego profilu zaufanego oraz o przyczynie niedokonania potwierdzenia, o której mowa w ust. 3, jest automatycznie wysyłana na adres poczty elektronicznej wnioskodawcy, podany w treści wniosku o potwierdzenie tymczasowego profilu zaufanego.

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

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

2. W przypadku zmiany adresu poczty elektronicznej, numeru telefonu komórkowego albo środka identyfikacji elektronicznej stosowanego do uwierzytelniania w systemie

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

3. Osoba posiadająca profil zaufany może samodzielnie dokonać unieważnienia swojego profilu zaufanego w systemie, w którym wydawany jest profil zaufany, albo wystąpić z wnioskiem o unieważnienie profilu zaufanego.

4. W celu unieważnienia profilu zaufanego na wniosek osoba posiadająca profil zaufany składa wniosek w wybranym przez siebie punkcie potwierdzającym, w którym osoba upoważniona do potwierdzenia profilu zaufanego unieważnia profil zaufany, stwierdzając uprzednio tożsamość osoby wnioskującej na podstawie okazanego dokumentu tożsamości.

5. Zakres danych oraz oświadczenia wymagane we wniosku o unieważnienie profilu zaufanego określa załącznik nr 4 do rozporządzenia.

§ 15. 1. Profil zaufany może być unieważniony, bez udziału jego posiadacza, w przypadku:

- 1) wykrycia nieprawidłowości w procedurze jego potwierdzenia lub przedłużenia jego ważności;
- 2) wykrycia nieprawidłowości mogących mieć wpływ na rozliczalność i niezaprzeczalność działań dokonywanych z wykorzystaniem profilu zaufanego:
 - a) stwierdzenia lub uzasadnionych przesłanek wskazujących na wysokie prawdopodobieństwo, że dane, które mogą pozwolić na użycie profilu zaufanego, przestały być pod wyłączną kontrolą jego posiadacza,
 - b) wykrycia nieuprawnionego użycia profilu zaufanego;
- 3) wykrycia w profilu zaufanym nieprawidłowości:
 - a) zagrażających bezpieczeństwu lub prawidłowemu działaniu systemu, w którym wydawany jest profil zaufany,
 - b) wykluczających użytkowanie profilu zaufanego w sposób zapewniający poziom bezpieczeństwa, o którym mowa w § 11 ust. 4;

2. W przypadku uzasadnionego podejrzenia nieprawidłowości, o których mowa w ust. 1, dopuszcza się dokonywanie przez ministra czynności sprawdzających mających na celu potwierdzenie lub zaprzeczenie istnienia tych nieprawidłowości.

3. W toku czynności, o których mowa w ust. 2, dopuszcza się możliwość żądania od posiadacza profilu zaufanego dokonania czynności lub przekazania danych, które pozwolą na zaprzeczenie istnienia nieprawidłowości.

§ 16. 1. Złożenie podpisu zaufanego jest możliwe w okresie ważności użytego do złożenia podpisu środka identyfikacji elektronicznej, o którym mowa w art. 20aa pkt 1 ustawy.

2. Czynność złożenia podpisu zaufanego wymaga autoryzacji, po której następuje opatrzenie podpisywanych danych w postaci elektronicznej pieczęcią elektroniczną ministra wykorzystywaną do zapewnienia integralności podpisanych danych oraz autentyczności złożonego podpisu.

3. Autoryzacja, o której mowa w ust. 2, dokonywana jest, odpowiednio do użytego środka identyfikacji elektronicznej:

- 1) w przypadku profilu osobistego - w sposób określony dla tego środka identyfikacji elektronicznej w przepisach wydanych na podstawie art. 12j ustawy z dnia 6 sierpnia 2010 r. o dowodach osobistych (Dz.U. z 2020 r. poz. 332);
- 2) w przypadku profilu zaufanego - w sposób, o którym mowa w § 11 ust. 7.

3. Weryfikacja integralności danych podpisanych przy użyciu podpisu zaufanego oraz autentyczności tego podpisu dokonywana jest za pomocą certyfikatu pieczęci elektronicznej udostępnionego przez ministra pod adresem elektronicznym wskazanym w Biuletynie Informacji Publicznej na stronie podmiotowej ministra.

4. Osoba podejmująca czynności zmierzające do złożenia podpisu zaufanego, przed faktycznym złożeniem tego podpisu elektronicznego, informowana jest w drodze komunikatu udostępnianego w interfejsie użytkownika oprogramowania umożliwiającego złożenie takiego podpisu, że dokonuje czynności złożenia podpisu zaufanego.

§ 17. 1. Podmioty, o których mowa w art. 20c ust. 3 ustawy, mogą pełnić funkcję punktu potwierdzającego profil zaufany po uprzednim przedłożeniu ministrowi oświadczenia o spełnieniu wymagań w zakresie opracowywania i ustanawiania, wdrażania i eksploataowania monitorowania i przeglądania oraz utrzymywania i doskonalenia systemu zarządzania bezpieczeństwem informacji spełniającego wymagania o których mowa w przepisach wydanych na podstawie art. 18 ustawy w zakresie, w jakim dotyczyć to będzie uprawnień i czynności osób upoważnionych do potwierdzania profilu zaufanego.

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

3. Punkt potwierdzający, o którym mowa w art. 20c ust. 3 pkt 2-5 ustawy, w przypadku gdy nie posiada instrukcji określającej zasady i tryb postępowania z dokumentacją wydanej na podstawie ustawy z dnia 14 lipca 1983 r. o narodowym zasobie archiwalnym i archiwach (Dz.U. z 2020 r. poz. 164), zapewnia wdrożenie instrukcji określającej zasady i tryb

postępowania z dokumentacją związaną z potwierdzaniem, przedłużaniem ważności i unieważnianiem profilu zaufanego oraz przedkłada ministrowi kopię tego dokumentu.

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

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

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

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

3. Obowiązek przechowania dokumentów, o których mowa w ust. 1 i 2, trwa przez okres 20 lat od chwili potwierdzenia albo przedłużenia ważności profilu zaufanego lub od chwili odmowy jego potwierdzenia albo odmowy przedłużenia ważności bądź od chwili jego unieważnienia z wyłączeniem nagrania, o którym mowa w § 6, które przechowuje się przez 6 lat.

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

§ 19. Unieważnienie profilu zaufanego może być dokonane za pośrednictwem systemu teleinformatycznego podmiotu niepublicznego, przy użyciu środka identyfikacji elektronicznej, o którym mowa w art. 20c ust. 8 ustawy.

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

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

² Zmiana wymienionego rozporządzenia została ogłoszona w Dz. Urz. UE L 345 z 20.12.2016, str. 142

oraz wykorzystywanie udostępnionych środków identyfikacji elektronicznej w systemie;

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

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

- 1) ważnego akredytowanego certyfikatu, obejmującego w swym zakresie stosowanie środków identyfikacji elektronicznej, systemu zarządzania bezpieczeństwem informacji, albo
- 2) protokołu pokontrolnego kontroli organu nadzoru, potwierdzającego wdrożenie wymogów określonych w przepisach wydanych na podstawie art. 137 ust. 1 pkt 5 ustawy z dnia 29 sierpnia 1997 r. - Prawo bankowe (Dz. U. z 2020 r. poz. 284, 288, 321) w zakresie dotyczącym zarządzania obszarami technologii informacyjnej i bezpieczeństwa środowiska teleinformatycznego w bankach, albo
- 3) pozytywnego wyniku audytu, o którym mowa w ust. 1 pkt 3, przeprowadzonego nie wcześniej niż 15 miesięcy przed dniem złożenia przez podmiot niepubliczny wniosku do ministra o wyrażenie zgody na wykorzystywanie do potwierdzania profilu zaufanego środków identyfikacji elektronicznej, stosowanych do uwierzytelniania w systemie teleinformatycznym podmiotu niepublicznego, albo
- 4) innego dokumentu potwierdzającego spełnianie warunków, o których mowa w ust. 1 pkt 1-4.

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

§ 21. 1. Podmiot niepubliczny przedstawia dokumenty, o których mowa w § 20 ust. 2 i 3, na żądanie ministra.

2. W przypadku, gdy do potwierdzenia profilu zaufanego wykorzystano środek identyfikacji elektronicznej, stosowany do uwierzytelniania w systemie teleinformatycznym podmiotu niepublicznego, wydany przez ten podmiot niepubliczny w procesie w którym okazanie dokumentu tożsamości nastąpiło w trakcie transmisji audiowizualnej, o której mowa w § 20 ust. 1 pkt 4 lit. a, podmiot ten przechowuje nagranie tej transmisji audiowizualnej, przez okres 6 lat, chyba, że przepisy odrębne wymagają dłuższego okresu przechowywania.

§ 22. System, w którym wydawany jest profil zaufany, uniemożliwia usunięcie konta profilu zaufanego w przypadku, gdy prowadziłoby to do utraty kontroli użytkownika tego konta nad jego kontem w ePUAP.

§ 23. 1 Minister co najmniej raz na dwa lata dokonuje sprawdzenia mającego na celu ustalenie kont nieużywanych celem ich usunięcia.

2. W przypadku ustalenia konta nieużywanego dokonuje się dwukrotnego powiadomienia użytkownika tego konta na adres poczty elektronicznej powiązany z tym kontem profilu zaufanego, w odstępie 30 dni, o zamiarze jego usunięcia.

3. Powiadomienie, o którym mowa w ust. 2, zawiera informację dotyczącą oczekiwanych czynności, jakich posiadacz konta profilu zaufanego może dokonać na potwierdzenie woli dalszego korzystania z wskazanego konta nieużywanego.

4. W przypadku niepodjęcia przez użytkownika konta profilu zaufanego czynności, o których mowa w ust. 3, w terminie 30 dni od przesłania drugiego powiadomienia, konto nieużywane jest usuwane.

§ 24. 1. Minister może, w drodze porozumienia lub umowy, upoważnić do potwierdzania tymczasowych profili zaufanych w sposób, o którym mowa w art. 20ca ustawy:

- 1) punkt potwierdzający, o którym mowa w art. 20c ust 2 pkt 1 - 4 ustawy,
- 2) jednostkę podległą lub nadzorowaną.

2. Porozumienie lub umowa, o których mowa w ust. 1, określają warunki organizacyjne i techniczne potwierdzania tymczasowego profilu zaufanego.

§ 25. Wnioski o potwierdzenie, profilu zaufanego złożone przed dniem wejścia w życie rozporządzenia są rozpatrywane na zasadach dotychczasowych.

§ 26. Wnioski, o których mowa w art. 20c ust. 4 ustawy, złożone przed dniem wejścia w życie rozporządzenia, są rozpatrywane na zasadach dotychczasowych.

§ 27. Zachowują moc zgody wydane, na podstawie art. 20c ust. 8 ustawy, przed dniem wejścia w życie niniejszego rozporządzenia.

§ 28. Rozporządzenie wchodzi w życie z dniem następującym po dniu ogłoszenia.³⁾

³⁾ Niniejsze rozporządzenie było poprzedzone rozporządzeniem Ministra Cyfryzacji z dnia 10 września 2018 r w sprawie profilu zaufanego i podpisu zaufanego (Dz.U. z 2018 r. poz. 1760 zm. Dz.U. z 2019 r. poz. 403), które utraci moc z dniem 1 października 2020 r., na podstawie art. 99 ustawy z dnia 31 marca 2020 r. o zmianie ustawy o zmianie ustawy o szczególnych rozwiązaniach związanych z zapobieganiem, przeciwdziałaniem i zwalczaniem COVID-19, innych chorób zakaźnych oraz wywołanych nimi sytuacji kryzysowych oraz niektórych innych ustaw (Dz.U. z 2020 r. poz. 568)

MINISTER CYFRYZACJI

Za zgodność pod względem prawnym,
legislacyjnym i redakcyjnym
Iwona Szulc
Zastępca Dyrektora
Departamentu Prawnego
w Ministerstwie Cyfryzacji
/podpisano elektronicznie/

Załączniki do rozporządzenia
Ministra Cyfryzacji
z dnia ... 2020 r. (poz. ...)

Załącznik nr 1

Zakres danych oraz oświadczenia wymagane we wniosku o potwierdzenie profilu zaufanego:

- 1) dane dotyczące osoby wnioskującej:
 - a) imię (imiona),
 - b) nazwisko,
 - c) numer PESEL,
 - d) identyfikator użytkownika,
 - e) identyfikator profilu zaufanego,
 - f) adres poczty elektronicznej,
 - g) numer telefonu komórkowego,
 - h) wybrane czynniki uwierzytelniania;
- 2) oświadczenia osoby wnioskującej, że:
 - a) dane zawarte we wniosku są prawdziwe i aktualne,
 - b) zapewni poufność danych, które mogłyby być wykorzystane do identyfikacji i uwierzytelnienia w systemie teleinformatycznym przy użyciu profilu zaufanego lub złożenia podpisu zaufanego przez osoby trzecie,
 - c) nie udostępni konta profilu zaufanego osobom trzecim,
 - d) niezwłocznie unieważni profil zaufany w przypadku utraty częściowej lub całkowitej kontroli nad tym profilem;
- 3)¹⁾ miejscowość i data oraz czytelny podpis osoby wnioskującej;
- 4)¹⁾ adnotacje osoby upoważnionej do potwierdzania profilu zaufanego w imieniu punktu potwierdzającego:
 - a) dane dotyczące punktu potwierdzającego:
 - nazwa punktu potwierdzającego,
 - znak sprawy nadany w punkcie potwierdzającym,
 - b) dane dotyczące osoby upoważnionej do potwierdzania profilu zaufanego:

imię,

¹⁾ dotyczy potwierdzenia profilu zaufanego w punkcie potwierdzającym.

- nazwisko,
 - stanowisko służbowe,
- c) w przypadku stwierdzania tożsamości osoby wnioskującej na podstawie dokumentu tożsamości niezawierającego numeru PESEL, jeżeli na jego podstawie stwierdzono tożsamość osoby wnioskującej - dane dotyczące tego dokumentu tożsamości:
- kraj wydania,
 - rodzaj,
 - numer,
- d) informacje dotyczące potwierdzenia profilu zaufanego:
- miejscowość i data,
 - czas potwierdzenia (godzina i minuta),
 - czytelny podpis osoby upoważnionej do potwierdzania profilu zaufanego albo informacje o niepotwierdzeniu profilu zaufanego:
 - przyczyna niepotwierdzenia,
 - miejscowość i data,
 - czas (godzina i minuta),
 - czytelny podpis osoby upoważnionej do potwierdzania profilu zaufanego,
- e) inne lub uzupełniające adnotacje.

Załącznik nr 2

Zakres danych wymagany we wniosku o potwierdzenie tymczasowego profilu zaufanego:

- 1) dane dotyczące osoby wnioskującej:
 - a) imię (imiona),
 - b) nazwisko,
 - c) numer PESEL,
 - d) identyfikator użytkownika,
 - e) identyfikator profilu zaufanego,
 - f) adres poczty elektronicznej,
 - g) numer telefonu komórkowego,
 - h) wybrane czynniki uwierzytelniania;
- 2) dane dotyczące punktu potwierdzającego:
 - a) nazwa punktu potwierdzającego,
 - b) znak sprawy nadany w punkcie potwierdzającym,
- 3) dane dotyczące osoby upoważnionej do potwierdzania profilu zaufanego:
 - a) imię,
 - b) nazwisko,
 - c) stanowisko służbowe,
- 4) w przypadku potwierdzenia wniosku o tymczasowy profil zaufany:
 - a) data,
 - b) czas potwierdzenia (godzina i minuta),
- 5) w przypadku odrzucenia wniosku o tymczasowy profil zaufany
 - a) data,
 - b) adnotacje dotyczące powodu odrzucenia;
- 6) inne lub uzupełniające adnotacje.

Załącznik nr 3

Zakres danych oraz oświadczenia wymagane we wniosku o przedłużenie ważności profilu zaufanego zawiera:

- 1) dane dotyczące osoby wnioskującej:
 - a) imię (imiona),
 - b) nazwisko,
 - c) numer PESEL,
 - d) identyfikator użytkownika,
 - e) identyfikator profilu zaufanego,
 - f) adres poczty elektronicznej,
 - g) numer telefonu komórkowego,
 - h) wybrane czynniki uwierzytelniania;
- 2) oświadczenia osoby wnioskującej, że:
 - a) dane zawarte we wniosku są prawdziwe i aktualne,
 - b) zapewni poufność danych, które mogłyby być wykorzystane do identyfikacji i uwierzytelnienia w systemie teleinformatycznym przy użyciu profilu zaufanego lub złożenia podpisu zaufanego przez osoby trzecie,
 - c) nie udostępni konta profilu zaufanego osobom trzecim,
 - d) niezwłocznie unieważni profil zaufany w przypadku utraty częściowej lub całkowitej kontroli nad tym profilem;
- 3)¹⁾ miejscowość i data oraz czytelny podpis osoby wnioskującej;
- 4)¹⁾ adnotacje osoby upoważnionej do potwierdzania profilu zaufanego w imieniu punktu potwierdzającego:
 - a) dane dotyczące punktu potwierdzającego:
 - nazwa punktu potwierdzającego,
 - znak sprawy nadany w punkcie potwierdzającym,
 - b) dane dotyczące osoby upoważnionej do potwierdzania profilu zaufanego:
 - imię,
 - nazwisko,
 - stanowisko służbowe,
 - c) informacje dotyczące przedłużenia profilu zaufanego:

¹⁾ dotyczy przedłużenia ważności profilu zaufanego w punkcie potwierdzającym.

- miejscowość i data,
 - czas przedłużenia (godzina i minuta),
 - czytelny podpis osoby upoważnionej do potwierdzania profilu zaufanego albo informacje o niedokonaniu przedłużenia profilu zaufanego:
 - przyczyna niedokonania przedłużenia,
 - miejscowość i data,
 - czytelny podpis osoby upoważnionej do potwierdzania profilu zaufanego,
- d) inne lub uzupełniające adnotacje.

Załącznik nr 4

Zakres danych oraz oświadczenia wymagane we wniosku o unieważnienie profilu zaufanego:

- 1) dane dotyczące osoby wnioskującej:
 - a) imię (imiona),
 - b) nazwisko,
 - c) numer PESEL,
 - d) identyfikator użytkownika,
 - e) identyfikator profilu zaufanego;
- 2) oświadczenie osoby wnioskującej, że dane zawarte we wniosku są prawdziwe i aktualne;
- 3)¹⁾ miejscowość i data oraz czytelny podpis osoby wnioskującej;
- 4)¹⁾ adnotacje osoby upoważnionej do potwierdzania profilu zaufanego w imieniu punktu potwierdzającego:
 - a) dane dotyczące punktu potwierdzającego:
 - nazwa punktu potwierdzającego,
 - znak sprawy nadany w punkcie potwierdzającym,
 - b) dane dotyczące osoby upoważnionej do potwierdzania profilu zaufanego:
 - imię,
 - nazwisko,
 - stanowisko służbowe,
 - c) informacje dotyczące wniosku o unieważnienie profilu zaufanego:
 - data złożenia wniosku,
 - czas złożenia wniosku (godzina i minuta),
 - d) informacje dotyczące unieważnienia profilu zaufanego:
 - miejscowość i data,
 - czytelny podpis osoby upoważnionej do potwierdzania profilu zaufanego,
 - e) inne lub uzupełniające adnotacje.

¹⁾ dotyczy unieważnienia profilu zaufanego w punkcie potwierdzającym.

UZASADNIENIE

Projektowane rozporządzenie stanowi wykonanie upoważnienia ustawowego zawartego w art. 20d ustawy z dnia 17 lutego 2005 r. o informatyzacji działalności podmiotów realizujących zadania publiczne (Dz. U z 2020 r. poz. 346 z poz. zm. 568 i 695) zwanej dalej „ustawą o informatyzacji”.

Konieczność wydania aktu wykonawczego wynika z faktu, iż na mocy art. 33 ustawy z dnia 31 marca 2020 r. o zmianie ustawy o szczególnych rozwiązaniach związanych z zapobieganiem, przeciwdziałaniem i zwalczaniem COVID-19, innych chorób zakaźnych oraz wywołanych nimi sytuacji kryzysowych oraz niektórych innych ustaw (Dz.U. z 2020 r. poz. 568), wprowadzone zostały do ustawy o informatyzacji zmiany dotyczące sposobu potwierdzania profilu zaufanego. W szczególności w dodanym art. 20ca ustawy o informatyzacji umożliwiono zdalne potwierdzanie tożsamości osoby fizycznej polegające na tym, że dokument tożsamości (dowód osobisty lub paszport) osoby, która złożyła wniosek o potwierdzenie profilu zaufanego o krótszym okresie ważności (tymczasowego profilu zaufanego), może być okazany w trakcie nagrywanej transmisji audiowizualnej. Aktualne rozporządzenie obowiązuje jedynie do momentu wydania nowego rozporządzenia, jednak nie dłużej niż do dnia 1 października 2020 r.

Regulacje zawarte w projektowanym rozporządzeniu stanowią w znacznej części powtórzenie przepisów zawartych w obowiązującym rozporządzeniu Ministra Cyfryzacji z dnia 10 września 2018 r w sprawie profilu zaufanego i podpisu zaufanego (Dz. U. poz. 1760 oraz z 2019 r. poz. 403). Dodano przepisy odnoszące się do nowych możliwości zdalnego potwierdzania tożsamości podczas transmisji audiowizualnej, o której mowa w art. 20ca ust. 5 pkt 1 lit a i b ustawy o informatyzacji, a także dookreślono sposób realizacji możliwości, o której mowa w art. 20ca ust. 5 pkt 1 lit c ustawy.

Mając na uwadze umocowaną już ustawowo możliwość zdalnego potwierdzania tożsamości osoby wnioskującej o profil zaufany w oparciu o dokument tożsamości okazywany zdalnie podczas transmisji audiowizualnej, panującą epidemię COVID-19, jak również

gotowość systemów teleinformatycznych stosowanych w bankowości elektronicznej⁴ umożliwiono także potwierdzenie profilu zaufanego za pomocą środka identyfikacji elektronicznej podmiotu niepublicznego wydanego zdalnie w oparciu o potwierdzenie tożsamości realizowane w trakcie nagrywanej w czasie rzeczywistym transmisji audiowizualnej, podczas której okazywany jest dokument tożsamości, który zawiera numer PESEL. Taka możliwość wymaga od podmiotu wydającego środek identyfikacji elektronicznej, tak samo jak w przypadku obecności fizycznej osoby okazującej dokument tożsamości, zachowania należytej staranności w ustaleniu autentyczności dokumentu tożsamości oraz działań zmierzających do zminimalizowania ryzyka, że tożsamość deklarowana przy użyciu okazanego dokumentu tożsamości jest niezgodna z faktyczną tożsamością osoby okazującej ten dokument. Banki krajowe, które mają już wdrożone rozwiązania umożliwiające bezpieczne zdalne potwierdzanie tożsamości w celu wydania środka identyfikacji elektronicznej w swoim systemie teleinformatycznym, będą mogły umożliwić swoim klientom także potwierdzanie profilu zaufanego co dotąd nie było możliwe. Przyczyni się to także do zmniejszenia obciążenia usługi zdalnego potwierdzania tymczasowego profilu zaufanego świadczonej przez ministra i zwiększy dostęp do profilu zaufanego dla osób, które nie powinny lub nawet nie mogą wychodzić z domu.

W przedkładanym projekcie rozporządzenia dokonano następujących zmian w stosunku do obowiązującego rozporządzenia :

1. Ustalono, że w celu uzyskania tymczasowego profilu zaufanego podobnie jak w przypadku profilu zaufanego o trzyletnim okresie ważności również należy złożyć wniosek wypełniając formularz elektroniczny udostępniony w systemie, w którym wydawany jest profil zaufany (§ 4).

2. W § 6 doprecyzowano proces potwierdzania tymczasowego profilu zaufanego. Wskazano, że to osoba potwierdzająca tymczasowy profil zaufany przejmuje inicjatywę potwierdzania złożonego wniosku o profil zaufany. W przeciwieństwie do procesu potwierdzania profilu zaufanego w punkcie potwierdzającym osoba wnioskująca nie

⁴ Zob. *Stanowisko UKNF dotyczące identyfikacji klienta i weryfikacji jego tożsamości w bankach oraz oddziałach instytucji kredytowych w oparciu o metodę wideoweryfikacji z 5 czerwca 2019 r.*

https://www.knf.gov.pl/knf/pl/komponenty/img/Stanowisko_UKNF_dot_identyfikacji_klienta_i_weryfikacji_jego_tozsamosci_w_bankach_oraz_oddzialach_instytucji_kredytowych_w_oparciu_o_metode_wideoweryfikacji_66066.pdf

kontaktuje się z punktem potwierdzającym tylko odwrotnie, osoba potwierdzająca profil zaufany wyszukuje w systemie niezalutowany wniosek o profil zaufany i to jej inicjatywy zaczyna się proces potwierdzania profilu zaufanego. W pierwszej kolejności osoba potwierdzająca profil zaufany weryfikuje czy imię (imiona), nazwisko i nr PESEL podane we wniosku zgadzają się z danymi rejestrze PESEL oraz czy w Rejestrze Dowodów Osobistych znajduje się fotografia wnioskodawcy wymagana przepisami ustawy. Weryfikacja następuje automatycznie za pomocą narzędzia udostępnionego w systemie, w którym wydawany jest profil zaufany aby jednocześnie maksymalnie uprościć proces potwierdzania profilu zaufanego, minimalizować możliwość pomyłek osoby potwierdzającej i nie udostępniać danych osobowych bez potrzeby w przypadku ich niezgodności z rejestrami. Jeżeli weryfikacja jest niepoprawna osoba potwierdzająca tymczasowy profil zaufany odrzuca wniosek z powodu niezgodności danych.

Jeżeli weryfikacja jest poprawna osoba potwierdzająca tymczasowy profil zaufany kontaktuje się z osobą wnioskującą – najpierw telefonicznie celem ustalenia sposobu i terminu połączenia umożliwiającego transmisję audiowizualną, a dopiero potem nawiązuje połączenie audiowizualne. Takie dwuetapowe rozwiązanie stanowi dodatkowe zabezpieczenie przed potencjalnymi oszustwami polegającymi na podawaniu się osoby nieuprawnionej za osobę upoważnioną do potwierdzenia profilu zaufanego celem wyłudzenia danych. Podczas połączenia telefonicznego jak również podczas transmisji audiowizualnej osoba upoważniona do potwierdzenia profilu zaufanego podaje numer wniosku automatycznie nadany przez system w którym wydawany jest profil zaufany – numer taki może być znany tylko osobie potwierdzającej co upewnia osobę wnioskującą, że nikt nie podszywa się pod osobę upoważnioną. Pozostawienie inicjatywy połączenia osobie potwierdzającej tymczasowe profile zaufane ma na celu umożliwienie kolejnego potwierdzania profili zaufanych w miarę możliwości osób potwierdzających. Ustalono regułę, że jakość transmisji audiowizualnej ma pozwolić na odczytanie danych zawartych w warstwie graficznej okazywanego podczas połączenia dowodu osobistego albo paszportu wnioskodawcy. Mając na uwadze, że w ustawie o dowodach osobistych jest wskazanie co zwiera warstwa graficzna dowodu osobistego oczywiste jest, że nagranie ma umożliwić odczytanie tych danych. Ten wymóg ma na celu zabezpieczenie przed potwierdzeniem profilu zaufanego na podstawie niemożliwych do późniejszego zweryfikowania danych jak również będzie stanowił, udokumentowany nagraniem audiowizualnym, dowód odmowy potwierdzenia profilu zaufanego z powodu niewystarczającej jakości transmisji, jak również dowód dla innych celów weryfikacyjnych lub

dowodowych. Mimo że art. 20 ca nie ma przewidzianego uprawnienia do weryfikacji i oceny jakości nagrania z transmisji audiowizualnej, po zakończeniu tej transmisji, mając na uwadze ust. 7 tego artykułu stanowiący że „minister właściwy do spraw informatyzacji sporządza nagranie audiowizualne z transmisji, o której mowa w ust. 5 pkt 1, i przechowuje je przez okres 6 lat” za oczywiste uznaje się, że dopiero po weryfikacji poprawności technicznej nagrania z transmisji audiowizualnej potwierdzenie wniosku jest możliwe. W przeciwnym razie nie byłoby pewności wykonania przez ministra wymogu ustanowionego ustawą.

Mając na uwadze, że w przypadku zdalnego potwierdzenia profilu zaufanego nie powstaje podpisany dokument zawierający deklarację posiadacza profilu zaufanego, dla zachowania reguł bezpieczeństwa użytkowania tego środka identyfikacji elektronicznej wymaga się, aby stosowne oświadczenia zostały złożone podczas transmisji audiowizualnej.

Tymczasowy profil zaufany podobnie jak profil zaufany potwierdzany w punkcie potwierdzającym jest podpisywany w systemie profilu zaufanego podpisem zaufanym lub kwalifikowanym podpisem elektronicznym osoby potwierdzającej podpisuje profil zaufany.

Doprecyzowano sposób wykorzystania możliwości, o której mowa w art. 20ca pkt 1 lit c ustawy, to znaczy weryfikacji wiedzy wnioskodawcy przy wykorzystaniu danych dotyczących wnioskodawcy zgromadzonych w rejestrach publicznych lub w systemach teleinformatycznych.

Przepis § 6 ust. 3 zobowiązuje osobę upoważnioną do potwierdzania tymczasowego profilu zaufanego do odrzucenia wniosku o tymczasowy profil zaufany w przypadku gdy nie jest możliwe uzyskania połączenia telefonicznego lub audiowizualnego z osobą wnioskującą. Mając na uwadze stworzenie koniecznej równowagi pomiędzy możliwością poświęcenia określonej ilości czasu na obsługę jednego wniosku przez osobę upoważnioną do potwierdzania tymczasowego profilu zaufanego, a przewidywanymi potrzebami w tym zakresie ustalono, że do odrzucenia wniosku wystarczają dwie nieudane próby uzyskania połączenia telefonicznego podejmowane w odstępie co najmniej jednego dnia. lub nieudana próba uzyskania połączenia celem rozpoczęcia transmisji audiowizualnej w wyznaczonym terminie.

3. W § 11 ust. 5 doprecyzowano, że użytkownik może używać adresu poczty elektronicznej zamiast unikatowego identyfikatora pod warunkiem, że w systemie, w którym wydawany jest profil zaufany, z tym adresem poczty powiązany jest tylko jeden identyfikator. Przepis stał się potrzebny ze względu na to, że to udogodnienie wprowadzane w licznych systemach wymagających identyfikacji użytkowników jest dość często mylnie rozumiane

przez posiadaczy profilu zaufanego jako utrudnienie. Dzieje się tak w przypadku gdy sam użytkownik założy kilka kont w systemie, w którym wydawany jest profil zaufany, co w efekcie powoduje, że nie ma możliwości przyporządkowania weryfikacji hasła, bo nie wiadomo do jakiego konta użytkownik zamierza się logować. Przepis rozwieje wątpliwości w tym zakresie.

4. W § 11 ust. 6 pkt 2 doprecyzowano, że uwierzytelnienie przy użyciu profilu zaufanego może następować również przy wykorzystaniu tylko jednego czynnika uwierzytelniania, o którym mowa w ust. 4, jeżeli przepisy prawa regulujące usługę online dopuszczają możliwość uwierzytelnienia użytkownika tej usługi w sposób zapewniający niski poziom bezpieczeństwa.

5. W § 11 ust. 9 doprecyzowuje się wymagania art. 20ca ust. 2-3 ustawy, z których wynika, że tymczasowy profil zaufany jest ważny tylko 3 miesiące a okres ważności takiego profilu zaufanego może wydłużyć minister właściwy do spraw informatyzacji uwzględniając szczególne okoliczności. Oznacza to, że dla posiadaczy tymczasowego profilu zaufanego nie mogą być dostępne możliwości samodzielnego przedłużenia ważności profilu zaufanego. System jest obecnie tak skonstruowany, że zmiana adresu poczty elektronicznej lub numeru telefonu komórkowego – realizowana samodzielnie w systemie, w którym wydawany jest profil zaufany – powoduje automatycznie wydłużenie ważności profilu zaufanego.

6. W § 13 ust. 1 dodano pkt 5-9 wskazujące w jakich szczególnych przypadkach nie potwierdza się profilu zaufanego w przypadku, gdy potwierdzenie profilu zaufanego następuje w ramach usługi, o której mowa w art. 20ca ustawy. Mając na uwadze, że tymczasowy profil zaufany wydawany w ramach tej usługi to także profil zaufany, tylko o krótszym terminie ważności, pozostałe przepisy ust. 1 też się do niego odnoszą.

7. W § 13 dodano ust. 3 i 4 regulujące sposób w jaki odnotowuje się niedokonanie potwierdzenia profilu zaufanego w ramach usługi, o której mowa w art. 20ca ustawy oraz w jaki sposób informowana jest o tym osoba wnioskująca.

8. W § 14 ust. 4 doprecyzowano że w tym przepisie chodzi o możliwość unieważnienia profilu zaufanego na wniosek w punkcie potwierdzającym. Istnieje bowiem możliwość unieważnienia profilu zaufanego zdalnie w systemie, w którym wydawany jest profil zaufany.

9. W § 17 ust. 1 zmieniono wymagania dla podmiotów o których mowa w art. 20c ust. 3 ustawy. Obecnie mogą one pełnić funkcję punktu potwierdzającego profil zaufany po uprzednim przedłożeniu ministrowi oświadczenia o spełnieniu wymagań określonych

w rozporządzeniu wydanym na podstawie art. 20a ust. 3 pkt 1 ustawy. Mając na uwadze zmiany wprowadzone w tym rozporządzeniu wskazano, że wystarczające będzie przedłożenie ministrowi oświadczenia o spełnieniu wymagań w zakresie opracowywania i ustanawiania, wdrażania i eksploataowania monitorowania i przeglądania oraz utrzymywania i doskonalenia systemu zarządzania bezpieczeństwem informacji spełniającego wymagania, o których mowa w przepisach wydanych na podstawie art. 18 ustawy.

10. W § 18 ust. 3 dodano wyjątek wskazujący, że nagranie audiowizualne z procesu zdalnej weryfikacji tożsamości, o którym mowa w § 6, przechowuje się krócej niż pozostałą dokumentację z procesu potwierdzenia profilu zaufanego, to znaczy przez 6 lat, zgodnie z wymogiem art. 20ca ust. 7 ustawy.

11. W § 20 ust. 1 pkt 4 lit. a zniesiono ograniczenie wymagające od środków identyfikacji elektronicznej nadających się do zdalnego potwierdzenia profilu zaufanego aby weryfikacja tożsamości osoby, której taki środek jest wydawany, wymagała okazania dokumentu tożsamości tej osoby podczas jej fizycznej obecności. Dopuszcza się też okazanie dokumentu tożsamości lub w trakcie nagrywanej w czasie rzeczywistym transmisji audiowizualnej pod warunkiem zachowania należytej staranności w ustaleniu autentyczności dokumentu tożsamości oraz w działaniach zmierzających do zminimalizowania ryzyka, że tożsamość deklarowana przy użyciu okazanego dokumentu tożsamości jest niezgodna z faktyczną tożsamością osoby okazującej ten dokument. Celem jest możliwość wykorzystania rozwiązań stosowanych już w praktyce przez banki krajowe⁵, które mają już wdrożone rozwiązania umożliwiające bezpieczne zdalne potwierdzanie tożsamości w celu wydania środka identyfikacji elektronicznej w swoim teleinformatycznym. Przyczyni się to także do zmniejszenia obciążenia usługi zdalnego potwierdzania tymczasowego profilu zaufanego świadczonej przez ministra i zwiększy dostęp do profilu zaufanego dla osób, które nie powinny lub nawet nie mogą wychodzić z domu.

Jednocześnie jednak nakłada się obowiązek przechowania nagrania transmisji audiowizualnej, przez okres 6 lat (§ 20 ust. 2).

⁵https://www.knf.gov.pl/knf/pl/komponenty/img/Stanowisko_UKNF_dot_identyfikacji_klienta_i_weryfikacji_jego_tozsamosci_w_bankach_oraz_oddzialach_instytucji_kredytowych_w_oparciu_o_metode_wideoweryfikacji_66066.pdf

12. Mając na uwadze znaczenie możliwości zdalnego potwierdzania profilu zaufanego z wykorzystaniem wideoweryfikacji w związku z panującą epidemią i co za tym idzie ogromne zainteresowanie tą usługą, kluczową kwestią staje się jej dostępność. Zapewnienie obywatelom wnoszącym tymczasowy profil zaufany możliwości jego niezwłocznego uzyskania wymaga rozwiązań organizacyjnych jednocześnie wysokodostępnych i bezpiecznych.

W tym celu wprowadzono rozwiązanie wskazane w § 24. Uwzględniając doświadczenie punktów potwierdzających zobowiązanych do potwierdzania profilu zaufanego wprost na podstawie art. 20c ust. 2 pkt 1-4 ustawy (punkty te potwierdzają profil zaufany od 10 lat) możliwość dołączenia ich do potwierdzania tymczasowego profilu zaufanego wychodzi naprzeciw obu tym potrzebom – to jest wysokiej dostępności i bezpieczeństwa. Podobne argumenty przemawiają za możliwością dołączenia jednostek podległych do grona podmiotów, które będą mogły obsługiwać usługę online służącą do potwierdzania tymczasowego profilu zaufanego. Zarządzanie usługą i uprawnieniami oczywiście pozostanie wyłącznie w gestii Ministra Cyfryzacji tak, aby możliwość potwierdzania profilu zaufanego na odległość posiadało tylko tyle osób, ile jest to niezbędne dla zapewnienia niezwłocznej obsługi wniosków.

13. Dodano nowy załącznik (nr 2) wskazujący zakres danych jaki znajdzie się we wniosku o potwierdzenie tymczasowego profilu zaufanego. Mając na uwadze, że wniosek będzie składany bez podpisu (odpowiednie oświadczenie woli będzie zawierało nagranie audiowizualne) należało odpowiednio dostosować zakres danych jaki się w nim będzie znajdował.

Projektowana regulacja nie będzie wymagała notyfikacji Komisji Europejskiej w trybie ustawy z dnia 30 kwietnia 2004 r. o postępowaniu w sprawach dotyczących pomocy publicznej (Dz. U. z 2018 r. poz. 362 oraz z 2019 r. poz. 730 i 1063).

Projektowane rozporządzenie nie będzie miało wpływu na działalność mikroprzedsiębiorców, małych i średnich przedsiębiorców.

Projekt rozporządzenia nie jest sprzeczny z prawem Unii Europejskiej.

Projektowane rozporządzenie nie wymaga przedstawienia instytucjom i organom Unii Europejskiej lub Europejskiemu Bankowi Centralnemu w celu uzyskania opinii, dokonania powiadomienia, konsultacji albo uzgodnienia.

Projektowane rozporządzenie zostało zamieszczone w Biuletynie Informacji Publicznej Ministra Cyfryzacji oraz w Biuletynie Informacji Publicznej Rządowego Centrum Legislacji, zgodnie z art. 5 ustawy z dnia 7 lipca 2005 r. o działalności lobbingowej w procesie stanowienia prawa (Dz. U. z 2017 r. poz. 248).

<p>Nazwa projektu Projekt rozporządzenia Ministra Cyfryzacji w sprawie profilu zaufanego i podpisu zaufanego</p> <p>Ministerstwo wiodące i ministerstwa współpracujące Ministerstwo Cyfryzacji</p> <p>Osoba odpowiedzialna za projekt w randze Ministra, Sekretarza Stanu lub Podsekretarza Stanu Minister Cyfryzacji Marek Zagórski</p> <p>Kontakt do opiekuna merytorycznego projektu Kazimierz Schmidt, Radca ministra w Departamencie Zarządzania Systemami: kazimierz.schmidt@mc.gov.pl, tel. 225568403</p>	<p>Data sporządzenia 20 maja 2020 r.</p> <p>Źródło: Upoważnienie ustawowe – art. 20d ustawy z dnia 17 lutego 2005 r. o informatyzacji działalności podmiotów realizujących zadania publiczne (Dz.U. z 2020 r. poz. 346, 568 i 695)</p>
---	--

OCENA SKUTKÓW REGULACJI

1. Jaki problem jest rozwiązywany?

Konieczność wydania aktu wykonawczego wynika z faktu, iż na mocy art. 33 ustawy z dnia 31 marca 2020 r. o zmianie ustawy o szczególnych rozwiązaniach związanych z zapobieganiem, przeciwdziałaniem i zwalczaniem COVID-19, innych chorób zakaźnych oraz wywołanych nimi sytuacji kryzysowych oraz niektórych innych ustaw (Dz. U. poz. 568), wprowadzone zostały do ustawy z dnia 17 lutego 2005 r. o informatyzacji działalności podmiotów realizujących zadania publiczne (Dz. U. z 2020 r. poz. 346, 568 i 695) zmiany dotyczące sposobu potwierdzania profilu zaufanego. W szczególności w nowym art. 20ca ustawy o informatyzacji umożliwiono zdalne potwierdzanie tożsamości osoby fizycznej polegające na tym, że dokument tożsamości (dowód osobisty lub paszport) osoby, która złożyła wniosek o potwierdzanie profilu zaufanego o krótszym okresie ważności (tymczasowego profilu zaufanego), może być okazany w trakcie nagrywanej transmisji audiowizualnej.

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

Wydanie nowego rozporządzenia.

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

Brak danych.

4. Podmioty, na które oddziałuje projekt

Grupa	Wielkość	Źródło danych	Oddziaływanie
Ministerstwo Cyfryzacji	1		Przygotowanie usługi zdalnej weryfikacji tożsamości w systemie, w którym potwierdzany jest profil zaufany. Powiązanie z rejestrami publicznymi,

			zapewnienie możliwości nagrywania wyszkolenie osób potwierdzających.
Podmioty niepubliczne mające możliwość udostępnienia swoim klientom potwierdzania profilu zaufanego w systemie w którym wydają środki identyfikacji elektronicznej	10	Strona rejestracji profilu zaufanego: https://pz.gov.pl/dt/registerByXidp	Analiza pewności świadczonych usług zdalnego potwierdzania tożsamości z wymogami rozporządzenia i ewentualne wykorzystanie możliwości potwierdzania profilu zaufanego dla klientów którzy założyli konto zdalnie.

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

Projektowane rozporządzenie zostało zamieszczone w Biuletynie Informacji Publicznej Ministra Cyfryzacji oraz w Biuletynie Informacji Publicznej Rządowego Centrum Legislacji, zgodnie z art. 5 ustawy z dnia 7 lipca 2005 r. o działalności lobbingsowej w procesie stanowienia prawa (Dz. U. z 2017 r. poz. 248).

Ponadto projekt został przekazany następującym podmiotom:

I. w ramach opiniowania:

1. Prezes Urzędu Ochrony Danych Osobowych
2. Prezes Urzędu Zamówień Publicznych
3. Prezes Zakładu Ubezpieczeń Społecznych
4. Prezes Kasy Rolniczego Ubezpieczenia Społecznego

II. w ramach konsultacji publicznych:

1. Polski Komitet Normalizacyjny (PKN)
2. Polskie Towarzystwo Informatyczne (PTI)
3. Polska Izba Informatyki i Telekomunikacji (PIIT)
4. Krajowa Izba Gospodarcza Elektroniki i Telekomunikacji (KIGeIT)
5. Stowarzyszenie Instytutu Informatyki Śledczej
6. Fundacja Panoptykon
7. Polska Izba Komunikacji Elektronicznej
8. Internet Society Poland
9. Rada Główna Instytutów Badawczych (RGIB)
10. Instytut Logistyki i Magazynowania (ILiM)
11. Poczta Polska S. A.

(oddzielnie)												
Wydatki ogółem	0,8	0	0	0	0	0	0	0	0	0	0	0,8
budżet państwa	0	0	0	0	0	0	0	0	0	0	0	0
JST	0	0	0	0	0	0	0	0	0	0	0	0
pozostałe jednostki (oddzielnie)	0	0	0	0	0	0	0	0	0	0	0	0
Saldo ogółem	- 0,8	0	0	0	0	0	0	0	0	0	0	-0,8
budżet państwa	0	0	0	0	0	0	0	0	0	0	0	0
JST	0	0	0	0	0	0	0	0	0	0	0	0
pozostałe jednostki (oddzielnie)	0	0	0	0	0	0	0	0	0	0	0	0
Źródła finansowania	Budżet państwa, cz. 27 Informatyzacja											
Dodatkowe informacje, w tym wskazanie źródeł danych i przyjętych do obliczeń założeń												
7. Wpływ na konkurencyjność gospodarki i przedsiębiorczość, w tym funkcjonowanie przedsiębiorców oraz na rodzinę, obywateli i gospodarstwa domowe												
Skutki												
Czas w latach od wejścia w życie zmian			0	1	2	3	5	10	<i>Łącznie (0-10)</i>			
W ujęciu pieniężnym (w mln zł, ceny stałe z r.)	duże przedsiębiorstwa		0	0	0	0	0	0	0	0		
	sektor mikro-, małych i średnich przedsiębiorstw		0	0	0	0	0	0	0	0		
	rodzina, obywatele oraz gospodarstwa domowe		0	0	0	0	0	0	0	0		
	(dodaj/usuń)		0	0	0	0	0	0	0	0		
W ujęciu niepieniężnym	duże przedsiębiorstwa		-									
	sektor mikro-, małych i średnich przedsiębiorstw		-									
	rodzina, obywatele oraz gospodarstwa domowe		-									
	(dodaj/usuń)											

Niemierzalne	(dodaj/usuń)	
	(dodaj/usuń)	
Dodatkowe informacje, w tym wskazanie źródeł danych i przyjętych do obliczeń założeń	Wejście w życie projektowanego rozporządzenia nie będzie miało wpływu na konkurencyjność gospodarki i przedsiębiorczość, w tym funkcjonowanie przedsiębiorców oraz na sytuację ekonomiczną i społeczną rodziny, a także osób niepełnosprawnych oraz osób starszych.	
8. Zmiana obciążeń regulacyjnych (w tym obowiązków informacyjnych) wynikających z projektu		
<input checked="" type="checkbox"/> nie dotyczy		
Wprowadzane są obciążenia poza bezwzględnie wymaganymi przez UE (szczegółowo w odwrotnej tabeli zgodności).	<input type="checkbox"/> tak <input type="checkbox"/> nie <input checked="" type="checkbox"/> nie dotyczy	
<input type="checkbox"/> zmniejszenie liczby dokumentów <input type="checkbox"/> zmniejszenie liczby procedur <input type="checkbox"/> skrócenie czasu na załatwienie sprawy <input type="checkbox"/> inne:	<input type="checkbox"/> zwiększenie liczby dokumentów <input type="checkbox"/> zwiększenie liczby procedur <input type="checkbox"/> wydłużenie czasu na załatwienie sprawy <input type="checkbox"/> inne:	
Wprowadzane obciążenia są przystosowane do ich elektroniczności.	<input type="checkbox"/> tak <input type="checkbox"/> nie <input checked="" type="checkbox"/> nie dotyczy	
Komentarz:		
9. Wpływ na rynek pracy		
Projektowane rozporządzenie nie będzie miało wpływu na rynek pracy.		
10. Wpływ na pozostałe obszary		
<input type="checkbox"/> środowisko naturalne <input type="checkbox"/> sytuacja i rozwój regionalny <input type="checkbox"/> inne:	<input type="checkbox"/> demografia <input type="checkbox"/> mienie państwowe	<input checked="" type="checkbox"/> informatyzacja <input type="checkbox"/> zdrowie
Omówienie wpływu	Zmiany wymogów dotyczących systemów teleinformatycznych przy pomocy których podmioty publiczne dokonują weryfikacji tożsamości użytkowników systemów teleinformatycznych wykorzystywanych przez te podmioty do realizacji zadań publicznych.	
11. Planowane wykonanie przepisów aktu prawnego		
Nie dotyczy.		
12. W jaki sposób i kiedy nastąpi ewaluacja efektów projektu oraz jakie mierniki zostaną zastosowane?		
Nie dotyczy.		
13. Załączniki (istotne dokumenty źródłowe, badania, analizy itp.)		
Brak		