Projekt z dnia 12 lipca 2018 r.

R O Z P O R Z Ą D Z E N I E

M I N I S T R A C Y F R Y Z A C J I [1)]

z dnia ……..….. 2018 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 2017 r. poz. 570 oraz z 2018 r. poz. 1000 i ….) 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 potwierdzania, 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 20 kwietnia 2018 r. w sprawie szczegółowego zakresu działania Ministra Cyfryzacji (Dz. U. poz. 761).

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 w okresie dłuższym niż 3 lata;
6) osoba wnioskująca - osobę fizyczna występującą z wnioskiem o potwierdzenie profilu zaufanego;
7) ustawa - ustawę z dnia 17 lutego 2005 r. informatyzacji działalności podmiotów realizujących zadania publiczne (Dz. U. z 2017 r. poz. 570 oraz z 2018 r. poz. 1000 i ….);
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 w sprawie identyfikacji elektronicznej i usług zaufania w odniesieniu do transakcji elektronicznych na rynku wewnętrznym oraz uchylające dyrektywę 1999/93/WE (Dz. U. L 257 z 28.8.2014, s. 73–114).

§ 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. Wniosek o potwierdzenie profilu zaufanego może stanowić element składowy formularza elektronicznego umożliwiającego założenie konta w ePUAP, o którym mowa w przepisach wydanych na podstawie art. 19a ust. 3 ustawy.

2. Jeżeli w okresie 14 dni od daty złożenia wniosku, o którym mowa w ust. 1, osoba wnioskująca nie zgłosi się do punktu potwierdzającego w celu potwierdzenia profilu zaufanego, wniosek ten uważa się za bezskuteczny.

§ 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 czas dokonania potwierdzenia.

5. W przypadku stwierdzania tożsamości osoby wnioskującej na podstawie dokumentu tożsamości niezawierającego numeru PESEL, o którym mowa w art. 20c ust. 1 pkt 1 lit. b ustawy, osoba upoważniona do potwierdzenia profilu zaufanego dodatkowo odnotowuje na wydruku wniosku kraj wydania oraz rodzaj i numer okazanego dokumentu tożsamości.

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

1) podpisem zaufanym albo
2) kwalifikowanym podpisem elektronicznym.

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

1) opatrując utworzony profil zaufany 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.

2. Profil zaufany potwierdzony w sposób, o którym mowa w ust. 1 pkt 2, opatruje się pieczęcią elektroniczną ministra właściwego do spraw informatyzacji.

3. W przypadku samodzielnego potwierdzenia profilu zaufanego:

1) dane identyfikujące osobę fizyczną, o których mowa w art. 20ad ust. 1 ustawy, ustalane 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 § 8 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.

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

§ 7. 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.

§ 8. 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. 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. Uwierzytelnienie przy użyciu profilu zaufanego może następować:

1) z wykorzystaniem czynników uwierzytelniania, spełniających warunki określone w ust. 3, 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 czynnika uwierzytelniania, o którym mowa w ust. 3 pkt 1, 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.

6. 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. 3 pkt 2, z uwzględnieniem czynników

uwierzytelniania, o których mowa w ust. 4 pkt 1, spełniających warunki określone w ust. 3 pkt 2.

7. 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 ust. 5, albo w punkcie potwierdzającym profil zaufany;
2) środka identyfikacji elektronicznej lub czynników uwierzytelniania, o których mowa w ust. 4 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.

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

9. Struktura danych profilu zaufanego oraz podpisu zaufanego udostępniane są w przez ministra właściwego do spraw informatyzacji, zwanego dalej „ministrem”, na stronie podmiotowej Biuletynu Informacji Publicznej.

§ 9. 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 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 2 do rozporządzenia.

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

1) przedłożenia nieważnego dokumentu, o którym mowa w § 4 ust. 2, 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.

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

§ 11. 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 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 3 do rozporządzenia.

§ 12. 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, w szczególności:
   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, w szczególności:
   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 § 8 ust. 3.

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.

§ 13. 1. Złożenie podpisu zaufanego jest możliwe w okresie ważności profilu zaufanego.

2. Czynność złożenia podpisu zaufanego wymaga autoryzacji, o której mowa w § 8 ust. 5, po której następuje opatrzenie podpisywanych danych w postaci elektronicznej pieczęcią elektroniczną ministra wykorzystywaną do zapewnienia integralności podpisanych danych oraz autentyczności złożonego podpisu.

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 w drodze komunikatu udostępnianego w interfejsie użytkownika oprogramowania umożliwiającego złożenie takiego podpisu, że dokonuje czynności złożenia podpisu zaufanego.

§ 14. 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, określonych w § 3 ust. 2 i 3 rozporządzenia Ministra Cyfryzacji z dnia 5 października 2016 r. w sprawie szczegółowych warunków organizacyjnych i technicznych, które powinien spełniać system teleinformatyczny służący do uwierzytelniania użytkowników (Dz. U. poz. 1627), w zakresie w jakim dotyczyć to będzie uprawnień i czynności osób upoważnionych do potwierdzania profili zaufanych.

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 2-4 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 2016 r. poz. 1506), 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.

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

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.

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.

§ 16. Unieważnienie profilu zaufanego może być dokonane w systemie teleinformatycznym podmiotu niepublicznego, przy użyciu środka identyfikacji elektronicznej, o którym mowa w art. 20c ust. 8 ustawy.

§ 17. 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 zaufania, wymaganych rozporządzeniem wykonawczym Komisji (UE) 2015/1502 z dnia 8 września 2015 r. w sprawie ustanowienia minimalnych specyfikacji technicznych i procedur dotyczących poziomów zaufania w zakresie środków identyfikacji elektronicznej 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), zwanym dalej „rozporządzeniem wykonawczym 2015/1502”;
2) opracowania i ustanawiania, wdrażania i eksploatowania, monitorowania i przeglądania oraz 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 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 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 2015 r. poz. 128, z późn. zm.), 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.

§ 18. Podmiot niepubliczny przedstawia dokumenty, o których mowa w § 17 ust. 2 i 3, na żądanie ministra.

§ 19. 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.

§ 20. 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 14 dni, o zamiarze ich usunięcia.

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

4. W przypadku braku reakcji użytkownika konta profilu zaufanego w ciągu 14 dni od przesłania drugiego powiadomienia, o którym mowa w ust. 2, nieużywane konto jest usuwane.

§ 21. Wnioski o potwierdzenie, przedłużenie ważności i unieważnienie profilu zaufanego ePUAP złożone przed dniem wejścia w życie rozporządzenia, są rozpatrywane na zasadach dotychczasowych.

§ 22. Wnioski, o których mowa w art. 20c ust. 4 ustawy, złożone przed dniem wejścia w życie rozporządzenia, są rozpatrywane zgodnie z dotychczasowymi przepisami.

§ 23. Rozporządzenie wchodzi w życie z dniem następującym po dniu ogłoszenia.

Za zgodność pod względem prawnym, legislacyjnym i redakcyjnym
Magdalena Witkowska-Krzymowska
Zastępca Dyrektora Departamentu Prawnego
/podpisano elektronicznie/

UZASADNIENIE

Projektowane rozporządzenie stanowi wykonanie upoważnienia ustawowego określonego w art. 20d ustawy z dnia 17 lutego 2005 r. o informatyzacji działalności podmiotów realizujących zadania publiczne (Dz. U. z 2017 r. poz. 570 oraz z 2018 r. poz. 1000 i …).

Konieczność przygotowania przedmiotowego rozporządzenia wynika z faktu, iż w drodze ustawy z dnia 5 lipca 2018 r. o zmianie ustawy o usługach zaufania oraz identyfikacji elektronicznej oraz niektórych innych ustaw (Dz. U. z 2018 r. ...) uchylony został art. 20a ust. 2 pkt 2 ustawy o informatyzacji działalności podmiotów realizujących zadania publiczne, stanowiący dotychczas podstawę prawną do wydania rozporządzenia Ministra Cyfryzacji z dnia 5 października 2016 r. w sprawie profilu zaufanego elektronicznej platformy usług administracji publicznej (Dz. U. z 2016 r. poz. 1633). Jednocześnie do przedmiotowej ustawy dodany został art. 20d upoważniający ministra właściwego do spraw informatyzacji do określenia w drodze rozporządzenia warunków wydawania, przedłużania ważności, wykorzystywania i unieważniania profilu zaufanego oraz składania podpisu zaufanego.

Projektowane rozporządzenie, w stosunku do poprzedniego rozporządzenia Ministra Cyfryzacji z dnia 5 października 2016 r. w sprawie profilu zaufanego elektronicznej platformy usług administracji publicznej, uwzględnia zmiany wprowadzone w ustawie o informatyzacji działalności podmiotów realizujących zadania publiczne, w szczególności formalne oddzielenie od platformy ePUAP systemu teleinformatycznego, który służył do obsługi „profilu zaufanego ePUAP". W konsekwencji powyższego dokonano zmiany nazwy wspomnianego wyżej środka identyfikacji elektronicznej na „profil zaufany". Jednocześnie pojęcie „podpis potwierdzony profilem zaufanym ePUAP" uległo zmianie na „podpis zaufany".

Profil zaufany będzie możliwy do uzyskania na dwa sposoby. Pierwszy sposób wymaga udania się do jednego z punktów potwierdzających, które zostały określone w ustawie o informatyzacji działalności podmiotów realizujących zadania publiczne. Drugim sposobem uzyskania profilu zaufanego jest procedura pozwalająca wnioskodawcy na samodzielne potwierdzenie profilu zaufanego w publicznym systemie teleinformatycznym, po uprzednim potwierdzeniu swojej tożsamości.

W § 3 i § 4 zawarto regulacje dotyczące czynności jakie zainteresowany musi podjąć celem uzyskania przedmiotowego środka identyfikacji elektronicznej w punkcie potwierdzającym oraz czynności jakie podejmowane są w ramach tej procedury przez pracowników punktu potwierdzającego. Wskazuje się tu w szczególności na konieczność złożenia wniosku przy

użyciu formularza elektronicznego udostępnionego systemie teleinformatycznym, w którym wydawany jest profil zaufany. Celem ułatwienia dla obywateli wprowadza się taką możliwość aby formularz elektroniczny wniosku o potwierdzenie profilu zaufanego mógł także stanowić integralną część formularza elektronicznego umożliwiającego założenia konta na ePUAP. Kolejnym krokiem, po wniesieniu wniosku w postaci elektronicznej, jest udanie się do wybranego przez siebie punktu potwierdzającego celem potwierdzenia swojej tożsamości. Czynność ta jest kluczowa dla procesu wydania profilu zaufanego, bowiem pozwala na przyporządkowanie tego środka identyfikacji elektronicznej do konkretnej osoby fizycznej o ustalonej i potwierdzonej tożsamości. Weryfikacji tożsamości wnioskodawcy dokonuje pracownik punktu potwierdzającego, który fakt przeprowadzonych w tym zakresie czynności odnotowuje na wydruku wniosku uwzględniając przy tym czas dokonania potwierdzenia. Powyższa procedura finalizowana wygenerowaniem nowego profilu zaufanego, który podpisywany jest przez upoważnionego do potwierdzenia profili zaufanych pracownika punktu potwierdzającego posiadanym przez niego podpisem zaufanym albo kwalifikowanym podpisem elektronicznym.

Przepis § 5 regulował będzie metody samodzielnego uzyskania profilu zaufanego w systemie teleinformatycznym w którym wydawany jest profil zaufany. W procedurze tej, podobnie jak wyżej, konieczne jest potwierdzenie tożsamości osoby której wydany zostanie przedmiotowy środek identyfikacji elektronicznej. Zainteresowany może potwierdzić swoją tożsamość w systemie teleinformatycznym na dwa sposoby. Pierwszym sposobem jest opatrzenie utworzonego profilu zaufanego kwalifikowanym podpisem elektronicznym, w tym przypadku jednocześnie zapewniana jest integralność przedmiotowego środka identyfikacji elektronicznej. Drugim sposobem jest zidentyfikowanie się i autoryzowanie czynności utworzenia i potwierdzenia profilu zaufanego przy użyciu posiadanego środka identyfikacji elektronicznej. Powyższe odnosi się wyłącznie do środków identyfikacji elektronicznej których użycie w takiej procedurze zostało zapewnione za zgodą ministra właściwego do spraw informatyzacji, wydaną na podstawie art. 20c ust. 8 ustawy o informatyzacji działalności podmiotów realizujących zadania publiczne. W przypadku skorzystania z wyżej wspominanego środka identyfikacji elektronicznej integralność nowego profilu zaufanego zapewniana będzie poprzez jego opatrzenie pieczęcią elektroniczną ministra właściwego do spraw informatyzacji. W ust. 3 wskazano ponadto metodę ustalania danych zamieszczanych w wydawanym profilu zaufanym.

W § 6 zawarto odniesienie do załącznika nr 1, w którym określony będzie zakres danych oraz oświadczenia wymagane we wniosku o potwierdzenie profilu zaufanego. Wspomniane wyżej dane i oświadczenia będą musiały być przekazane przez wnioskodawcę toku każdej procedury

prowadzącej do potwierdzenia profilu zaufanego.

W § 7 wskazano wymogi bezpiecznego, przede wszystkim dla posiadacza, użytkowania profilu zaufanego.

Przepis § 8 regulował będzie kluczowe kwestie dotyczące profilu zaufanego. Określa się tu zakres danych gromadzonych w przedmiotowym środku identyfikacji elektronicznej oraz w reguluje się zakaz ponownego nadania uprzednio już przydzielonego identyfikatora użytkownika. Mając zaś na uwadze planowaną notyfikację profilu zaufanego Komisji Europejskiej, celem umożliwienia uwierzytelnienia jego posiadaczy w publicznych usługach online w całej UE, wprowadza się przepisy dostosowujące profil zaufany do tych potrzeb. I tak w § 8 ust. 3 pkt 2 i 3 wprowadza się regulacje stanowiące odpowiedź na potrzebę odróżniania profili zaufanych potwierdzonych w sposób inny niż w punkcie potwierdzającym. Powyższe pozwoli, w przypadku naruszenia bezpieczeństwa systemu teleinformatycznego w którym wydawany będzie profil zaufany, na zawieszenie lub wyłączenie procedury uwierzytelniania tylko w zakresie obsługi części profili zaufanych, które potwierdzone zostały w określony sposób. Wykluczy to jednocześnie konieczność wyłączenia całego systemu teleinformatycznego w którym wydawany jest profil zaufany, o czym mowa jest w art. 10 rozporządzenia Parlamentu Europejskiego i Rady (UE) nr 910/2014 w sprawie identyfikacji elektronicznej i usług zaufania w odniesieniu do transakcji elektronicznych na rynku wewnętrznym oraz uchylające dyrektywę 1999/93/WE (Dz. U. L 257 z 28.8.2014, s. 73–114), zwanego dalej „rozporządzeniem 910/2014”.

Ważnym jest ust. 4, który stanowił będzie, że „profil zaufany” jest środkiem identyfikacji elektronicznej zapewniającym średni poziom bezpieczeństwa, a uwierzytelnienie przy jego użyciu będzie, odpowiednio do wymogów dla takiego poziomu bezpieczeństwa, dokonywane będzie każdorazowo przy wykorzystaniu co najmniej dwóch czynników uwierzytelnienia, należących do co najmniej dwóch różnych kategorii. Ustala się tu jednocześnie jakiego rodzaju mogą być wspomniane wyżej czynniki uwierzytelniania. W ust. 5 pkt 1 dopuszcza się stosowanie w procesie uwierzytelnienia przy użyciu profilu zaufanego czynnika uwierzytelniania stanowiącego element środka identyfikacji elektronicznej, stosowanego do uwierzytelniania w systemie teleinformatycznym podmiotu niepublicznego, o którym mowa w art. 20d ust. 8 ustawy. Mając na uwadze, że mogą istnieć publiczne usługi online wymagające uwierzytelnienia użytkownika na niskim poziomie bezpieczeństwa, dopuszcza się możliwość dokonania uwierzytelnienia w takim przypadku przy wykorzystaniu jednego czynnika uwierzytelniania profilu zaufanego, określonego w ust. 4 pkt 1. Ust. 5 stanowił będzie, że autoryzacje, w rozumieniu art. 3 pkt 27 ustawy o informatyzacji działalności podmiotów realizujących

zadania publiczne, mogą być dokonywane przy użyciu drugiego czynnika uwierzytelnienia, o którym mowa w ust. 4 pkt 2, z zastrzeżeniem, że użytkownik został uprzednio uwierzytelniony przy użyciu profilu zaufanego, a więc przy wykorzystaniu dwóch czynników uwierzytelniania wykorzystywanych w ramach tego środka identyfikacji elektronicznej. Kolejne ustępy regulują odpowiednio metody przy użyciu których posiadacz może dokonywać zmian w danych profilu zaufanego, sposób przekazywania posiadaczowi komunikatów dotyczących profilu zaufanego, oraz miejsce publikacji struktury danych profilu zaufanego.

Profil zaufany będzie mógł być potwierdzony na okres 3 lat. Istotnym jest, że jego ważność będzie mogła być przedłużona samodzielnie przez jego posiadacza na taki sam okres. Powyższe regulował będzie § 9, w którym ustala się, że taka czynność będzie mogła być dokonana systemie teleinformatycznym, w takim przypadku będzie dokonywana przy wykorzystaniu profilu zaufanego albo kwalifikowanego podpisu elektronicznego, oraz w punkcie potwierdzającym. Wymaganym będzie aby historia kolejnych przedłużeń gromadzona była w systemie teleinformatycznym w którym wydawany jest profil zaufany. W ust. 4 zawarto odniesienie do załącznika nr 2, w którym określony będzie zakres danych oraz oświadczenia wymagane we wniosku o przedłużenie ważności profilu zaufanego. Wspomniane wyżej dane i oświadczenia będą musiały być przekazane przez wnioskodawcę w procedurach przedłużenia profilu zaufanego, o których mowa w ust. 2 pkt 1 i 2.

W § 10 określa się przypadki wykluczające możliwość potwierdzenia profilu zaufanego. Przypadki te dotyczą kluczowego problemu dla procedury wydawania środka identyfikacji elektronicznej, czyli niemożności skutecznego potwierdzenia tożsamości osoby ubiegającej się o profil zaufany. Wprowadza się jednocześnie obowiązek odnotowania i zachowania czasu i przyczyny niedokonania potwierdzenia przez osobę upoważnioną do potwierdzenia profilu zaufanego w punkcie potwierdzającym.

W § 11 i § 12 reguluje się sytuacje w których profil zaufany traci ważność. Przepis § 11 odnosi się do przypadków unieważnienia stanowiących wynik działania posiadacza profilu zaufanego, jest tu więc mowa o takich czynnościach jak: usunięcie konta profilu zaufanego, dokonanie zmian w określonych danych profilu zaufanego, unieważnienie tego środka identyfikacji elektronicznej w systemie w którym wydawany jest profil zaufany albo na wniosek złożony w punkcie potwierdzającym. W § 16 dopuszcza się ponadto możliwość unieważnienia profilu zaufanego w systemie teleinformatycznym podmiotu niepublicznego, przy użyciu środka identyfikacji elektronicznej, o którym mowa w art. 20c ust. 8 ustawy o informatyzacji działalności podmiotów realizujących zadania publiczne.

Przepis § 12 regulował będzie przypadki, w których minister właściwy do spraw informatyzacji będzie mógł unieważnić profil zaufany działając niezależnie od woli jego posiadacza. Wymienione są tu zdarzenia w rezultacie których profil zaufany stanowiłby zagrożenie dla bezpieczeństwa lub prawidłowego działania systemu teleinformatycznego w którym jest on wydawany, oraz zdarzenia czyniące profil zaufany niegodnym ze stawianymi mu wymogami jako środkowi identyfikacji elektronicznej zapewniającemu średni poziom bezpieczeństwa. Uprawnia się jednocześnie ministra do podejmowania działań mających na celu ustalenie czy faktycznie występują w systemie podejrzewane przez niego nieprawidłowości, w tym także takich działań, które dopuszczają oczekiwanie określonych reakcji ze strony posiadaczy profilu zaufanego. Powyższe pozwolić ma na przykład na ustalenie czy profil zaufany nadal pozostaje pod pełną kontrolą jego posiadacza.

W § 13 reguluje się warunki użytkowania podpisu zaufanego. Podpis zaufany będzie mógł być złożony przy wykorzystaniu profilu zaufanego w okresie ważności tego środka identyfikacji elektronicznej. Złożenie podpisu zaufanego na dokumencie elektronicznym będzie wymagało autoryzacji tej czynności przy użyciu profilu zaufanego. System teleinformatyczny, przy użyciu którego składany będzie przedmiotowy podpis elektroniczny, przed każdym złożeniem tego podpisu, będzie informował posiadacza profilu zaufanego, że dokonuje on czynności podpisu elektronicznego. Integralność podpisanych w ten sposób danych elektronicznych oraz autentyczności złożonego podpisu elektronicznego będzie zapewniana przy użyciu pieczęci elektronicznej ministra właściwego do spraw informatyzacji. Wspomniane wyżej cechy podpisanego dokumentu będą weryfikowane za pomocą certyfikatu wspomnianej wyżej pieczęci.

W § 14 i § 15 reguluje się wymogi jakie zobowiązane są spełniać podmioty, określone w ustawie o informatyzacji działalności podmiotów realizujących zadania publiczne, aby mogły rozpocząć pełnienie funkcji punktu potwierdzającego profil zaufany, a także w trakcie pełnienia tej funkcji. Przepisy te odnoszą się do kwestii bezpieczeństwa związanych z działaniem punktu potwierdzającego profil zaufany jak również do wymogów postępowania z dokumentacją powstającą w toku procedur związanych z obsługą procesów związanych z profilem zaufanym.

Przepisy § 17 i § 18 określały będą wymogi jaki muszą spełniać podmioty niepubliczne, wydające wspomniane już wyżej środki identyfikacji elektronicznej, które za zgodą ministra właściwego do spraw informatyzacji wykorzystywane będą do potwierdzenia profilu zaufanego, oraz dokonywania autoryzacji przy użyciu tego środka identyfikacji elektronicznej. Wymogi te nawiązują do przepisów dotyczących poziomów bezpieczeństwa środków identyfikacji elektronicznej zawartych w rozporządzeniu 910/2014 oraz w rozporządzeniu wykonawczym

Komisji (UE) 2015/1502 z dnia 8 września 2015 r. w sprawie ustanowienia minimalnych specyfikacji technicznych i procedur dotyczących poziomów zaufania w zakresie środków identyfikacji elektronicznej 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.

W §19 zastrzega się, że system, w którym wydawany jest profil zaufany, nie może pozwolić użytkownikowi na usunięcie konta profilu zaufanego w przypadku gdy taka czynność prowadziłaby do utraty kontroli użytkownika tego konta nad kontem w ePUAP. Może bowiem na przykład zaistnieć sytuacja, że z takim usuwanym kontem będzie powiązany profil zaufany, który został przez użytkownika wskazany jako metoda jego uwierzytelnienia w systemie ePUAP, Usunięcie więc konta profilu zaufanego powodowałoby utratę „profilu zaufanego", a tym samym także utratę możliwości dostępu do konta w ePUAP.

Posługiwanie się profilem zaufanym wiąże się z koniecznością posiadania konta w systemie teleinformatycznym w którym wydawany jest ten środek identyfikacji elektronicznej. Część z tych kont obecnie, z różnych względów, nie jest używana i zbytecznie zajmuje zasoby systemu teleinformatycznego w którym wydawany jest profil zaufany. W związku z powyższym w § 20 wprowadza się przepisy, które pozwolą ministrowi właściwemu do spraw informatyzacji na wyszukanie i usunięcie takich nieaktywnych kont. Przyjmuje się jednakże, że przed usunięciem tych kont wymagane będzie powiadomienie ich posiadaczy o takim zamiarze, celem umożliwienia im ewentualnego potwierdzenia woli dalszego korzystania z tych kont.

Rozporządzenie wchodzi w życie z dniem następującym po dniu ogłoszenia. Skrócenie terminu wejścia w życie niniejszego rozporządzenia podyktowane jest zaawansowanym etapem prac nad ustawą o zmianie ustawy o usługach zaufania oraz identyfikacji elektronicznej oraz niektórych innych ustaw, wprowadzającą zmiany prawne istotne dla materii regulowanej w tym rozporządzeniu. Stąd też konieczne jest skorelowanie terminów wejścia w życie obu aktów prawnych.

Projekt rozporządzenia nie jest sprzeczny z prawem Unii Europejskiej.

Projektowana regulacja nie zawiera przepisów technicznych w rozumieniu rozporządzenia Rady Ministrów z dnia 23 grudnia 2002 r. w sprawie sposobu funkcjonowania krajowego systemu notyfikacji norm i aktów prawnych (Dz. U. poz. 2039 oraz z 2004 r. poz. 597).

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).

Projekt rozporządzenia nie wymaga przedłożenia instytucjom i organom Unii Europejskiej, w tym Europejskiemu Bankowi Centralnemu w celu uzyskania opinii, dokonania powiadomienia, konsultacji albo uzgodnienia.

Projekt rozporządzenia nie dotyczy majątkowych praw i obowiązków przedsiębiorców lub praw i obowiązków przedsiębiorców wobec administracji publicznej, nie podlega zatem obowiązkowi dokonania oceny przewidywanego wpływu na działalność mikroprzedsiębiorców oraz małych i średnich przedsiębiorców.

Projekt rozporządzenia został udostępniony na stronie Rządowego Centrum Legislacji w serwisie „Rządowy Proces Legislacyjny" oraz w Biuletynie Informacji Publicznej na stronie podmiotowej Ministra Cyfryzacji, 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).