Projekt z dnia 26 lutego 2020 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 …….. 2020 r.

**w sprawie szczegółowych warunków organizacyjnych i technicznych, które powinien spełniać system teleinformatyczny służący do uwierzytelniania użytkowników**

Na podstawie art. 20a ust. 3 pkt 1 ustawy z dnia 17 lutego 2005 r. o informatyzacji działalności podmiotów realizujących zadania publiczne (Dz. U. z 2019 r. poz. 700, 730, 848, 1590 i 2294) zarządza się, co następuje:

**§ 1**. Rozporządzenie określa szczegółowe warunki organizacyjne i techniczne, które powinien spełniać system teleinformatyczny służący do wydania certyfikatu oraz stosowania technologii, o których mowa w art. 20a ust. 2 ustawy z dnia 17 lutego 2005 r. o informatyzacji działalności podmiotów realizujących zadania publiczne, zwanej dalej „ustawą” w tym zakres i okres przechowywania danych w systemie oraz obowiązki informacyjne, do których zobowiązany jest administrator systemu.

**§ 2.** 1. System teleinformatyczny służący do wydania certyfikatu wykorzystywanego przez podmioty publiczne do uwierzytelniania użytkowników spełnia następujące warunki techniczne i organizacyjne:

1) umożliwia wystawienie certyfikatu oraz jego wydanie użytkownikowi, dla którego został on wystawiony;
2) umożliwia niezwłoczne unieważnienie certyfikatu;
3) określa dokładny czas wystawienia i unieważnienia certyfikatu, zgodnie z czasem uniwersalnym koordynowanym UTC(PL);
4) potwierdza tożsamość użytkownika, któremu wydano certyfikat;
5) posiada zabezpieczenia w zakresie bezpieczeństwa teleinformatycznego dobierane na podstawie szacowania ryzyka;

---

[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).

6) nie gromadzi ani nie kopiuje danych służących użytkownikom do potwierdzania tożsamości z wykorzystaniem certyfikatów.

2. System, o którym mowa w ust. 1, przechowuje dane dotyczące wystawionych certyfikatów przez okres 20 lat, licząc od dnia 1 stycznia roku następującego po roku, w którym certyfikat został wystawiony.

3. Bieżące zapewnienie poprawności i użyteczności funkcjonalnej systemu, o którym mowa w ust. 1, wymaga spełnienia następujących warunków technicznych i organizacyjnych:

1) dokonywania systematycznego przeglądu skuteczności zastosowanych środków w zakresie bezpieczeństwa teleinformatycznego, w celu wprowadzania ich usprawnień;
2) utrzymywania w stanie aktualnym dokumentacji operacyjnej i technicznej systemu, w celu zapewnienia jego bezpiecznej eksploatacji;
3) zapewniania organizacyjnego, technicznego i kryptograficznego bezpieczeństwa działania systemu;
4) prowadzenia działań zapobiegających fałszowaniu certyfikatów, w tym zapewniania poufności podczas procesu tworzenia danych do potwierdzania tożsamości;
5) informowania osób ubiegających się o certyfikat o warunkach stosowania certyfikatu zawartych w polityce certyfikacji.

4. Warunki, o których mowa w ust. 1 – 3, zostały spełnione, gdy:

1) została wdrożona polityka certyfikacji spełniająca wymagania wskazane w normie PN-ETSI EN 319 411 lub nowszej;
2) zapewnione zostały warunki organizacyjne i techniczne zgodne z wymaganiami specyfikacji technicznej CEN/TS 419261 lub nowszej w zakresie świadczenia usług innych niż wydawanie certyfikatów kwalifikowanych;
3) zastosowane zostały systemy i produkty zgodne z wymaganiami specyfikacji technicznej CEN/TS 419221 lub nowszej.

5. Administrator systemu, o którym mowa w ust. 1, udostępnia deklarację o spełnieniu wymagań określonych w ust. 3 oraz politykę certyfikacji:

1) w Biuletynie Informacji Publicznej, albo
2) na stronie internetowej administratora - w przypadku podmiotów niezobowiązanych do udostępniania informacji publicznej w Biuletynie Informacji Publicznej.

**§ 3.** 1. System teleinformatyczny przetwarzający dane dotyczące tożsamości użytkowników wykorzystywany przez podmioty publiczne do uwierzytelniania użytkowników w oparciu o inne technologie niż certyfikat:

1) rejestruje użytkowników;
2) potwierdza tożsamość użytkowników;
3) przechowuje i udostępnia dane identyfikacyjne użytkowników systemom autoryzującym uprawnionym do ich otrzymania;
4) umożliwia zablokowanie konta użytkownika na jego żądanie;
5) zapewnia rozliczalność, rozumianą jako przypisanie określonego działania w systemie do osoby fizycznej lub procesu oraz umiejscowienie ich w czasie;
6) zapewnia integralność, autentyczność i poufność danych identyfikacyjnych i uwierzytelniających użytkownika;
7) zapewnia codzienną synchronizację czasu systemowego z czasem uniwersalnym koordynowanym UTC(PL).

2. System, o którym mowa w ust. 1, przechowuje dane dotyczące tożsamości użytkownika przez okres 20 lat, licząc od dnia 1 stycznia roku następującego po roku, w którym wykonano w systemie ostatnią operację z użyciem tożsamości tego użytkownika.

3. System, o którym mowa w ust. 1, spełnia następujące warunki techniczne i organizacyjne w zakresie administrowania:

1) zapewnianie wiarygodności procesu rejestracji użytkowników i potwierdzania ich tożsamości;
2) utrzymywanie w stanie aktualnym dokumentacji operacyjnej i technicznej systemu, w celu zapewnienia jego bezpiecznej eksploatacji;
3) opracowywanie i ustanawianie, wdrażanie i eksploatowanie, monitorowanie i przeglądanie oraz utrzymywanie i doskonalenie systemu zarządzania bezpieczeństwem informacji spełniającego wymagania Polskiej Normy PN-EN ISO/IEC 27001, o którym mowa w przepisach wydanych na podstawie art. 18 ustawy.

4. Warunki określone w ust. 3 uważa się za spełnione, jeśli:

1) system zarządzania bezpieczeństwem informacji został oceniony pozytywnie przez jednostkę oceniającą zgodność , zgodnie z ustawą z dnia 13 kwietnia 2016 r. o systemach oceny zgodności i nadzoru rynku (Dz. U. z 2019 r. poz. 544), albo
2) administrator systemu, o którym mowa w ust. 1, udostępnił deklarację o spełnieniu wymagań określonych w ust. 3:

a) w Biuletynie Informacji Publicznej, albo

b) na stronie internetowej administratora - w przypadku podmiotów niezobowiązanych do udostępniania informacji publicznej w Biuletynie Informacji Publicznej.

**§ 4.** 1. System teleinformatyczny, o którym mowa w art. 20a ust 2 ustawy, uwierzytelniając użytkowników dokonuje weryfikacji tożsamości użytkowników wykorzystując certyfikaty wydane w systemie, o którym mowa w § 2 ust. 1 lub usługi systemu, o którym mowa w § 3 ust. 1 oraz przechowuje dane potwierdzające tę weryfikację.

2. Dane potwierdzające weryfikację, o których mowa w ust. 1, powinny w sposób jednoznaczny umożliwiać:

1) ustalenie tożsamości użytkownika, który dokonał czynności w postaci elektronicznej;
2) ustalenie czasu dokonania czynności;
3) stwierdzenie ważności uprawnień w momencie dokonania czynności.

**§ 5.** 1. Zakres danych przetwarzanych w certyfikatach wydawanych w systemie , o którym mowa w § 2 ust. 1 w przypadku wydawania certyfikatów:

1) osobom fizycznym jest zgodny z profilem certyfikatu określonym w normie PN-ETSI EN 319 412-2 lub nowszej,
2) osobom prawnym jest zgodny z profilem certyfikatu określonym w normie PN-ETSI EN 319 412-3 lub nowszej.

2. Zakres przetwarzanych danych w systemie, o którym mowa w § 3 ust. 1 odnoszących się do tożsamości użytkowników jest odpowiedni do zakresu określonego dla profilu zaufanego w przepisach wydanych na podstawie art. 20d ustawy.

**§ 6.** Systemy teleinformatyczne podmiotów realizujących zadania publiczne, służące do wydania certyfikatu oraz stosowania technologii, o których mowa w art. 20a ust. 2 ustawy, funkcjonujące w dniu wejścia w życie rozporządzenia, należy dostosować do wymagań określonych w przepisach niniejszego w rozporządzeniu nie później niż do 12 marca 2022 r.

**§ 6**. Rozporządzenie wchodzi w życie z dniem 12 marca 2020 r.[2)]

---

[2)] Niniejsze rozporządzenie było poprzedzone rozporządzeniem Ministra Spraw Wewnętrznych i Administracji z dnia 5 października 2016 r. w sprawie szczegółowych warunków organizacyjnych i technicznych, które powinien spełniać system teleinformatyczny służący do identyfikacji użytkowników (Dz. U. poz. 1627), które utraci moc z dniem 11 marca 2020 r., na podstawie art. 61 ustawy z dnia 5 lipca 2018 r. o zmianie ustawy o usługach zaufania i identyfikacji elektronicznej oraz niektórych innych ustaw (Dz. U. poz. 1544 oraz z 2019 r. poz. 60 i 934)

**MINISTER CYFRYZACJI**

***Za zgodność pod względem prawnym,***
***legislacyjnym i redakcyjnym***
*Magdalena Witkowska-Krzymowska*
*Dyrektor Departamentu Prawnego*
*w Ministerstwie Cyfryzacji*
*(podpisano elektronicznie )*

**U Z A S A D N I E N I E**

Projektowane rozporządzenie stanowi wykonanie upoważnienia ustawowego zawartego w art. 20a ust. 3 pkt 1ustawy z dnia 17 lutego 2005 r. *o informatyzacji działalności podmiotów realizujących zadania publiczne* (Dz. U. z 2019 r. poz. 700, 730, 848, 1590 i 2294) zwanej dalej *„ustawą o informatyzacji”*.

Konieczność wydania aktu wykonawczego wynika z faktu, iż na mocy art. 61 ustawy z dnia 5 lipca 2018 r. o zmianie ustawy o usługach zaufania oraz identyfikacji elektronicznej oraz niektórych innych ustaw (Dz. U. poz. 1544 oraz z 2019 r. poz. 60 i 934), aktualne rozporządzenie obowiązuje jedynie do momentu wydania nowego rozporządzenia, jednak nie dłużej niż do dnia 11 marca 2020 r. Niewydanie nowego rozporządzenia spowoduje powstanie luki w przepisach prawa.

Regulacje zawarte w rozporządzeniu stanowią w większości powtórzenie przepisów zawartych w obowiązującym rozporządzeniu 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 przedkładanym projekcie rozporządzenia dokonano następujących zmian w stosunku do zmienianego rozporządzenia :

1. Zaktualizowano wycofaną specyfikację techniczną ETSI TS 102 042 wskazując z zamian zastępującą ją normę PN ETSI EN 319 411 (§ 2 ust. 4 pkt 1). Podobnie zaktualizowano wycofane porozumienia warsztatowe CWA 14167-1-4 i wskazując zastępujące je obecnie specyfikacje techniczne CEN/TS 419261 oraz CEN/TS 419221 (§ 2 ust. 4 pkt 2 i 3).

2. Dokonano poprawek mających na celu zachowanie spójności stosowanych pojęć z ustawą o informatyzacji. W tym zakresie zrezygnowano z pojęć „system certyfikujący” „system zarządzania tożsamością” oraz „system autoryzujący” wskazując, że chodzi odpowiednio o „system teleinformatyczny służący do wydawania certyfikatów wykorzystywanych przez podmioty publiczne do uwierzytelniania użytkowników” (§ 2 ust. 1), „system przetwarzający dane dotyczące tożsamości użytkowników wykorzystywany przez podmioty publiczne do uwierzytelniania użytkowników w oparciu o inne metody niż certyfikat (§ 3 ust. 1) oraz odpowiednie działanie systemu służącego do uwierzytelniania użytkowników lub wykorzystującego usługi systemu, o którym mowa w § 3 rozporządzenia (§ 4 ust. 1).

3. Doprecyzowano, że dla określania czasu wystawienia i unieważnienia certyfikatu należy stosować uniwersalny czas koordynowany UTC(PL) (§ 2 ust. 1 pkt 3).

4. Poprawiono pod względem językowym wymagania mające na celu zapewnienie bieżącej poprawności i użyteczności funkcjonalnej systemu teleinformatycznego służącego do wydawania certyfikatów wykorzystywanych przez podmioty publiczne do uwierzytelniania użytkowników, w tym:

a) poprawiono do czego ma służyć utrzymywanie w stanie aktualnym dokumentacji operacyjnej i technicznej systemu (bezpiecznej eksploatacji), a nie jak dotąd mogło być rozumiane że samo istnienie dokumentacji zapewnia bezpieczna eksploatację (§ 2 ust. 3 pkt 2),

b) doprecyzowano brzmienie przepisu (§ 2 ust. 3 pkt 5) wskazując, że chodzi o informowanie osób ubiegających się o certyfikat o warunkach stosowania certyfikatu zawartych w polityce certyfikacji, a nie zapewnienie im tylko informacji gdzie ta polityka jest udostępniona. Jest to podobne wymaganie jak przypadku kwalifikowanych usług zaufania w art. 24 ust. 2 lit d Rozporządzenia Parlamentu Europejskiego i Rady (UE) Nr 910/2014 z dnia 23 lipca 2014 r. w sprawie identyfikacji elektronicznej i usług zaufania w odniesieniu do transakcji elektronicznych na rynku wewnętrznym.

5. Zmieniono redakcję przepisu § 2 ust. 4 tak, aby nie było wątpliwości, że zakres dostosowania do norm i specyfikacji technicznych wymienionych w tym przepisie dotyczy wymagań określonych w ust. 1-3 i co za tym idzie wymienione normy i specyfikacje nie mogą być stosowane zamiast przepisów ust. 1-3.

6. Uzupełniono przepis 3 ust. 3 pkt 3 dodając wskazanie normę PN-EN ISO/IEC 27001 celem rozwiania wątpliwości czy ma ona zastosowania przy ocenie systemu zarządzania bezpieczeństwem informacji dokonywanej przez jednostkę oceniająca zgodność.

7. Dla systemów przetwarzających dane dotyczące tożsamości użytkowników wykorzystywanych przez podmioty publiczne do uwierzytelniania użytkowników w oparciu o inne metody niż certyfikat dodano alternatywną możliwość uznania spełnienia wymagań podobnie jak to ma już teraz miejsce dla systemów wykorzystujących certyfikaty. Po zmianach możliwe to będzie albo przez uzyskanie pozytywnej oceny z jednostki oceniającej zgodność, albo na podstawie deklaracji ogłoszonej w BIP lub na stronie internetowej podmiotu – w przypadku podmiotów niezobowiązanych do prowadzenia Biuletynu Informacji Publicznej.

8. Wskazano zakres przetwarzanych danych. W przypadku, w którym do uwierzytelniania użytkowników wykorzystywany jest system wykorzystujący certyfikaty zakres ten ma być odpowiedni jak określono profile certyfikatów w normach PN-ETSI EN 319 412-2 lub PN-ETSI EN 319 412-3. Dla przypadków gdy wykorzystywany jest system wykorzystujący inne metody niż certyfikat zakres ma być odpowiedni do zakresu określonego dla profilu zaufanego. Zakres ten ma być odpowiedni a nie identyczny, ponieważ nie może on zawierać identyfikatora profilu zaufanego, tylko właściwy dla danego systemu identyfikator.

Mając na uwadze, że rozporządzenie w niewielkim stopniu zmienia wymagania zawarte w obowiązującym rozporządzeniu Ministra Cyfryzacji z dnia 5 października 2016 r. *w sprawie szczegółowych warunków organizacyjnych i technicznych, które powinien spełniać system teleinformatyczny służący do uwierzytelniania użytkowników* i co za tym idzie systemy zgodne z obecnymi wymaganiami zwykle będą zgodnie też z nowymi wymaganiami, aby nie wymuszać spiętrzenia natychmiastowych dostosowań do nowych norm i specyfikacji techniczny przewidziano dwuletni okres dostosowawczy. W tym kontekście znaczenia mają też znaczenie przepisy art. 60 ustawy z dnia 5 lipca 2018 r. o zmianie ustawy o usługach zaufania oraz identyfikacji elektronicznej oraz niektórych innych ustaw, które wymuszają na podmiotach publicznych zapewnienie możliwości uwierzytelnienia użytkowników z wykorzystaniem środków identyfikacji elektronicznej wydanych w systemach identyfikacji elektronicznej przyłączonych do węzła krajowego identyfikacji elektronicznej najpóźniej od dnia 1 stycznia 2022 r. Oznacza to, że część podmiotów może w ogóle zrezygnować z możliwości jakie daje art. 20a ust. 2 ustawy o informatyzacji i co za tym idzie nie dawać możliwości uwierzytelniania w inny sposób. Mogą to być zwłaszcza te podmioty, które uznają, że dostosowanie i dalsze utrzymywanie własnego systemu identyfikacji nie jest już potrzebne wobec możliwości jakie stwarza węzeł krajowy. Tym bardziej że za pośrednictwem węzła krajowego będą mogły z usług online podmiotu publicznego korzystać także osoby posiadające środki identyfikacji elektronicznej wydane w innych państwach członkowskich Unii Europejskiej.

Wskazane w projekcie normy i specyfikacje techniczne Europejskiego Instytutu Norm Telekomunikacyjnych oraz Europejskiego Komitetu Normalizacyjnego to aktualne wersje znajdujących się w obowiązującej wersji rozporządzenia ogólnie uznanych norm ”dla produktów z podpisem elektronicznym” wymaganych dla systemów w których wydawane są certyfikaty zaawansowanych podpisów elektronicznych. Normy te zostały wskazane w ramach

standaryzacyjnych wydanych zgodnie z mandatem M460[3)]. W związku z tym nie podlega notyfikacji zgodnie z trybem przewidzianym w przepisach 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 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).

---

[3)] https://ec.europa.eu/growth/toolsdatabases/mandates/index.cfm?fuseaction=search.detail&id=442

| | |
|---|---|
| **Nazwa projektu**<br>Projekt rozporządzenia Ministra Cyfryzacji w sprawie szczegółowych warunków organizacyjnych i technicznych, które powinien spełniać system teleinformatyczny służący do identyfikacji użytkowników<br>**Ministerstwo wiodące i ministerstwa współpracujące**<br>Ministerstwo Cyfryzacji<br>**Osoba odpowiedzialna za projekt w randze Ministra, Sekretarza Stanu lub Podsekretarza Stanu**<br>Minister Cyfryzacji Marek Zagórski<br>**Kontakt do opiekuna merytorycznego projektu**<br>Kazimierz Schmidt, Radca ministra w Departamencie Systemów Państwowych: kazimierz.schmidt@mc.gov.pl<br>Tel. 225568403 | **Data sporządzenia**<br>26 lutego 2020 r.<br>**Źródło:**<br>Upoważnienie ustawowe – art. 20a ust. 3 pkt 1 ustawy z dnia 17 lutego 2005 r. *o informatyzacji działalności podmiotów realizujących zadania publiczne* (Dz. U. z 2019 r. poz. 700, 730, 848, 1590 i 2294)<br>**Nr w wykazie prac:**<br>**150** |

**OCENA SKUTKÓW REGULACJI**

**1. Jaki problem jest rozwiązywany?**

Konieczność wydania aktu wykonawczego wynika z faktu, iż na mocy art. 61 ustawy z dnia 5 lipca 2018 r. o zmianie ustawy o usługach zaufania oraz identyfikacji elektronicznej oraz niektórych innych ustaw (Dz. U. poz. 1544 oraz z 2019 r. poz. 60 i 934), aktualne rozporządzenie obowiązuje jedynie do momentu wydania nowego rozporządzenia, jednak nie dłużej niż do dnia 11 marca 2020 r. Niewydanie nowego rozporządzenia spowoduje powstanie luki w przepisach prawa.

Ponadto w projekcie zaktualizowano odniesienia do norm i specyfikacji technicznych, które zostały wycofane. Dokonano również poprawek mających na celu zachowanie spójności stosowanych pojęć z ustawą z dnia 17 lutego 2005 r. o informatyzacji działalności podmiotów realizujących zadania publiczne (Dz. U. z 2019 r. poz. 700, 730, 848, 1590 i 2294).

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

Wydanie nowego rozporządzenia z terminem wejścia w życie w dniu następnym po dniu, w którym uchylone zostanie z mocy prawa obowiązujące obecnie 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 |
|---|---|---|---|
| Podmioty publiczne określone w art. 2 ust 1 ustawy z dnia 17 lutego 2005 r. o informatyzacji działalności podmiotów realizujących zadania publiczne (Dz. U. z 2019 r. poz. 700, 730, 848, 1590 i 2294) oraz wskazane w art. 2 ust 2 tj. podmioty którym powierzono lub | Około 700 | Liczba podmiotów przyłączonych do krajowego węzła identyfikacji elektronicznej lub będących w trakcie przyłączania (obecnie ok. 170) + liczba podmiotów które dotąd zadeklarowały w odpowiedzi na pismo Ministra Cyfryzacji że będą wnioskować o przyłączenia (ok. 500).<br>Mając na uwadze, że wszystkie podmioty stosujące obecnie sposoby | Podmioty objęte rozporządzeniem powinny dostosować swoje systemu służące uwierzytelnianiu użytkowników w ciągu 2 lat. Mogą też zrezygnować z utrzymywania własnych systemów |

| | | | |
|---|---|---|---|
| zlecono realizację zadania publicznego. | | uwierzytelnia użytkowników jakie daje art. 20a ust 2 ustawy o informatyzacji muszą najpóźniej do 1 stycznia 2022 r zgodnie art. 60 ustawy z dnia 5 lipca 2018 r. o zmianie ustawy o usługach zaufania oraz identyfikacji elektronicznej oraz niektórych innych ustaw (Dz. U. poz. 1544 oraz z 2019 r. poz. 60 i 934) przyłączyć się do węzła krajowego – liczba podmiotów przyłączanych lub przyłączonych do węzła będzie w przybliżeniu oznaczała podmiotu posiadające obecnie „własny" system do uwierzytelniania użytkowników . | polegając wyłącznie na uwierzytelnieniu za pośrednictwa węzła krajowego. |

**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 lobbingowej w procesie stanowienia prawa (Dz. U. z 2017 r. poz. 248).

Ponadto projekt został przekazany następującym podmiotom:

I. w ramach opiniowania:
1. Prezes Prokuratorii Generalnej Rzeczypospolitej Polskiej,
2. Prezes Urzędu Ochrony Danych Osobowych,
3. Prezes Urzędu Zamówień Publicznych,
4. Prezes Zakładu Ubezpieczeń Społecznych (ZUS),
5. 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.,
12. Związek Banków Polskich,
13. Izba Gospodarki Elektronicznej,
14. Polska lzba Informatyki Medycznej.
III. w ramach konsultacji publicznych z organizacjami pracodawców i pracowników:
1. Rada Dialogu Społecznego,
2. Business Centre Club – Związek Pracodawców,

3. Forum Związków Zawodowych,
4. Niezależny Samorządny Związek Zawodowy „Solidarność",
5. Konfederacja Lewiatan,
6. Ogólnopolskie Porozumienie Związków Zawodowych
7. Pracodawcy Rzeczypospolitej Polskiej
8. Związek Rzemiosła Polskiego,
9. Związek Przedsiębiorców i Pracodawców,
10. Związek Pracodawców Branży Internetowej Interactive Advertising Bureau Polska.

W wyniku uzgodnień i konsultacji zastąpiono wycofane porozumienie techniczne CWA 14167 aktualnymi specyfikacjami CEN/TS 419261 oraz CEN/TS 419221. Poprawiono niejasności dotyczące niektórych przepisów w tym stosowania czasu UTC(PL), wskazano normę PN-EN ISO/IEC 27001 celem rozwiania wątpliwości, że ma ona zastosowanie przy ocenie systemu zarządzania bezpieczeństwem informacji dokonywanej przez jednostkę oceniająca zgodność.

Wskazano także zakres przetwarzanych danych. W przypadku, w którym do uwierzytelniania użytkowników wykorzystywany jest system wykorzystujący certyfikaty zakres ten ma być odpowiedni jak określono profile certyfikatów w normach PN-ETSI EN 319 412-2 lub PN-ETSI EN 319 412-3. Dla przypadków gdy wykorzystywany jest system wykorzystujący inne metody niż certyfikat zakres ma być odpowiedni do zakresu określonego dla profilu zaufanego.

Dla systemów przetwarzających dane dotyczące tożsamości użytkowników wykorzystywanych przez podmioty publiczne do uwierzytelniania użytkowników w oparciu o inne metody niż certyfikat dodano alternatywną możliwość uznania spełnienia wymagań podobnie jak to ma już teraz miejsce dla systemów wykorzystujących certyfikaty. Po zmianach możliwe to będzie albo przez uzyskanie pozytywnej oceny z jednostki certyfikującej oceniającą zgodność, albo na podstawie deklaracji ogłoszonej w BIP lub na stronie internetowej podmiotu – w przypadku podmiotów niezobowiązanych do prowadzenia Biuletynu Informacji Publicznej.

Dokonano poprawek mających na celu zachowanie spójności stosowanych pojęć z ustawą z dnia 17 lutego 2005 r. o informatyzacji działalności podmiotów realizujących zadania publiczne (Dz. U. z 2019 r. poz. 700, 730, 848, 1590 i 2294).

**6. Wpływ na sektor finansów publicznych**

| (ceny stałe z …… r.) | Skutki w okresie 10 lat od wejścia w życie zmian [mln zł] | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | 0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 | *Łącznie (0-10)* |
| **Dochody ogółem** | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 |
| 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 |
| **Wydatki ogółem** | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 |
| 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 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 |
| 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 | – nie dotyczy |
| Dodatkowe informacje, w tym wskazanie źródeł danych i przyjętych do obliczeń założeń | Wejście w życie projektowanego rozporządzenia nie będzie miało wpływu na sektor finansów publicznych. |

**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 | *Łącznie (0-10)* |
| W ujęciu pieniężnym (w mln zł, ceny stałe z …… r.) | duże przedsiębiorstwa | 0 | 0 | 0 | 0 | 0 | 0 | 0 |
| | sektor mikro-, małych i średnich przedsiębiorstw | 0 | 0 | 0 | 0 | 0 | 0 | 0 |
| | rodzina, obywatele oraz gospodarstwa domowe | 0 | 0 | 0 | 0 | 0 | 0 | 0 |
| | (dodaj/usuń) | 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 sytuacje ekonomiczna i społeczną rodziny, a także osób niepełnosprawnych oraz osób starszych. |

**8. Zmiana obciążeń regulacyjnych (w tym obowiązków informacyjnych) wynikających z projektu**

☒ nie dotyczy

| | |
|---|---|
| Wprowadzane są obciążenia poza bezwzględnie wymaganymi przez UE (szczegóły w odwróconej tabeli zgodności). | ☐ tak<br>☐ nie<br>☒ nie dotyczy |
| ☐ zmniejszenie liczby dokumentów<br>☐ zmniejszenie liczby procedur<br>☐ skrócenie czasu na załatwienie sprawy<br>☐ inne: | ☐ zwiększenie liczby dokumentów<br>☐ zwiększenie liczby procedur<br>☐ wydłużenie czasu na załatwienie sprawy<br>☐ inne: |
| Wprowadzane obciążenia są przystosowane do ich elektronizacji. | ☐ tak<br>☐ nie<br>☒ nie dotyczy |
| Komentarz: | |

| **9. Wpływ na rynek pracy** |
|---|
| Projektowane rozporządzenie nie będzie miało wpływu na rynek pracy. |

| **10. Wpływ na pozostałe obszary** | | |
|---|---|---|
| ☐ środowisko naturalne<br>☐ sytuacja i rozwój regionalny<br>☐ inne: | ☐ demografia<br>☐ mienie państwowe | ☒ informatyzacja<br>☐ 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 |