►B 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.U. L 257 z 28.8.2014, s. 73)

zmienione przez:

		Dziennik Urzędowy		
		nr	strona	data
►M1	Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2024/1183 z dnia 11 kwietnia 2024 r.	L 1183	1	30.4.2024

▼B

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

ROZDZIAŁ I

PRZEPISY OGÓLNE

▼M1

Artykuł 1

Przedmiot

Celem niniejszego rozporządzenia jest zapewnienie właściwego funkcjonowania rynku wewnętrznego oraz odpowiedniego poziomu bezpieczeństwa środków identyfikacji elektronicznej i usług zaufania wykorzystywanych w całej Unii, aby umożliwić i ułatwić osobom fizycznym i prawnym korzystanie z prawa do bezpiecznego uczestnictwa w społeczeństwie cyfrowym oraz dostępu do usług publicznych i prywatnych online w całej Unii. W tym celu niniejsze rozporządzenie:

a) określa warunki, na jakich państwa członkowskie mają zapewniać i uznawać środki identyfikacji elektronicznej osób fizycznych i prawnych, które objęte są notyfikowanym systemem identyfikacji elektronicznej innego państwa członkowskiego, oraz zapewniać i uznawać europejskie portfele tożsamości cyfrowej;

b) określa przepisy dotyczące usług zaufania, w szczególności na potrzeby transakcji elektronicznych;

c) ustanawia ramy prawne dla podpisów elektronicznych, pieczęci elektronicznych, elektronicznych znaczników czasu, dokumentów elektronicznych, usług rejestrowanego doręczenia elektronicznego, usług certyfikacyjnych uwierzytelniania witryn internetowych, archiwizacji elektronicznej, elektronicznego poświadczenia atrybutów, urządzeń do składania podpisu elektronicznego, urządzeń do składania pieczęci elektronicznej, oraz rejestrów elektronicznych.

▼B

Artykuł 2

Zakres stosowania

▼M1

1. Niniejsze rozporządzenie ma zastosowanie do systemów identyfikacji elektronicznej notyfikowanych przez państwo członkowskie, do europejskich portfeli tożsamości cyfrowej zapewnianych przez państwo członkowskie oraz do dostawców usług zaufania mających siedzibę w Unii.

▼B

2. Niniejsze rozporządzenie nie ma zastosowania do świadczenia usług zaufania wykorzystywanych wyłącznie w obrębie zamkniętych systemów wynikających z prawa krajowego lub z porozumień zawartych przez określoną grupę uczestników.

▼M1

3. Niniejsze rozporządzenie nie ma wpływu na prawo Unii ani prawo krajowe dotyczące zawierania i ważności umów, innych obowiązków prawnych lub proceduralnych dotyczących ich formy, ani na wymogi sektorowe dotyczące ich formy.

▼M1

4. Niniejsze rozporządzenie pozostaje bez uszczerbku dla rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 ([1]).

▼B

Artykuł 3

Definicje

Do celów niniejszego rozporządzenia stosuje się następujące definicje:

▼M1

1) „identyfikacja elektroniczna” oznacza proces używania danych identyfikujących osobę, w postaci elektronicznej, niepowtarzalnie reprezentujących osobę fizyczną lub prawną, lub osobę fizyczną reprezentującą inną osobę fizyczną lub osobę prawną;

2) „środek identyfikacji elektronicznej” oznacza materialną lub niematerialną jednostkę zawierającą dane identyfikujące osobę i używaną do celów uwierzytelniania dla usługi online lub, w stosownych przypadkach, dla usługi offline;

3) „dane identyfikujące osobę” oznaczają zestaw danych, który jest wydawany zgodnie z prawem Unii lub prawem krajowym i który umożliwia ustalenie tożsamości osoby fizycznej lub prawnej, lub osoby fizycznej reprezentującej inną osobę fizyczną lub osobę prawną;

4) „system identyfikacji elektronicznej” oznacza system identyfikacji elektronicznej, w ramach którego wydaje się środki identyfikacji elektronicznej osobom fizycznym lub prawnym, lub osobom fizycznym reprezentującym inne osoby fizyczne lub osoby prawne;

5) „uwierzytelnianie” oznacza proces elektroniczny, który umożliwia potwierdzenie identyfikacji elektronicznej osoby fizycznej lub prawnej, lub potwierdzenie pochodzenia i integralności danych w postaci elektronicznej;

5a) „użytkownik” oznacza osobę fizyczną lub prawną, lub osobę fizyczną reprezentującą inną osobę fizyczną lub osobę prawną, korzystającą z usług zaufania lub środków identyfikacji elektronicznej świadczonych lub zapewnianych zgodnie z niniejszym rozporządzeniem;

6) „strona ufająca” oznacza osobę fizyczną lub prawną, która polega na identyfikacji elektronicznej, europejskich portfelach tożsamości cyfrowej lub innym środku identyfikacji elektronicznej, lub na usłudze zaufania;

▼B

7) „podmiot sektora publicznego” oznacza organ państwowy, regionalny lub lokalny, podmiot prawa publicznego lub stowarzyszenie utworzone przez jeden lub kilka takich organów lub jeden lub kilka takich podmiotów prawa publicznego, lub jednostkę prywatną, której co najmniej jeden z tych organów, podmiotów lub jedno z takich stowarzyszeń udzieliły upoważnienia do świadczenia usług publicznych, gdy działa ona na podstawie takiego upoważnienia;

([1]) Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych) (Dz.U. L 119 z 4.5.2016, s. 1).

▼B

8) „podmiot prawa publicznego” oznacza podmiot zdefiniowany w art. 2 ust. 1 pkt 4 dyrektywy Parlamentu Europejskiego i Rady 2014/24/UE ([1]);

9) „podpisujący” oznacza osobę fizyczną, która składa podpis elektroniczny;

10) „podpis elektroniczny” oznacza dane w postaci elektronicznej, które są dołączone lub logicznie powiązane z innymi danymi w postaci elektronicznej, i które użyte są przez podpisującego jako podpis;

11) „zaawansowany podpis elektroniczny” oznacza podpis elektroniczny, który spełnia wymogi określone w art. 26;

12) „kwalifikowany podpis elektroniczny” oznacza zaawansowany podpis elektroniczny, który jest składany za pomocą kwalifikowanego urządzenia do składania podpisu elektronicznego i który opiera się na kwalifikowanym certyfikacie podpisu elektronicznego;

13) „dane służące do składania podpisu elektronicznego” oznaczają unikalne dane, których podpisujący używa do składania podpisu elektronicznego;

14) „certyfikat podpisu elektronicznego” oznacza poświadczenie elektroniczne, które przyporządkowuje dane służące do walidacji podpisu elektronicznego do osoby fizycznej i potwierdza co najmniej imię i nazwisko lub pseudonim tej osoby;

15) „kwalifikowany certyfikat podpisu elektronicznego” oznacza certyfikat podpisu elektronicznego, który jest wydawany przez kwalifikowanego dostawcę usług zaufania i spełnia wymogi określone w załączniku I;

▼M1

16) „usługa zaufania” oznacza usługę elektroniczną zazwyczaj świadczoną za wynagrodzeniem i obejmującą którąkolwiek z następujących czynności:

   a) wydawanie certyfikatów podpisów elektronicznych, certyfikatów pieczęci elektronicznych, certyfikatów uwierzytelniania witryn internetowych lub certyfikatów do celów świadczenia innych usług zaufania;

   b) walidację certyfikatów podpisów elektronicznych, certyfikatów pieczęci elektronicznych, certyfikatów uwierzytelniania witryn internetowych lub certyfikatów do celów świadczenia innych usług zaufania;

   c) tworzenie podpisów elektronicznych lub pieczęci elektronicznych;

   d) walidację podpisów elektronicznych lub pieczęci elektronicznych;

   e) konserwację podpisów elektronicznych, pieczęci elektronicznych, certyfikatów podpisów elektronicznych lub certyfikatów pieczęci elektronicznych;

   f) zarządzanie urządzeniami do składania podpisu elektronicznego na odległość lub urządzeniami do składania pieczęci elektronicznej na odległość;

   g) wydawanie elektronicznych poświadczeń atrybutów;

   h) walidację elektronicznych poświadczeń atrybutów;

([1]) Dyrektywa Parlamentu Europejskiego i Rady 2014/24/UE z dnia 26 lutego 2014 r. w sprawie zamówień publicznych, uchylająca dyrektywę 2004/18/WE (Dz.U. L 94 z 28.3.2014, s. 65).

▼M1

i) tworzenie elektronicznych znaczników czasu;

j) walidację elektronicznych znaczników czasu;

k) świadczenie usług rejestrowanego doręczenia elektronicznego;

l) walidację danych przekazywanych za pośrednictwem usług rejestrowanego doręczenia elektronicznego i związanych z nimi dowodów;

m) archiwizację elektroniczną danych elektronicznych i dokumentów elektronicznych;

n) rejestrowanie danych elektronicznych w rejestrze elektronicznym;

▼B

17) „kwalifikowana usługa zaufania” oznacza usługę zaufania, która spełnia stosowne wymogi określone w niniejszym rozporządzeniu;

▼M1

18) „jednostka oceniająca zgodność” oznacza jednostkę oceniającą zgodność zdefiniowaną w art. 2 pkt 13 rozporządzenia (WE) nr 765/2008, która jest akredytowana zgodnie z tym rozporządzeniem jako właściwa do przeprowadzania oceny zgodności kwalifikowanego dostawcy usługi zaufania i świadczonych przez niego kwalifikowanych usług zaufania, lub jako właściwa do dokonywania certyfikacji europejskich portfeli tożsamości cyfrowej lub środków identyfikacji elektronicznej;

▼B

19) „dostawca usług zaufania” oznacza osobę fizyczną lub prawną, która świadczy przynajmniej jedną usługę zaufania, jako kwalifikowany lub niekwalifikowany dostawca usług zaufania;

20) „kwalifikowany dostawca usług zaufania” oznacza dostawcę usług zaufania, który świadczy przynajmniej jedną kwalifikowaną usługę zaufania i któremu status kwalifikowany nadał organ nadzoru;

▼M1

21) „produkt” oznacza sprzęt lub oprogramowanie, lub odpowiednie komponenty sprzętu lub oprogramowania, które są przeznaczone do wykorzystywania w zapewnianiu usług identyfikacji elektronicznej i usług zaufania;

▼B

22) „urządzenie do składania podpisu elektronicznego” oznacza skonfigurowane oprogramowanie lub skonfigurowany sprzęt, które wykorzystuje się do składania podpisu elektronicznego;

23) „kwalifikowane urządzenie do składania podpisu elektronicznego” oznacza urządzenie do składania podpisu elektronicznego, które spełnia wymogi określone w załączniku II;

▼M1

23a) „kwalifikowane urządzenie do składania podpisu elektronicznego na odległość” oznacza kwalifikowane urządzenie do składania podpisu elektronicznego, którym zarządza kwalifikowany dostawca usług zaufania zgodnie z art. 29a w imieniu podpisującego;

▼M1

23b) „kwalifikowane urządzenie do składania pieczęci elektronicznej na odległość” oznacza kwalifikowane urządzenie do składania pieczęci elektronicznej, którym zarządza kwalifikowany dostawca usług zaufania zgodnie z art. 39a w imieniu składającego pieczęć;

▼B

24) „podmiot składający pieczęć” oznacza osobę prawną, która składa pieczęć elektroniczną;

25) „pieczęć elektroniczna” oznacza dane w postaci elektronicznej dodane do innych danych w postaci elektronicznej lub logicznie z nimi powiązane, aby zapewnić autentyczność pochodzenia oraz integralność powiązanych danych;

26) „zaawansowana pieczęć elektroniczna” oznacza pieczęć elektroniczną, która spełnia wymogi określone w art. 36;

27) „kwalifikowana pieczęć elektroniczna” oznacza zaawansowaną pieczęć elektroniczną, która została złożona za pomocą kwalifikowanego urządzenia do składania pieczęci elektronicznej i która opiera się na kwalifikowanym certyfikacie pieczęci elektronicznej;

28) „dane służące do składania pieczęci elektronicznej” oznaczają niepowtarzalne dane, które podmiot składający pieczęć wykorzystuje do złożenia pieczęci elektronicznej;

29) „certyfikat pieczęci elektronicznej” oznacza poświadczenie elektroniczne, które łączy dane służące do walidacji pieczęci elektronicznej z osobą prawną i potwierdza nazwę tej osoby;

30) „kwalifikowany certyfikat pieczęci elektronicznej” oznacza certyfikat pieczęci elektronicznej, który jest wydawany przez kwalifikowanego dostawcę usług zaufania i spełnia wymogi określone w załączniku III;

31) „urządzenie do składania pieczęci elektronicznej” oznacza skonfigurowane oprogramowanie lub skonfigurowany sprzęt, które wykorzystuje się do składania pieczęci elektronicznej;

32) „kwalifikowane urządzenie do składania pieczęci elektronicznej” oznacza urządzenie do składania pieczęci elektronicznej, które spełnia odpowiednio wymogi określone w załączniku II;

33) „elektroniczny znacznik czasu” oznacza dane w postaci elektronicznej, które wiążą inne dane w postaci elektronicznej z określonym czasem, stanowiąc dowód na to, że te inne dane istniały w danym czasie;

34) „kwalifikowany elektroniczny znacznik czasu” oznacza elektroniczny znacznik czasu, który spełnia wymogi określone w art. 42;

35) „dokument elektroniczny” oznacza każdą treść przechowywaną w postaci elektronicznej, w szczególności tekst lub nagranie dźwiękowe, wizualne lub audiowizualne;

36) „usługa rejestrowanego doręczenia elektronicznego” oznacza usługę umożliwiającą przesłanie danych między stronami trzecimi drogą elektroniczną i zapewniającą dowody związane z posługiwaniem się przesyłanymi danymi, w tym dowód wysłania i otrzymania danych, oraz chroniącą przesyłane dane przed ryzykiem utraty, kradzieży, uszkodzenia lub jakiejkolwiek nieupoważnionej zmiany;

▼B

37) „kwalifikowana usługa rejestrowanego doręczenia elektronicznego” oznacza usługę rejestrowanego doręczenia elektronicznego, która spełnia wymogi określone w art. 44;

▼M1

38) „certyfikat uwierzytelniania witryn internetowych” oznacza poświadczenie elektroniczne, które umożliwia uwierzytelnianie witryn internetowych i przyporządkowuje witrynę internetową do osoby fizycznej lub prawnej, której wydano certyfikat;

▼B

39) „kwalifikowany certyfikat uwierzytelniania witryn internetowych” oznacza certyfikat uwierzytelniania witryn internetowych, który jest wydawany przez kwalifikowanego dostawcę usług zaufania i spełnia wymogi określone w załączniku IV;

40) „dane służące do walidacji” oznaczają dane używane do walidacji podpisu elektronicznego lub pieczęci elektronicznej;

▼M1

41) „walidacja” oznacza proces weryfikacji i potwierdzania, że dane w postaci elektronicznej są ważne zgodnie z niniejszym rozporządzeniem;

42) „europejski portfel tożsamości cyfrowej” oznacza środek identyfikacji elektronicznej, który umożliwia użytkownikowi bezpieczne przechowywanie i walidację danych identyfikujących osobę i elektronicznych poświadczeń atrybutów oraz bezpieczne zarządzanie tymi danymi i poświadczeniami na potrzeby udostępniania ich stronom ufającym oraz innym użytkownikom europejskich portfeli tożsamości cyfrowej, i który umożliwia składanie kwalifikowanych podpisów elektronicznych lub kwalifikowanych pieczęci elektronicznych;

43) „atrybut” oznacza cechę charakterystyczną, właściwość, prawo lub zezwolenie osoby fizycznej lub prawnej lub przedmiotu;

44) „elektroniczne poświadczenie atrybutów” oznacza poświadczenie w postaci elektronicznej, które umożliwia uwierzytelnienie atrybutów;

45) „kwalifikowane elektroniczne poświadczenie atrybutów” oznacza elektroniczne poświadczenie atrybutów, które jest wydawane przez kwalifikowanego dostawcę usług zaufania oraz spełnia wymogi określone w załączniku V;

46) „elektroniczne poświadczenie atrybutów wydane przez podmiot sektora publicznego odpowiedzialny za źródło autentyczne lub w jego imieniu” oznacza elektroniczne poświadczenie atrybutu wydane przez podmiot sektora publicznego, który jest odpowiedzialny za źródło autentyczne, lub przez podmiot sektora publicznego, który jest wyznaczony przez państwo członkowskie do wydawania takich poświadczeń atrybutów w imieniu podmiotów sektora publicznego odpowiedzialnych za źródła autentyczne zgodnie z art. 45f oraz z załącznikiem VII;

47) „źródło autentyczne” oznacza repozytorium lub system, za prowadzenie którego odpowiedzialny jest podmiot sektora publicznego lub podmiot prywatny, które zawiera i udostępnia atrybuty dotyczące osoby fizycznej lub prawnej lub przedmiotu i które uważa się za podstawowe źródło tych informacji lub uznaje za autentyczne zgodnie z prawem Unii lub prawem krajowym, w tym z praktykami administracyjnymi;

▼M1

48) „archiwizacja elektroniczna” oznacza usługę zapewniającą odbiór, przechowywanie, pobieranie i usuwanie danych elektronicznych i dokumentów elektronicznych w celu zapewnienia ich trwałości i czytelności, a także zachowywania ich integralności, poufności i dowodu pochodzenia przez cały okres ich przechowywania;

49) „kwalifikowana usługa archiwizacji elektronicznej” oznacza usługę archiwizacji elektronicznej, która jest świadczona przez kwalifikowanego dostawcę usług zaufania i która spełnia wymogi określone w art. 45j;

50) „unijny znak zaufania dla portfela tożsamości cyfrowej” oznacza weryfikowalne i rozpoznawalne wskazanie, które w jasny sposób informuje, że europejski portfel tożsamości cyfrowej zapewniono zgodnie z niniejszym rozporządzeniem;

51) „silne uwierzytelnienie użytkownika” oznacza uwierzytelnienie w oparciu o zastosowanie co najmniej dwóch składników uwierzytelniania należących do różnych kategorii: wiedza, czyli coś, co wie wyłącznie użytkownik, posiadanie, czyli coś, co posiada wyłącznie użytkownik, albo cecha użytkownika, czyli coś, czym jest użytkownik, niezależnych w tym znaczeniu, że naruszenie jednego z nich nie osłabia wiarygodności pozostałych, które to uwierzytelnienie jest zaprojektowane, tak aby zapewniać ochronę poufności danych uwierzytelniających;

52) „rejestr elektroniczny” oznacza sekwencję elektronicznych wpisów danych zapewniającą integralność tych wpisów i prawidłowość ich chronologicznego uporządkowania;

53) „kwalifikowany rejestr elektroniczny” oznacza rejestr elektroniczny, który jest zapewniany przez kwalifikowanego dostawcę usług zaufania i który spełnia wymogi określone w art. 45l;

54) „dane osobowe” oznaczają wszelkie informacje zdefiniowane w art. 4 pkt 1 rozporządzenia (UE) 2016/679;

55) „dopasowywanie tożsamości” oznacza proces, w którym dane identyfikujące osobę lub środki identyfikacji elektronicznej są dopasowywane lub przyporządkowywane do istniejącego konta należącego do tej samej osoby;

56) „wpis danych” oznacza dane elektroniczne zarejestrowane wraz z powiązanymi metadanymi wspierającymi przetwarzanie danych;

57) „tryb offline” oznacza – w odniesieniu do europejskich portfeli tożsamości cyfrowej – interakcję między użytkownikiem a stroną trzecią w fizycznej lokalizacji przy użyciu technologii zbliżeniowych, przy czym europejski portfel tożsamości cyfrowej nie musi mieć dostępu do systemów zdalnych za pośrednictwem sieci komunikacji elektronicznej do celów tej interakcji.

▼B

Artykuł 4

Zasada rynku wewnętrznego

1. Nie ogranicza się świadczenia usług zaufania na terytorium państwa członkowskiego przez dostawcę usług zaufania mającego siedzibę w innym państwie członkowskim z powodów związanych z dziedzinami objętymi niniejszym rozporządzeniem.

▼B

2. Produkty i usługi zaufania spełniające wymogi niniejszego rozporządzenia dopuszcza się do swobodnego obrotu na rynku wewnętrznym.

▼M1

Artykuł 5

Pseudonimy w transakcji elektronicznej

Bez uszczerbku dla szczegółowych przepisów prawa Unii lub prawa krajowego wymagających od użytkowników, aby zidentyfikowali się, lub dla skutku prawnego, jaki prawo krajowe przyznaje pseudonimom, nie zakazuje się używania pseudonimów wybranych przez użytkownika.

▼B

ROZDZIAŁ II

IDENTYFIKACJA ELEKTRONICZNA

▼M1

SEKCJA 1

europejski portfel tożsamości cyfrowej

Artykuł 5a

Europejskie portfele tożsamości cyfrowej

1. W celu zapewnienia wszystkim osobom fizycznym i prawnym w Unii bezpiecznego, zaufanego i niezakłóconego transgranicznego dostępu do usług publicznych i prywatnych, przy jednoczesnym zachowaniu pełnej kontroli nad ich danymi, każde państwo członkowskie zapewnia co najmniej jeden europejski portfel tożsamości cyfrowej w terminie 24 miesięcy od dnia wejścia w życie aktów wykonawczych, o których mowa w ust. 23 niniejszego artykułu i art. 5c ust. 6.

2. Europejskie portfele tożsamości cyfrowej muszą być zapewniane w co najmniej jeden z następujących sposobów:

a) bezpośrednio przez państwo członkowskie;

b) na podstawie upoważnienia od państwa członkowskiego;

c) niezależnie od państwa członkowskiego, lecz uznawane przez to państwo członkowskie.

3. Kod źródłowy komponentów oprogramowania użytkowego europejskich portfeli tożsamości cyfrowej musi być objęty licencją otwartego oprogramowania. Państwa członkowskie mogą postanowić, że z należycie uzasadnionych powodów nie ujawnia się kodu źródłowego poszczególnych komponentów innych niż zainstalowane na urządzeniach użytkownika.

4. Europejskie portfele tożsamości cyfrowej muszą umożliwiać użytkownikowi, w sposób przyjazny, przejrzysty i identyfikowalny dla użytkownika:

a) bezpieczne żądanie, otrzymywanie, wybieranie, łączenie, przechowywanie, usuwanie, udostępnianie i prezentację – pod wyłączną kontrolą użytkownika – danych identyfikujących osobę oraz, w stosownych przypadkach, w połączeniu z elektronicznymi poświadczeniami atrybutów, uwierzytelnianie wobec stron ufających w trybie online oraz, w stosownych przypadkach, w trybie offline, w celu uzyskania dostępu do usług publicznych i prywatnych, przy jednoczesnym zapewnieniu możliwości selektywnego ujawniania danych;

▼M1

b) generowanie pseudonimów i przechowywanie ich w zaszyfrowanej formie i lokalnie w europejskim portfelu tożsamości cyfrowej;

c) bezpieczne uwierzytelnianie europejskiego portfela tożsamości cyfrowej innej osoby oraz otrzymywanie i udostępnianie danych identyfikujących osobę i elektronicznych poświadczeń atrybutów w bezpieczny sposób między dwoma europejskimi portfelami tożsamości cyfrowej;

d) dostęp do rejestru wszystkich transakcji przeprowadzonych z wykorzystaniem europejskiego portfela tożsamości cyfrowej za pomocą wspólnego panelu zarządzania umożliwiającego użytkownikowi:

(i) przeglądanie aktualnej listy stron ufających, z którymi użytkownik ustanowił połączenie, oraz, w stosownych przypadkach, wszystkich udostępnionych danych;

(ii) łatwe zażądanie od strony ufającej usunięcia danych osobowych zgodnie z art. 17 rozporządzenia (UE) 2016/679;

(iii) łatwe zgłaszanie strony ufającej właściwemu krajowemu organowi ochrony danych, w przypadku otrzymania przypuszczalnie niezgodnego z prawem lub podejrzanego żądania udostępnienia danych;

e) składanie kwalifikowanych podpisów elektronicznych i kwalifikowanych pieczęci elektronicznych;

f) pobieranie, w zakresie, w jakim jest to technicznie wykonalne, danych użytkownika, elektronicznych poświadczeń atrybutów i konfiguracji;

g) korzystanie z praw użytkownika do przenoszenia danych.

5. Europejskie portfele tożsamości cyfrowej, w szczególności:

a) muszą być zgodne ze wspólnymi protokołami i interfejsami:

(i) do celów wydawania danych identyfikujących osobę, kwalifikowanych i niekwalifikowanych elektronicznych poświadczeń atrybutów lub kwalifikowanych i niekwalifikowanych certyfikatów do europejskiego portfela tożsamości cyfrowej;

(ii) na potrzeby stron ufających do celów żądania danych identyfikujących osobę i elektronicznych poświadczeń atrybutów oraz ich walidacji;

(iii) na potrzeby udostępniania i prezentacji stronom ufającym danych identyfikujących osobę, elektronicznych poświadczeń atrybutów lub selektywnie ujawnionych powiązanych danych w trybie online oraz, w stosownych przypadkach, w trybie offline;

(iv) aby umożliwić użytkownikowi interakcję z europejskim portfelem tożsamości cyfrowej oraz wyświetlenie unijnego znaku zaufania dla portfela tożsamości cyfrowej;

(v) na potrzeby bezpiecznej rejestracji użytkownika przy użyciu środka identyfikacji elektronicznej zgodnie z art. 5a ust. 24;

(vi) na potrzeby interakcji między europejskimi portfelami tożsamości cyfrowej dwóch osób do celów otrzymywania, walidowania oraz udostępniania danych identyfikujących osobę i elektronicznych poświadczeń atrybutów w bezpieczny sposób;

▼M1

(vii) na potrzeby uwierzytelnienia i identyfikacji stron ufających poprzez wdrożenie mechanizmów uwierzytelniania zgodnie z art. 5b;

(viii) na potrzeby stron ufających do celów weryfikowania autentyczności i ważności europejskich portfeli tożsamości cyfrowej;

(ix) na potrzeby zażądania od strony ufającej usunięcia danych osobowych zgodnie z art. 17 rozporządzenia (UE) 2016/679;

(x) na potrzeby zgłoszenia strony ufającej właściwemu krajowemu organowi ochrony danych w przypadku otrzymania przypuszczalnie niezgodnego z prawem lub podejrzanego żądania udostępnienia danych;

(xi) na potrzeby składania kwalifikowanych podpisów elektronicznych lub pieczęci elektronicznych za pomocą kwalifikowanych urządzeń do składania podpisów elektronicznych lub pieczęci elektronicznych;

b) nie mogą dostarczać dostawcom usług zaufania elektronicznych poświadczeń atrybutów jakichkolwiek informacji na temat wykorzystywania tych elektronicznych poświadczeń;

c) muszą zapewniać możliwość uwierzytelnienia i identyfikacji stron ufających poprzez wdrożenie mechanizmów uwierzytelniania zgodnie z art. 5b;

d) muszą spełniać wymogi określone w art. 8 w odniesieniu do wysokiego poziomu bezpieczeństwa, w szczególności w zakresie wymogów dotyczących potwierdzania i weryfikacji tożsamości, zarządzania środkami identyfikacji elektronicznej oraz uwierzytelniania;

e) w przypadku elektronicznego poświadczenia atrybutów z wbudowanymi regułami ujawniania – muszą wdrażać odpowiedni mechanizmu informowania użytkownika, że strona ufająca lub użytkownik europejskiego portfela tożsamości cyfrowej wnioskujący o udostępnienie tego elektronicznego poświadczenia atrybutów ma zezwolenie na dostęp do takiego poświadczenia;

f) muszą zapewniać, aby dane identyfikujące osobę, które są dostępne w systemie identyfikacji elektronicznej, w ramach którego zapewniany jest europejski portfel tożsamości cyfrowej, niepowtarzalnie reprezentowały osobę fizyczną, osobę prawną, lub osobę fizyczną reprezentującą osobę fizyczną lub prawną, oraz były powiązane z tym europejskim portfelem tożsamości cyfrowej;

g) muszą oferować wszystkim osobom fizycznym możliwości składania kwalifikowanych podpisów elektronicznych, domyślnie i nieodpłatnie.

Niezależnie od akapitu pierwszego lit. g) państwa członkowskie mogą przewidzieć proporcjonalne środki w celu zapewnienia, aby nieodpłatne używanie kwalifikowanych podpisów elektronicznych przez osoby fizyczne było ograniczone do celów innych niż profesjonalne.

6. Państwa członkowskie bez zbędnej zwłoki informują użytkowników o wszelkich naruszeniach bezpieczeństwa, które mogłyby spowodować całkowite lub częściowe skompromitowanie ich europejskich portfeli tożsamości cyfrowej lub zawartości tych portfeli, w szczególności jeżeli ich europejski portfel tożsamości cyfrowej został zawieszony lub unieważniony zgodnie z art. 5e.

▼M1

7. Bez uszczerbku dla art. 5f państwa członkowskie mogą przewidzieć, zgodnie z prawem krajowym, dodatkowe funkcje europejskich portfeli tożsamości cyfrowej, w tym interoperacyjność z istniejącymi krajowymi środkami identyfikacji elektronicznej. Te dodatkowe funkcje muszą być zgodne z niniejszym artykułem.

8. Państwa członkowskie zapewniają mechanizmy walidacji nieodpłatnie, aby:

a) zapewnić możliwość weryfikacji autentyczności i ważności europejskich portfeli tożsamości cyfrowej;

b) umożliwić użytkownikom weryfikację autentyczności i ważności tożsamości stron ufających zarejestrowanych zgodnie z art. 5b.

9. Państwa członkowskie zapewniają, aby europejski portfel tożsamości cyfrowej mógł zostać unieważniony w następujących przypadkach:

a) na wyraźne żądanie użytkownika;

b) w przypadku bezpieczeństwo europejskiego portfela tożsamości cyfrowej zostało skompromitowane;

c) po śmierci użytkownika lub zaprzestaniu działalności przez osobę prawną.

10. Dostawcy europejskich portfeli tożsamości cyfrowej muszą zapewniać użytkownikom możliwość łatwego zwracania się o wsparcie techniczne oraz zgłaszania problemów technicznych lub wszelkich innych incydentów mających negatywny wpływ na używanie europejskiego portfela tożsamości cyfrowej.

11. Europejskie portfele tożsamości cyfrowej zapewnia się w ramach systemu identyfikacji elektronicznej, na wysokim poziomie bezpieczeństwa.

12. Europejskie portfele tożsamości cyfrowej muszą zapewniać uwzględnianie bezpieczeństwa na etapie projektowania.

13. Wydawanie wykorzystywanie i unieważnianie europejskich portfeli tożsamości cyfrowej musi być nieodpłatne dla wszystkich osób fizycznych.

14. Użytkownicy muszą mieć pełną kontrolę nad używaniem swojego europejskiego portfela tożsamości cyfrowej oraz znajdujących się w nim danych. Dostawca europejskiego portfela tożsamości cyfrowej nie może gromadzić informacji na temat używania europejskiego portfela tożsamości cyfrowej, które nie są niezbędne do świadczenia usług europejskiego portfela tożsamości cyfrowej, ani łączyć danych identyfikujących osobę lub jakichkolwiek innych danych osobowych przechowywanych lub związanych z używaniem europejskiego portfela tożsamości cyfrowej z danymi osobowymi pochodzącymi z jakichkolwiek innych usług oferowanych przez tego dostawcę lub z usług osób trzecich, które nie są niezbędne do świadczenia usług europejskiego portfela tożsamości cyfrowej, chyba że użytkownik wyraźnie tego zażąda. Dane osobowe związane z dostarczaniem europejskiego portfela tożsamości cyfrowej muszą być logicznie oddzielone od wszelkich innych danych będących w posiadaniu dostawcy danego europejskiego portfela tożsamości cyfrowej. Jeżeli europejski portfel tożsamości cyfrowej jest dostarczany przez podmioty prywatne zgodnie z ust. 2 lit. b) i c) niniejszego artykułu, przepisy art. 45h ust. 3 stosuje się odpowiednio.

▼M1

15. Używanie europejskich portfeli tożsamości cyfrowej musi być dobrowolne. Osobom fizycznym i prawnym, które nie korzystają z europejskich portfeli tożsamości cyfrowej, nie można w żaden sposób ograniczać ani utrudniać dostępu do usług publicznych i prywatnych, dostępu do rynku pracy i swobody prowadzenia działalności gospodarczej. Nadal musi być możliwy dostęp do usług publicznych i prywatnych za pomocą innych istniejących środków identyfikacji i uwierzytelniania.

16. Ramy techniczne europejskiego portfela tożsamości cyfrowej:

a) nie mogą zezwalać dostawcom elektronicznych poświadczeń atrybutów lub jakiejkolwiek innej stronie, po wydaniu poświadczenia atrybutów, na uzyskanie danych umożliwiających śledzenie, przyporządkowanie lub skorelowanie transakcji lub zachowań użytkowników, lub uzyskanie w inny sposób wiedzy na temat transakcji lub zachowań użytkowników, chyba że użytkownik wyraźnie wyrazi na to zgodę;

b) muszą umożliwiać stosowanie technik ochrony prywatności, które – w przypadku gdy poświadczenie atrybutów nie wymaga identyfikacji użytkownika – zapewniają uniemożliwienie powiązania tożsamości użytkownika z tym poświadczeniem.

17. Wszelkie przetwarzanie danych osobowych przez państwa członkowskie lub w ich imieniu przez podmioty lub strony odpowiedzialne za dostarczenie europejskich portfeli tożsamości cyfrowej jako środka identyfikacji elektronicznej musi odbywać się zgodnie z odpowiednimi i skutecznymi środkami ochrony danych. Zgodność takiego przetwarzania z rozporządzeniem (UE) 2016/679 musi zostać wykazana. Państwa członkowskie mogą wprowadzić przepisy krajowe w celu doprecyzowania stosowania takich środków.

18. Państwa członkowskie bez zbędnej zwłoki przekazują Komisji informacje dotyczące:

a) podmiotu odpowiedzialnego za sporządzenie i prowadzenie wykazu zarejestrowanych stron ufających, które polegają na europejskich portfelach tożsamości cyfrowej zgodnie z art. 5b ust. 5, oraz informacje o miejscu dostępności tego wykazu;

b) podmiotów odpowiedzialnych za dostarczenie europejskich portfeli tożsamości cyfrowej zgodnie z art. 5a ust. 1;

c) podmiotów odpowiedzialnych za zapewnienie powiązania danych identyfikujących osobę z europejskim portfelem tożsamości cyfrowej zgodnie z art. 5a ust. 5 lit. f);

d) mechanizmu umożliwiającego walidację danych identyfikujących osobę, o których mowa w art. 5a ust. 5 lit. f), oraz walidację tożsamości stron ufających;

e) mechanizmu walidacji autentyczności i ważności europejskich portfeli tożsamości cyfrowej.

Komisja – przy użyciu zabezpieczonego kanału komunikacji – udostępnia publicznie informacje przekazane zgodnie z akapitem pierwszym, w postaci pozwalającej na automatyczne przetwarzanie, elektronicznie podpisane lub opatrzone pieczęcią elektroniczną.

▼M1

19. Bez uszczerbku dla ust. 22 niniejszego artykułu, art. 11 stosuje się odpowiednio do europejskiego portfela tożsamości cyfrowej.

20. Art. 24 ust. 2 lit. b) oraz lit. d) – h) stosuje się odpowiednio do dostawców europejskich portfeli tożsamości cyfrowej.

21. Europejskie portfele tożsamości cyfrowej udostępnia się do użytku osobom z niepełnosprawnościami na równi z innymi użytkownikami zgodnie z dyrektywą Parlamentu Europejskiego i Rady (UE) 2019/882 ([1]).

22. Do celów zapewniania europejskich portfeli tożsamości cyfrowej, europejskie portfele tożsamości cyfrowej i systemy identyfikacji elektronicznej, w ramach których są one zapewniane, nie podlegają wymogom określonym w art. 7, 9, 10, 12 i 12a.

23. Do dnia 21 listopada 2024 r. Komisja, w drodze aktów wykonawczych, sporządzi wykaz norm referencyjnych oraz, w razie potrzeby, ustanowi specyfikacje i procedury w odniesieniu do wymogów, o których mowa w ust. 4, 5, 8 i 18 niniejszego artykułu, dotyczących wdrożenia europejskich portfeli tożsamości cyfrowej. Te akty wykonawcze przyjmuje się zgodnie z procedurą sprawdzającą, o której mowa w art. 48 ust. 2.

24. Komisja, w drodze aktów wykonawczych, sporządza wykaz norm referencyjnych oraz, w razie potrzeby, ustanawia specyfikacje i procedury w celu ułatwienia rejestracji użytkowników w europejskim portfelu tożsamości cyfrowej za pomocą środków identyfikacji elektronicznej zgodnych z wysokim poziomem bezpieczeństwa albo środków identyfikacji elektronicznej zgodnych ze średnim poziomem bezpieczeństwa, w połączeniu z dodatkowymi procedurami zdalnej rejestracji, które łącznie spełniają wymogi dotyczące wysokiego poziomu bezpieczeństwa. Te akty wykonawcze przyjmuje się zgodnie z procedurą sprawdzającą, o której mowa w art. 48 ust. 2.

Artykuł 5b

Strony ufające europejskich portfeli tożsamości cyfrowej

1. W przypadku gdy strona ufająca zamierza polegać na europejskich portfelach tożsamości cyfrowej na potrzeby świadczenia usług publicznych lub prywatnych za pośrednictwem cyfrowej interakcji, strona ufająca rejestruje się w państwie członkowskim, w którym ma siedzibę.

2. Proces rejestracji musi być efektywny kosztowo i proporcjonalny względem zagrożeń. Strona ufająca przekazuje co najmniej:

a) informacje niezbędne do uwierzytelnienia w europejskich portfelach tożsamości cyfrowej, które obejmują co najmniej:

   (i) państwo członkowskie, w którym strona ufająca ma siedzibę; oraz

([1]) Dyrektywa Parlamentu Europejskiego i Rady (UE) 2019/882 z dnia 17 kwietnia 2019 r. w sprawie wymogów dostępności produktów i usług (Dz.U. L 151 z 7.6.2019, s. 70).

▼M1

(ii) nazwę strony ufającej oraz, w stosownych przypadkach, jej numer rejestrowy podany zgodnie z oficjalnym rejestrem wraz z danymi identyfikacyjnymi zawartymi w tym oficjalnym rejestrze;

b) dane kontaktowe strony ufającej;

c) zamierzone używanie europejskich portfeli tożsamości cyfrowej, w tym wskazanie danych, o które strona ufająca będzie zwracać się do użytkowników.

3. Strony ufające nie mogą zwracać się do użytkowników o udostępnienie jakichkolwiek danych innych niż te, które zostały wskazane zgodnie z ust. 2 lit. c).

4. Ust. 1 i 2 pozostają bez uszczerbku dla prawa Unii lub prawa krajowego mającego zastosowanie do świadczenia określonych usług.

5. Państwa członkowskie udostępniają publicznie informacje, o których mowa w ust. 2, online, w postaci pozwalającej na automatyczne przetwarzanie, elektronicznie podpisane lub opatrzone pieczęcią elektroniczną.

6. Strony ufające zarejestrowane zgodnie z niniejszym artykułem niezwłocznie informują państwa członkowskie o wszelkich zmianach w informacjach przekazanych w ramach rejestracji zgodnie z ust. 2.

7. Państwa członkowskie zapewniają wspólny mechanizm umożliwiający identyfikację i uwierzytelnianie stron ufających, o którym mowa w art. 5a ust. 5 lit. c).

8. W przypadku gdy strony ufające zamierzają polegać na europejskich portfelach tożsamości cyfrowej, muszą potwierdzić swoją tożsamość wobec użytkownika.

9. Strony ufające odpowiedzialne są za przeprowadzenie procedury uwierzytelniania i walidacji danych identyfikujących osobę oraz elektronicznego poświadczenia atrybutów żądanych z europejskich portfeli tożsamości cyfrowej. Strony ufające nie mogą odmówić używania pseudonimów, w przypadkach gdy identyfikacja użytkownika nie jest wymagana na podstawie prawa Unii lub prawa krajowego.

10. Pośrednicy działający w imieniu stron ufających uznawani są za strony ufające i nie mogą przechowywać danych na temat treści transakcji.

11. Do dnia 21 listopada 2024 r. Komisja ustanowi specyfikacje techniczne i procedury w odniesieniu do wymogów, o których mowa w ust. 2, 5 i 6–9 niniejszego artykułu, w drodze aktów wykonawczych dotyczących wdrożenia europejskich portfeli tożsamości cyfrowej, o których mowa w art. 5a ust. 23. Te akty wykonawcze przyjmuje się zgodnie z procedurą sprawdzającą, o której mowa w art. 48 ust. 2.

Artykuł 5c

Certyfikacja europejskich portfeli tożsamości cyfrowej

1. Zgodność europejskich portfeli tożsamości cyfrowej i systemu identyfikacji elektronicznej, w ramach którego są one zapewniane, z wymogami określonymi w art. 5a ust. 4, 5 i 8, z wymogiem dotyczącym logicznego oddzielenia określonym w art. 5a ust. 14 oraz, w stosownych przypadkach, z normami i specyfikacjami technicznymi, o których mowa w art. 5a ust. 24, musi być certyfikowana przez jednostki oceniające zgodność wyznaczone przez państwa członkowskie.

▼M1

2. Certyfikację zgodności europejskich portfeli tożsamości cyfrowej lub ich części z wymogami, o których mowa w ust. 1 niniejszego artykułu, które są związane z cyberbezpieczeństwem, przeprowadza się zgodnie z europejskimi programami certyfikacji cyberbezpieczeństwa przyjętymi na podstawie rozporządzenia Parlamentu Europejskiego i Rady (UE) 2019/881 ([1]) oraz wymienionymi w aktach wykonawczych, o których mowa w ust. 6 niniejszego artykułu.

3. W odniesieniu do wymogów, o których mowa w ust. 1 niniejszego artykułu, które nie są związane z cyberbezpieczeństwem, oraz w odniesieniu do wymogów, o których mowa w ust. 1 niniejszego artykułu, które są związane z cyberbezpieczeństwem, w zakresie, w jakim programy certyfikacji cyberbezpieczeństwa, o których mowa w ust. 2 niniejszego artykułu, nie obejmują tych wymogów dotyczących cyberbezpieczeństwa lub obejmują je tylko częściowo, również w odniesieniu do tych wymogów, państwa członkowskie ustanawiają krajowe programy certyfikacji zgodnie z wymogami określonymi w aktach wykonawczych, o których mowa w ust. 6 niniejszego artykułu. Państwa członkowskie przekazują swoje projekty krajowych programów certyfikacji Grupie Współpracy na rzecz Europejskiej Tożsamości Cyfrowej ustanowionej na podstawie art. 46e ust. 1 (zwanej dalej „grupą współpracy”). Grupa współpracy może wydawać opinie i zalecenia.

4. Certyfikacja zgodna z ust. 1 ważna jest przez okres do pięciu lat, pod warunkiem że co dwa lata przeprowadza się ocenę podatności na zagrożenia. W przypadku gdy zostanie stwierdzona podatność na zagrożenia i nie zostanie ona terminowo wyeliminowana, certyfikacja zostaje odwołana.

5. Spełnienie wymogów określonych w art. 5a niniejszego rozporządzenia związanych z operacjami przetwarzania danych osobowych może zostać certyfikowane na podstawie rozporządzenia (UE) 2016/679.

6. Do dnia 21 listopada 2024 r. Komisja, w drodze aktów wykonawczych, sporządzi wykaz norm referencyjnych oraz, w razie potrzeby, ustanowi specyfikacje i procedury do celów certyfikacji europejskich portfeli tożsamości cyfrowej, o której mowa w ust. 1, 2 i 3 niniejszego artykułu. Te akty wykonawcze przyjmuje się zgodnie z procedurą sprawdzającą, o której mowa w art. 48 ust. 2.

7. Państwa członkowskie przekazują Komisji nazwy i adresy jednostek oceniających zgodność, o których mowa w ust. 1. Komisja udostępnia te informacje wszystkim państwom członkowskim.

8. Komisja jest uprawniona do przyjmowania aktów delegowanych, zgodnie z art. 47, ustanawiających szczególne kryteria, które mają spełniać wyznaczone jednostki oceniające zgodność, o których mowa w ust. 1 niniejszego artykułu.

([1]) Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2019/881 z dnia 17 kwietnia 2019 r. w sprawie ENISA (Agencji Unii Europejskiej ds. Cyberbezpieczeństwa) oraz certyfikacji cyberbezpieczeństwa w zakresie technologii informacyjno-komunikacyjnych oraz uchylenia rozporządzenia (UE) nr 526/2013 (akt o cyberbezpieczeństwie) (Dz.U. L 151 z 7.6.2019, s. 15).

▼M1

Artykuł 5d

Publikacja wykazu certyfikowanych europejskich portfeli tożsamości cyfrowej

1. Państwa członkowskie bez zbędnej zwłoki informują Komisję oraz grupę współpracy ustanowioną na podstawie art. 46e ust. 1 o europejskich portfelach tożsamości cyfrowej, które zostały zapewnione zgodnie z art. 5a i certyfikowane przez jednostki oceniające zgodność, o których mowa w art. 5c ust. 1. Państwa członkowskie informują Komisję oraz grupę współpracy ustanowioną na podstawie art. 46e ust. 1 bez zbędnej zwłoki o odwołaniu certyfikacji oraz podają przyczyny odwołania.

2. Bez uszczerbku dla art. 5a ust. 18 informacje przekazywane przez państwa członkowskie zgodnie z ust. 1 niniejszego artykułu obejmują co najmniej:

a) certyfikat i sprawozdanie z oceny certyfikacji certyfikowanego europejskiego portfela tożsamości cyfrowej;

b) opis systemu identyfikacji elektronicznej, w ramach którego zapewniany jest europejski portfel tożsamości cyfrowej;

c) mający zastosowanie system nadzoru oraz informacje na temat systemu odpowiedzialności w odniesieniu do strony dostarczającej europejski portfel tożsamości cyfrowej;

d) organ lub organy odpowiedzialne za system identyfikacji elektronicznej;

e) ustalenia dotyczące zawieszania lub unieważniania systemu identyfikacji elektronicznej lub uwierzytelnienia lub ich skompromitowanych części.

3. Na podstawie informacji otrzymanych zgodnie z ust. 1 Komisja ustanawia, publikuje w *Dzienniku Urzędowym Unii Europejskiej* oraz prowadzi w formie nadającej się do odczytu maszynowego wykaz certyfikowanych europejskich portfeli tożsamości cyfrowej.

4. Państwo członkowskie może przedłożyć Komisji wniosek o usunięcie z wykazu, o którym mowa w ust. 3, europejskiego portfela tożsamości cyfrowej i systemu identyfikacji elektronicznej, w ramach którego portfel ten jest zapewniany.

5. W przypadku zmian w informacjach przekazanych zgodnie z ust. 1 państwo członkowskie przekazuje Komisji zaktualizowane informacje.

6. Komisja aktualizuje wykaz, o którym mowa w ust. 3, publikując w *Dzienniku Urzędowym Unii Europejskiej* odpowiednie zmiany w wykazie w terminie miesiąca od otrzymania wniosku zgodnie z ust. 4 lub zaktualizowanych informacji zgodnie z ust. 5.

7. Do dnia 21 listopada 2024 r. Komisja ustanowi formaty i procedury mające zastosowanie do celów ust. 1, 4 i 5 niniejszego artykułu, w drodze aktów wykonawczych dotyczących wdrożenia europejskich portfeli tożsamości cyfrowej, o którym mowa w art. 5a ust. 23. Te akty wykonawcze przyjmuje się zgodnie z procedurą sprawdzającą, o której mowa w art. 48 ust. 2.

▼M1

Artykuł 5e

Naruszenie bezpieczeństwa europejskich portfeli tożsamości cyfrowej

1. W przypadku naruszenia lub częściowej kompromitacji europejskich portfeli tożsamości cyfrowej zapewnianych zgodnie z art. 5a, mechanizmów walidacji, o których mowa w art. 5a ust. 8, lub systemu identyfikacji elektronicznej, w ramach którego te europejskie portfele tożsamości cyfrowej są zapewniane, w sposób, który wpływa na ich wiarygodność lub na wiarygodność innych europejskich portfeli tożsamości cyfrowej, państwo członkowskie, które zapewniło dane europejskie portfele tożsamości cyfrowej, bez zbędnej zwłoki zawiesza zapewnianie i używanie europejskich portfeli tożsamości cyfrowej.

W przypadku gdy jest to uzasadnione wagą naruszenia bezpieczeństwa lub kompromitacji, o których mowa w akapicie pierwszym, państwo członkowskie bez zbędnej zwłoki wycofuje europejskie portfele tożsamości cyfrowej.

Państwo członkowskie informuje użytkowników, których to dotyczy, pojedyncze punkty kontaktowe wyznaczone zgodnie z art. 46c ust. 1, strony ufające oraz Komisję.

2. Jeżeli naruszenie bezpieczeństwa lub kompromitacja, o których mowa w ust. 1 akapit pierwszy niniejszego artykułu, nie zostaną wyeliminowane w terminie trzech miesięcy od zawieszenia, państwo członkowskie, które zapewniło europejskie portfele tożsamości cyfrowej, wycofuje europejskie portfele tożsamości cyfrowej i je unieważnia. Państwo członkowskie informuje o tym wycofaniu użytkowników, których to dotyczy, pojedyncze punkty kontaktowe wyznaczone zgodnie z art. 46c ust. 1, strony ufające oraz Komisję.

3. W przypadku gdy naruszenie bezpieczeństwa lub kompromitacja, o których mowa w akapicie pierwszym niniejszego artykułu, zostaną wyeliminowane, zapewniające państwo członkowskie przywraca zapewnianie i używanie europejskich portfeli tożsamości cyfrowej oraz informuje o tym bez zbędnej zwłoki użytkowników, których to dotyczy, strony ufające, pojedyncze punkty kontaktowe wyznaczone zgodnie z art. 46c ust. 1 oraz Komisję.

4. Komisja bez zbędnej zwłoki publikuje w *Dzienniku Urzędowym Unii Europejskiej* odpowiednie zmiany w wykazie, o którym mowa w art. 5d.

5. Do dnia 21 listopada 2024 r. Komisja, w drodze aktów wykonawczych, ustanowi wykaz norm referencyjnych oraz, w razie potrzeby, ustanowi specyfikacje i procedury do celów środków, o których mowa w ust. 1, 2 i 3 niniejszego artykułu. Te akty wykonawcze przyjmuje się zgodnie z procedurą sprawdzającą, o której mowa w art. 48 ust. 2.

Artykuł 5f

Transgraniczne poleganie na europejskich portfelach tożsamości cyfrowej

1. W przypadku gdy państwa członkowskie wymagają identyfikacji elektronicznej oraz uwierzytelnienia w celu dostępu do usługi online świadczonej przez podmiot sektora publicznego, akceptują również europejskie portfele tożsamości cyfrowej, które są zapewniane zgodnie z niniejszym rozporządzeniem.

▼M1

2. W przypadku gdy prywatne strony ufające, które świadczą usługi – z wyjątkiem mikroprzedsiębiorstw i małych przedsiębiorstw zdefiniowanych w art. 2 załącznika do zalecenia Komisji 2003/361/WE ([1])– zobowiązane są na podstawie prawa Unii lub prawa krajowego do stosowania silnego uwierzytelnienia użytkownika do celów identyfikacji elektronicznej lub w przypadku gdy silne uwierzytelnienie użytkownika do celów identyfikacji elektronicznej wymagane jest na podstawie zobowiązania umownego, w tym w obszarach transportu, energii, bankowości, usług finansowych, zabezpieczenia społecznego, zdrowia, wody pitnej, usług pocztowych, infrastruktury cyfrowej, edukacji lub telekomunikacji, te prywatne strony ufające, nie później niż 36 miesięcy od dnia wejścia w życie aktów wykonawczych, o których mowa w art. 5a ust. 23 i art. 5c ust. 6, oraz wyłącznie na dobrowolny wniosek użytkownika, również akceptują europejskie portfele tożsamości cyfrowej, które są zapewniane zgodnie z niniejszym rozporządzeniem.

3. W przypadku gdy dostawcy bardzo dużych platform internetowych, o których mowa w art. 33 rozporządzenia Parlamentu Europejskiego i Rady (UE) 2022/2065 ([2]), wymagają uwierzytelniania użytkownika do celów dostępu do usług online, akceptują i ułatwiają oni również używanie europejskich portfeli tożsamości cyfrowej, które są zapewniane zgodnie z niniejszym rozporządzeniem, do celów uwierzytelnienia użytkownika, wyłącznie na dobrowolny wniosek użytkownika oraz w odniesieniu do minimalnych danych niezbędnych do celów konkretnej usługi online, która wymaga uwierzytelnienia użytkownika.

4. We współpracy z państwami członkowskimi Komisja ułatwia opracowywanie kodeksów postępowania, w ścisłej współpracy ze wszystkimi odpowiednimi zainteresowanymi stronami, w tym ze społeczeństwem obywatelskim, aby przyczynić się do szerokiej dostępności i użyteczności europejskich portfeli tożsamości cyfrowej objętych zakresem stosowania niniejszego rozporządzenia, oraz zachęcać dostawców usług do ukończenia opracowywania kodeksów postępowania.

5. W terminie 24 miesięcy po wprowadzeniu europejskich portfeli tożsamości cyfrowej Komisja dokonuje oceny popytu na europejskie portfele tożsamości cyfrowej oraz ich dostępności i użyteczność, biorąc pod uwagę kryteria takie jak rozpowszechnienie wśród użytkowników, transgraniczna obecność dostawców usług, rozwój technologiczny, zmiany sposobów użytkowania oraz popyt ze strony konsumentów.

▼M1

SEKCJA 2

systemy identyfikacji elektronicznej

▼B

Artykuł 6

Wzajemne uznawanie

1. Jeżeli zgodnie z prawem krajowym lub zgodnie z krajową praktyką administracyjną dostęp do usługi *online* świadczonej przez podmiot sektora publicznego w jednym państwie członkowskim

([1]) Zalecenie Komisji 2003/361/WE z dnia 6 maja 2003 r. w sprawie definicji mikroprzedsiębiorstw oraz małych i średnich przedsiębiorstw (Dz.U. L 124 z 20.5.2003, s. 36).

([2]) Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2022/2065 z dnia 19 października 2022 r. w sprawie jednolitego rynku usług cyfrowych oraz zmiany dyrektywy 2000/31/WE (akt o usługach cyfrowych) (Dz.U. L 277 z 27.10.2022, s. 1).

▼B

wymaga identyfikacji elektronicznej przy użyciu środka identyfikacji elektronicznej oraz uwierzytelnienia, w tym pierwszym państwie członkowskim na potrzeby transgranicznego uwierzytelnienia dla tej usługi *online* uznaje się środek identyfikacji elektronicznej wydany w innym państwie członkowskim, pod warunkiem że spełnione są następujące warunki:

a) środek identyfikacji elektronicznej jest wydany w ramach systemu identyfikacji elektronicznej wymienionego w wykazie publikowanym przez Komisję na podstawie art. 9;

b) poziom bezpieczeństwa środka identyfikacji elektronicznej odpowiada poziomowi bezpieczeństwa równemu lub wyższemu od poziomu bezpieczeństwa wymaganego przez odpowiedni podmiot sektora publicznego na potrzeby dostępu do tej usługi *online* w pierwszym państwie członkowskim, pod warunkiem że poziom bezpieczeństwa tego środka identyfikacji elektronicznej odpowiada średniemu lub wysokiemu poziomowi bezpieczeństwa;

c) odpowiedni podmiot sektora publicznego korzysta ze średniego lub wysokiego poziomu bezpieczeństwa w odniesieniu do dostępu do tej usługi *online*.

Takiego uznania dokonuje się nie później niż 12 miesięcy po opublikowaniu przez Komisję wykazu, o którym mowa w akapicie pierwszym lit. a).

2. Środek identyfikacji elektronicznej, który jest wydawany w ramach systemu identyfikacji elektronicznej wymienionego w wykazie publikowanym przez Komisję na podstawie art. 9 i który odpowiada niskiemu poziomowi bezpieczeństwa, może być uznany przez podmioty sektora publicznego na potrzeby transgranicznego uwierzytelniania dla usługi *online* świadczonej przez te podmioty.

Artykuł 7

Systemy identyfikacji elektronicznej kwalifikujące się do notyfikowania

System identyfikacji elektronicznej kwalifikuje się do notyfikowania na podstawie art. 9 ust. 1, jeżeli spełnione zostaną wszystkie następujące warunki:

a) środki identyfikacji elektronicznej w ramach systemu identyfikacji elektronicznej są wydawane:

   (i) przez notyfikujące państwo członkowskie;

   (ii) na mocy upoważnienia od notyfikującego państwa członkowskiego; lub

   (iii) niezależnie od notyfikującego państwa członkowskiego i są uznawane przez to państwo członkowskie;

b) środki identyfikacji elektronicznej w ramach systemu identyfikacji elektronicznej mogą być używane w celu uzyskania dostępu do co najmniej jednej usługi świadczonej przez podmiot sektora publicznego, wymagającej identyfikacji elektronicznej w notyfikującym państwie członkowskim;

c) system identyfikacji elektronicznej i środki identyfikacji elektronicznej wydane w jego ramach spełniają wymogi co najmniej jednego z poziomów bezpieczeństwa określonych w akcie wykonawczym, o którym mowa w art. 8 ust. 3;

▼B

d) notyfikujące państwo członkowskie zapewnia, aby dane identyfikujące osobę unikalnie reprezentujące daną osobę przyporządkowane były – zgodnie z technicznymi specyfikacjami, standardami i procedurami dotyczącymi odpowiedniego poziomu bezpieczeństwa określonego w akcie wykonawczym, o którym mowa w art. 8 ust. 3 – osobie fizycznej lub prawnej, o której mowa w art. 3 pkt 1, w momencie wydania środka identyfikacji elektronicznej w ramach tego systemu;

e) strona wydająca środek identyfikacji elektronicznej w ramach tego systemu zapewnia, aby środek identyfikacji elektronicznej był przyporządkowany osobie, o której mowa w lit. d) niniejszego artykułu, zgodnie z technicznymi specyfikacjami, standardami i procedurami dotyczącymi odpowiedniego poziomu bezpieczeństwa określonego w akcie wykonawczym, o którym mowa w art. 8 ust. 3;

f) notyfikujące państwo członkowskie zapewnia dostępność uwierzytelniania *online*, tak aby każda strona ufająca mająca siedzibę na terytorium innego państwa członkowskiego mogła potwierdzić dane identyfikujące osobę otrzymane w postaci elektronicznej.

W odniesieniu do stron ufających innych niż podmioty sektora publicznego notyfikujące państwo członkowskie może określić warunki dostępu do tego uwierzytelnienia. Transgraniczne uwierzytelnienie jest świadczone bezpłatnie, gdy jest ono dokonywane w powiązaniu z usługą *online* świadczoną przez podmiot sektora publicznego.

Państwa członkowskie nie nakładają żadnych specjalnych niewspółmiernych wymogów technicznych na strony ufające, które zamierzają dokonać takiego uwierzytelnienia, w przypadku gdyby takie wymogi miały uniemożliwić lub znacznie utrudnić interoperacyjność notyfikowanych systemów identyfikacji elektronicznej;

▼M1

g) co najmniej sześć miesięcy przed notyfikacją na podstawie art. 9 ust. 1 notyfikujące państwo członkowskie przekazuje pozostałym państwom członkowskim, do celów art. 12 ust. 5, opis tego systemu zgodnie z warunkami proceduralnymi ustanowionymi w aktach wykonawczych przyjętych zgodnie z art. 12 ust. 6;

▼B

h) system identyfikacji elektronicznej spełnia wymogi określone w akcie wykonawczym, o którym mowa w art. 12 ust. 8.

Artykuł 8

Poziomy bezpieczeństwa systemów identyfikacji elektronicznej

1. System identyfikacji elektronicznej notyfikowany na podstawie art. 9 ust. 1 określa niski, średni lub wysoki poziom bezpieczeństwa w odniesieniu do środka identyfikacji elektronicznej wydanego w ramach tego systemu.

2. Niski, średni i wysoki poziom bezpieczeństwa oznaczają spełnienie, odpowiednio, następujących kryteriów:

▼B

a) niski poziom bezpieczeństwa odnosi się w kontekście systemu identyfikacji elektronicznej do środka identyfikacji elektronicznej, który zapewnia ograniczony stopień zaufania względem podawanej lub zgłaszanej tożsamości danej osoby i jest charakteryzowany w odniesieniu do technicznych specyfikacji, standardów i procedur powiązanych z nim, w tym zabezpieczeń technicznych, których celem jest obniżenie ryzyka podszycia się lub modyfikacji tożsamości;

b) średni poziom bezpieczeństwa odnosi się w kontekście systemu identyfikacji elektronicznej do środka identyfikacji elektronicznej, który zapewnia średni stopień zaufania względem podawanej lub zgłaszanej tożsamości danej osoby i jest charakteryzowany w odniesieniu do technicznych specyfikacji, standardów i procedur powiązanych z nim, w tym zabezpieczeń technicznych, których celem jest znaczne obniżenie ryzyka podszycia się lub modyfikacji tożsamości;

c) wysoki poziom bezpieczeństwa odnosi się w kontekście systemu identyfikacji elektronicznej do środka identyfikacji elektronicznej, który zapewnia wyższy stopień zaufania względem podawanej lub zgłaszanej tożsamości danej osoby niż środek identyfikacji elektronicznej o średnim poziomie pewności i jest charakteryzowany w odniesieniu do technicznych specyfikacji, standardów i procedur powiązanych z nim, w tym zabezpieczeń technicznych, których celem jest zapobieganie podszyciu się lub modyfikacji tożsamości.

▼M1

3. Do dnia 18 września 2015 r., uwzględniając odpowiednie normy międzynarodowe oraz z zastrzeżeniem ust. 2, Komisja określi, w drodze aktów wykonawczych, minimalne techniczne specyfikacje, normy i procedury, w odniesieniu do których określone zostaną niski, średni i wysoki poziom bezpieczeństwa dla środka identyfikacji elektronicznej.;

▼B

Te minimalne techniczne specyfikacje, standardy i procedury są określane przez odniesienie do wiarygodności i jakości następujących elementów:

a) procedury wykazującej i weryfikującej tożsamość osób fizycznych lub prawnych wnioskujących o wydanie środka identyfikacji elektronicznej;

b) procedury wydawania wnioskowanego środka identyfikacji elektronicznej;

c) mechanizmu uwierzytelniania, w którym osoba fizyczna lub prawna używa środka identyfikacji elektronicznej do potwierdzenia swojej tożsamości wobec strony ufającej;

d) jednostki wydającej środek identyfikacji elektronicznej;

e) każdego innego organu zaangażowanego w ramach wniosku o wydanie środka identyfikacji elektronicznej; oraz

f) specyfikacji technicznych i specyfikacji bezpieczeństwa wydanego środka identyfikacji elektronicznej.

Te akty wykonawcze przyjmuje się zgodnie z procedurą sprawdzającą, o której mowa w art. 48 ust. 2.

▼B

Artykuł 9

Notyfikacja

1. Notyfikujące państwo członkowskie notyfikuje Komisji następujące informacje i, bez zbędnej zwłoki, wszelkie późniejsze w nich zmiany:

a) opis systemu identyfikacji elektronicznej, w tym jego poziomy bezpieczeństwa oraz wydawcę lub wydawców środków identyfikacji elektronicznej w ramach tego systemu;

b) mający zastosowanie system nadzoru i informacje na temat systemu odpowiedzialności w odniesieniu do następujących stron:

(i) strony wydającej środki identyfikacji elektronicznej; oraz

(ii) strony przeprowadzającej procedurę uwierzytelniania;

c) organ lub organy odpowiedzialne za system identyfikacji elektronicznej;

d) informacje na temat jednostki lub jednostek, które zarządzają rejestracją unikalnych danych identyfikujących osobę;

e) opis sposobu spełnienia wymogów określonych w aktach wykonawczych, o których mowa w art. 12 ust. 8;

f) opis uwierzytelnienia, o którym mowa w art. 7 lit. f);

g) ustalenia dotyczące zawieszania lub unieważniania notyfikowanego systemu identyfikacji elektronicznej lub uwierzytelnienia lub też ich skompromitowanych części.

▼M1

2. Komisja bez zbędnej zwłoki publikuje w *Dzienniku Urzędowym Unii Europejskiej* wykaz systemów identyfikacji elektronicznej, które zostały notyfikowane zgodnie z ust. 1, wraz z podstawowymi informacjami na temat tych systemów.

3. Komisja publikuje w *Dzienniku Urzędowym Unii Europejskiej* zmiany w wykazie, o którym mowa w ust. 2, w terminie miesiąca od dnia otrzymania notyfikacji.

▼B

4. Państwo członkowskie może przekazać Komisji wniosek o usunięcie z wykazu, o którym mowa w ust. 2, systemu identyfikacji elektronicznej notyfikowanego przez to państwo członkowskie. Komisja publikuje w *Dzienniku Urzędowym Unii Europejskiej* odpowiednie zmiany w wykazie w terminie jednego miesiąca od daty otrzymania wniosku państwa członkowskiego.

▼B

5. Komisja może w drodze aktów wykonawczych określić okoliczności, formaty i procedury dotyczące notyfikacji określonej w ust. 1. Te akty wykonawcze przyjmuje się zgodnie z procedurą sprawdzającą, o której mowa w art. 48 ust. 2.

Artykuł 10

▼M1

Naruszenie bezpieczeństwa systemów identyfikacji elektronicznej

▼B

1. W przypadku gdy nastąpi naruszenie lub częściowa kompromitacja systemu identyfikacji elektronicznej notyfikowanego na podstawie art. 9 ust. 1, albo uwierzytelnienia, o którym mowa w art. 7 lit. f), mające wpływ na wiarygodność transgranicznego uwierzytelnienia tego systemu, notyfikujące państwo członkowskie bezzwłocznie zawiesza lub unieważnia to transgraniczne uwierzytelnianie lub dane skompromitowane części oraz powiadamia o tym pozostałe państwa członkowskie i Komisję.

2. W przypadku gdy naruszenie lub kompromitacja, o których mowa w ust. 1, zostanie wyeliminowane, notyfikujące państwo członkowskie przywraca transgraniczne uwierzytelnianie i bez zbędnej zwłoki powiadamia o tym pozostałe państwa członkowskie i Komisję.

3. Jeżeli naruszenie lub kompromitacja, o których mowa w ust. 1, nie zostanie wyeliminowane w ciągu trzech miesięcy od zawieszenia lub unieważnienia, notyfikujące państwo członkowskie powiadamia pozostałe państwa członkowskie i Komisję o wycofaniu systemu identyfikacji elektronicznej.

Komisja bez zbędnej zwłoki publikuje w *Dzienniku Urzędowym Unii Europejskiej* odpowiednie zmiany w wykazie, o którym mowa w art. 9 ust. 2.

Artykuł 11

Odpowiedzialność

1. Notyfikujące państwo członkowskie jest odpowiedzialne za szkody wyrządzone, w sposób zamierzony lub z powodu zaniedbania, osobie fizycznej lub prawnej w związku z niewypełnieniem swoich obowiązków na mocy art. 7 lit. d) i f), w ramach transgranicznej transakcji.

2. Strona wydająca środek identyfikacji elektronicznej jest odpowiedzialna za szkody wyrządzone, w sposób zamierzony lub z powodu zaniedbania, osobie fizycznej lub prawnej w związku z niewypełnieniem obowiązku, o którym mowa w art. 7 lit. e), w ramach transgranicznej transakcji.

3. Strona przeprowadzająca procedurę uwierzytelniania jest odpowiedzialna za szkody wyrządzone, w sposób zamierzony lub z powodu zaniedbania, osobie fizycznej lub prawnej w związku z niezapewnieniem poprawnego przebiegu uwierzytelniania, o którym mowa w art. 7 lit. f), w ramach transgranicznej transakcji.

4. Ust. 1, 2 i 3 mają zastosowanie zgodnie z krajowymi przepisami dotyczącymi odpowiedzialności.

▼B

5. Ust. 1, 2 i 3 pozostają bez uszczerbku dla odpowiedzialności, na mocy prawa krajowego właściwego dla stron transakcji, na potrzeby której zastosowano środki identyfikacji elektronicznej objęte systemem identyfikacji elektronicznej notyfikowanym na podstawie art. 9 ust. 1.

▼M1

Artykuł 11a

Transgraniczne dopasowywanie tożsamości

1. Działając jako strony ufające w odniesieniu do usług transgranicznych, państwa członkowskie zapewniają jednoznaczne dopasowywanie tożsamości osób fizycznych z użyciem notyfikowanych środków identyfikacji elektronicznej lub europejskich portfeli tożsamości cyfrowej.

2. Państwa członkowskie określają środki techniczne i organizacyjne w celu zapewnienia wysokiego poziomu ochrony danych osobowych wykorzystywanych do dopasowywania tożsamości oraz w celu zapobiegania profilowaniu użytkowników.

3. Do dnia 21 listopada 2024 r. Komisja, w drodze aktów wykonawczych, ustanowi wykaz norm referencyjnych oraz, w razie potrzeby, ustanowi specyfikacje i procedury w odniesieniu do wymogów, o których mowa w ust. 1 niniejszego artykułu. Te akty wykonawcze przyjmuje się zgodnie z procedurą sprawdzającą, o której mowa w art. 48 ust. 2.

▼B

Artykuł 12

▼M1

Interoperacyjność

▼B

1. Krajowe systemy identyfikacji elektronicznej notyfikowane na podstawie art. 9 ust. 1 muszą być interoperacyjne.

2. Do celów ust. 1 ustanowia się ramy interoperacyjności.

3. Ramy interoperacyjności spełniają następujące kryteria:

a) są neutralne pod względem technologicznym i nie dyskryminują żadnych konkretnych krajowych rozwiązań technicznych w zakresie identyfikacji elektronicznej w danym państwie członkowskim;

b) są zgodne, w miarę możliwości, z europejskimi i międzynarodowymi standardami;

▼M1

c) ułatwiają wdrożenie zasad prywatności i bezpieczeństwa na etapie projektowania;

———————

▼B

4. Ramy interoperacyjności zawierają:

a) odniesienie do minimalnych wymogów technicznych powiązanych z poziomami bezpieczeństwa określonych w art. 8;

▼B

b) przyporządkowanie krajowych poziomów bezpieczeństwa notyfikowanych systemów identyfikacji elektronicznej względem poziomów bezpieczeństwa na mocy art. 8;

c) odniesienie do minimalnych wymogów technicznych dotyczących interoperacyjności;

▼M1

d) odniesienie do minimalnego zbioru danych identyfikujących osobę niezbędnych do niepowtarzalnego reprezentowania osoby fizycznej lub prawnej, lub osoby fizycznej reprezentującej inną osobę fizyczną lub osobę prawną, które jest dostępne w ramach systemów identyfikacji elektronicznej;

▼B

e) regulamin wewnętrzny;

f) ustalenia dotyczące rozstrzygania sporów; oraz

g) wspólne operacyjne standardy bezpieczeństwa.

▼M1

5. Państwa członkowskie przeprowadzają wzajemne oceny systemów identyfikacji elektronicznej, które objęte są zakresem stosowania niniejszego rozporządzenia, i które mają być notyfikowane zgodnie z art. 9 ust. 1 lit. a).

6. Do dnia 18 marca 2025 r. Komisja ustanowi, w drodze aktów wykonawczych, niezbędne warunki proceduralne wzajemnych ocen, o których mowa w ust. 5 niniejszego artykułu, w celu zapewnienia wysokiego poziomu zaufania i bezpieczeństwa, stosownie do poziomu ryzyka. Te akty wykonawcze przyjmuje się zgodnie z procedurą sprawdzającą, o której mowa w art. 48 ust. 2.

_____

8. Do dnia 18 września 2025 r., w celu określenia jednolitych warunków wdrożenia wymogu, o którym mowa w ust. 1 niniejszego artykułu, z zastrzeżeniem kryteriów określonych w ust. 3 niniejszego artykułu oraz z uwzględnieniem rezultatów współpracy między państwami członkowskimi, Komisja przyjmie akty wykonawcze dotyczące ram interoperacyjności określonych w ust. 4 niniejszego artykułu. Te akty wykonawcze przyjmuje się zgodnie z procedurą sprawdzającą, o której mowa w art. 48 ust. 2.

▼B

9. Akty wykonawcze, o których mowa w ust. 7 i 8 niniejszego artykułu, przyjmuje się zgodnie z procedurą sprawdzającą, o której mowa w art. 48 ust. 2.

▼M1

Artykuł 12a

Certyfikacja systemów identyfikacji elektronicznej

1. Zgodność systemów identyfikacji elektronicznej, które mają być notyfikowane, z wymogami dotyczącymi cyberbezpieczeństwa określonymi w niniejszym rozporządzeniu, w tym zgodność z wymogami związanymi z cyberbezpieczeństwem określonymi w art. 8 ust. 2 dotyczącymi poziomów bezpieczeństwa systemów identyfikacji elektronicznej, certyfikują jednostki oceniające zgodność wyznaczone przez państwa członkowskie.

▼M1

2. Certyfikację zgodnie z ust. 1 niniejszego artykułu przeprowadza się w ramach odpowiedniego programu certyfikacji cyberbezpieczeństwa na podstawie rozporządzenia (UE) 2019/881 lub jego części, w zakresie, w jakim certyfikat cyberbezpieczeństwa lub jego części obejmują te wymogi w zakresie cyberbezpieczeństwa.

3. Certyfikacja na podstawie ust. 1 jest ważna przez okres do pięciu lat, pod warunkiem że co dwa lata przeprowadza się ocenę podatności na zagrożenia. W przypadku gdy zostanie stwierdzona podatność na zagrożenia i nie zostanie ona wyeliminowana w terminie trzech miesięcy od takiego stwierdzenia, certyfikacja zostaje odwołana.

4. Niezależnie od ust. 2 państwa członkowskie, zgodnie z tym ustępem, mogą zwrócić się do notyfikującego państwa członkowskiego o dodatkowe informacje na temat systemów identyfikacji elektronicznej lub ich części.

5. Wzajemna ocena systemów identyfikacji elektronicznej, o której mowa w art. 12 ust. 5, nie ma zastosowania do systemów identyfikacji elektronicznej certyfikowanych zgodnie z ust. 1 niniejszego artykułu ani do części takich systemów. Państwa członkowskie mogą wykorzystać certyfikat lub deklarację zgodności, wydane zgodnie z odpowiednim programem certyfikacji lub częściami takich programów, z wymogami niezwiązanymi z cyberbezpieczeństwem określonymi w art. 8 ust. 2 w zakresie poziomu bezpieczeństwa systemów identyfikacji elektronicznej.

6. Państwa członkowskie przekazują Komisji nazwy i adresy jednostek oceniających zgodność, o których mowa w ust. 1. Komisja udostępnia te informacje wszystkim państwom członkowskim.

Artykuł 12b

Dostęp do funkcji sprzętu i oprogramowania

W przypadku gdy dostawcy europejskich portfeli tożsamości cyfrowej i wydawcy notyfikowanych środków identyfikacji elektronicznej działający w celach handlowych lub zawodowych oraz korzystający z podstawowych usług platformowych zdefiniowanych w art. 2 pkt 2 rozporządzenia Parlamentu Europejskiego i Rady (UE) 2022/1925 ([1]) do celów świadczenia użytkownikom końcowym usług europejskiego portfela tożsamości cyfrowej i środków identyfikacji elektronicznej lub w trakcie świadczenia takich usług i środków są użytkownikami biznesowymi zgodnie z definicją w art. 2 pkt 21 tego rozporządzenia, strażnicy dostępu umożliwiają im w szczególności skuteczną interoperacyjność z tym samym systemem operacyjnym oraz funkcjami sprzętu lub oprogramowania oraz dostęp do tego systemu operacyjnego i tych funkcji na potrzeby interoperacyjności. Taką skuteczną interoperacyjność i dostęp zapewnia się nieodpłatnie oraz niezależnie od tego, czy funkcje sprzętu lub oprogramowania stanowią część systemu operacyjnego, są dostępne dla tego strażnika dostępu lub wykorzystywane przez niego podczas świadczenia takich usług w rozumieniu art. 6 ust. 7 rozporządzenia (UE) 2022/1925. Niniejszy artykuł pozostaje bez uszczerbku dla art. 5a ust. 14 niniejszego rozporządzenia.

([1]) Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2022/1925 z dnia 14 września 2022 r. w sprawie kontestowalnych i uczciwych rynków w sektorze cyfrowym oraz zmiany dyrektyw (UE) 2019/1937 i (UE) 2020/1828 (akt o rynkach cyfrowych) (Dz.U. L 265 z 12.10.2022, s. 1).

▼B

ROZDZIAŁ III

USŁUGI ZAUFANIA

SEKCJA 1

Przepisy ogólne

Artykuł 13

Odpowiedzialność i ciężar dowodu

▼M1

1. Niezależnie od ust. 2 niniejszego artykułu oraz bez uszczerbku dla rozporządzenia (UE) 2016/679, dostawcy usług zaufania są odpowiedzialni za szkody wyrządzone w sposób zamierzony lub w wyniku niedbalstwa osobie fizycznej lub prawnej z powodu nieprzestrzegania obowiązków określonych w niniejszym rozporządzeniu. Każda osoba fizyczna lub prawna, która poniosła szkodę majątkową lub niemajątkową w wyniku naruszenia niniejszego rozporządzenia przez dostawcę usług zaufania, ma prawo dochodzić odszkodowania zgodnie z prawem Unii i krajowym.

Ciężar dowiedzenia zamiaru lub niedbalstwa po stronie niekwalifikowanego dostawcy usług zaufania spoczywa na osobie fizycznej lub prawnej zgłaszającej szkodę, o której mowa w akapicie pierwszym.

Domniemywa się zamiar lub niedbalstwo kwalifikowanego dostawcy usług zaufania, chyba że kwalifikowany dostawca usług zaufania udowodni, że szkoda, o której mowa w akapicie pierwszym, nie nastąpiła w wyniku zamiaru lub niedbalstwa.

▼B

2. W przypadku gdy dostawcy usług zaufania z wyprzedzeniem należycie powiadomią swoich klientów o ograniczeniach w korzystaniu ze świadczonych przez siebie usług i ograniczenia te mogą być rozpoznane przez strony trzecie, dostawcy usług zaufania nie są odpowiedzialni za szkody powstałe w wyniku korzystania z usług przekraczającego wskazane ograniczenia.

3. Ust. 1 i 2 mają zastosowanie zgodnie z krajowymi przepisami dotyczącymi odpowiedzialności.

▼M1

Artykuł 14

Aspekty międzynarodowe

1. Usługi zaufania świadczone przez dostawców usług zaufania mających siedzibę w państwie trzecim lub przez organizację międzynarodową uznaje się za prawnie równoważne kwalifikowanym usługom zaufania świadczonym przez kwalifikowanych dostawców usług zaufania mających siedzibę w Unii, w przypadku gdy usługi zaufania pochodzące z państwa trzeciego lub organizacji międzynarodowej są uznawane w drodze aktów wykonawczych lub umowy zawartej między Unią a danym państwem trzecim lub organizacją międzynarodową zgodnie z art. 218 TFUE.

Akty wykonawcze, o których mowa w akapicie pierwszym, przyjmuje się zgodnie z procedurą sprawdzającą, o której mowa w art. 48 ust. 2.

▼M1

2. Akty wykonawcze i umowa, o których mowa w ust. 1, zapewniają, aby wymogi mające zastosowanie do kwalifikowanych dostawców usług zaufania mających siedzibę w Unii oraz do świadczonych przez nich kwalifikowanych usług zaufania były spełniane przez dostawców usług zaufania w danym państwie trzecim lub przez organizację międzynarodową oraz przez świadczone przez nich usługi zaufania. Państwa trzecie i organizacje międzynarodowe w szczególności ustanawiają, prowadzą i publikują zaufaną listę uznawanych dostawców usług zaufania.

3. Umowa, o której mowa w ust. 1, zapewnia, aby kwalifikowane usługi zaufania świadczone przez kwalifikowanych dostawców usług zaufania mających siedzibę w Unii były uznawane za prawnie równoważne usługom zaufania świadczonym przez dostawców usług zaufania w danym państwie trzecim lub przez organizację międzynarodową, z którymi zawarta została dana umowa.

Artykuł 15

Dostępność dla osób z niepełnosprawnościami i osób o specjalnych potrzebach

Zapewniane środki identyfikacji elektronicznej, usługi zaufania oraz produkty przeznaczone dla użytkownika końcowego stosowane do świadczenia tych usług udostępnia się w prostym i zrozumiałym języku, zgodnie z Konwencją Narodów Zjednoczonych o prawach osób niepełnosprawnych oraz zgodnie z wymogami dostępności określonymi dyrektywie (UE) 2019/882, przynosząc w ten sposób korzyści również osobom z ograniczeniami funkcjonalnymi, takim jak osoby starsze, oraz osobom z ograniczonym dostępem do technologii cyfrowych.

Artykuł 16

Kary

1. Bez uszczerbku dla art. 31 dyrektywy Parlamentu Europejskiego i Rady (UE) 2022/2555 ([1]) państwa członkowskie ustanawiają przepisy dotyczące kar mających zastosowanie w przypadku naruszeń niniejszego rozporządzenia. Kary te muszą być skuteczne, proporcjonalne i odstraszające.

2. Państwa członkowskie zapewniają, aby naruszenia niniejszego rozporządzenia przez kwalifikowanych i niekwalifikowanych dostawców usług zaufania podlegały administracyjnej karze pieniężnej w maksymalnej wysokości co najmniej:

a) 5 000 000 EUR – w przypadku gdy dostawca usług zaufania jest osobą fizyczną; lub

b) w przypadku gdy dostawca usług zaufania jest osobą prawną – 5 000 000 EUR lub 1 % całkowitego rocznego światowego obrotu przedsiębiorstwa, do którego należał dostawca usług zaufania, w roku obrotowym poprzedzającym rok, w którym miało miejsce naruszenie, w zależności od tego, która z tych wartości jest wyższa.

([1]) Dyrektywa Parlamentu Europejskiego i Rady (UE) 2022/2555 z dnia 14 grudnia 2022 r. w sprawie środków na rzecz wysokiego wspólnego poziomu cyberbezpieczeństwa na terytorium Unii, zmieniająca rozporządzenie (UE) nr 910/2014 i dyrektywę (UE) 2018/1972 oraz uchylająca dyrektywę (UE) 2016/1148 (dyrektywa NIS 2) (Dz.U. L 333 z 27.12.2022, s. 80).

▼M1

3. W zależności od systemu prawnego państw członkowskich przepisy dotyczące administracyjnych kar pieniężnych można stosować w taki sposób, że o zastosowanie kary pieniężnej wnosi właściwy organ nadzorczy, a nakładają ją właściwe sądy krajowe. Zastosowanie takich przepisów w tych państwach członkowskich musi zapewniać, aby te środki prawne były skuteczne i miały skutek administracyjny równoważny karom pieniężnym nakładanym bezpośrednio przez organy nadzorcze.

▼B

SEKCJA 2

▼M1

Niekwalifikowani dostawcy usług zaufania

▼B

Artykuł 19

Wymogi w zakresie bezpieczeństwa mające zastosowanie do dostawców usług zaufania

1. Kwalifikowani i niekwalifikowani dostawcy usług zaufania przyjmują odpowiednie środki techniczne i organizacyjne w celu zarządzania ryzykiem, na jakie narażone jest bezpieczeństwo świadczonych przez nich usług zaufania. Przy uwzględnieniu najnowszych osiągnięć w dziedzinie technologii środki te zapewniają poziom bezpieczeństwa współmierny ze stopniem ryzyka. W szczególności należy podjąć środki zapobiegające incydentom związanym z bezpieczeństwem lub minimalizujące ich wpływ oraz należy informować zainteresowane strony o negatywnych skutkach wszelkich takich incydentów.

2. Kwalifikowani i niekwalifikowani dostawcy usług zaufania, bez zbędnej zwłoki, a w każdym razie nie później niż 24 godziny od otrzymania informacji o wystąpieniu zdarzenia, zawiadamiają organ nadzoru i, w stosownych przypadkach, inne właściwe podmioty, takie jak właściwy krajowy organ ds. bezpieczeństwa informacji lub organ ochrony danych, o wszelkich przypadkach naruszenia bezpieczeństwa lub utraty integralności, które mają znaczący wpływ na świadczoną usługę zaufania lub przetwarzane w jej ramach dane osobowe..

W przypadku gdy prawdopodobne jest, że naruszenie bezpieczeństwa lub utrata integralności niekorzystnie wpłyną na osobę fizyczną lub prawną, na rzecz której świadczona była usługa zaufania, dostawca usług zaufania bez zbędnej zwłoki zawiadamia także tę osobę fizyczną lub prawną o tym naruszeniu bezpieczeństwa lub utracie integralności.

W stosownych przypadkach, w szczególności jeżeli naruszenie bezpieczeństwa lub utrata integralności dotyczą dwóch lub większej liczby państw członkowskich, zawiadomiony organ nadzoru powiadamia organy nadzoru w pozostałych zainteresowanych państwach członkowskich oraz ENISA.

Zawiadomiony organ nadzoru podaje zaistniałe fakty do wiadomości publicznej lub nakłada taki obowiązek na dostawcę usług zaufania, w przypadku gdy uzna, że ujawnienie naruszenia bezpieczeństwa lub utraty integralności leży w interesie publicznym.

▼B

3. Raz do roku organ nadzoru przekazuje ENISA zestawienie zawiadomień o naruszeniach bezpieczeństwa lub utraty integralności otrzymanych od dostawców usług zaufania.

4. Komisja może w drodze aktów wykonawczych:

a) określić bardziej szczegółowo środki, o których mowa w ust. 1; oraz

b) określić formaty i procedury, w tym również terminy, mające zastosowanie na użytek ust. 2.

Te akty wykonawcze przyjmuje się zgodnie z procedurą sprawdzającą, o której mowa w art. 48 ust. 2.

▼M1

Artykuł 19a

Wymogi dla niekwalifikowanych dostawców usług zaufania

1. Niekwalifikowany dostawca usług zaufania świadczący niekwalifikowane usługi zaufania:

a) musi posiadać odpowiednie polityki i wprowadzać odpowiednie środki w celu zarządzania ryzykiem prawnym, biznesowym, operacyjnym oraz innymi bezpośrednimi lub pośrednimi ryzykami dla świadczenia niekwalifikowanej usługi zaufania, które – niezależnie od art. 21 dyrektywy (UE) 2022/2555 – obejmują co najmniej środki związane z:

   (i) procedurami rejestracji i wdrażania w odniesieniu do usługi zaufania;

   (ii) kontrolami proceduralnymi lub administracyjnymi niezbędnymi do świadczenia usług zaufania:

   (iii) zarządzaniem usługami zaufania i ich wdrażaniem;

b) powiadomienie organu nadzoru, możliwych do zidentyfikowania osób fizycznych, których to dotyczy, oraz opinii publicznej, jeżeli leży to w interesie publicznym, oraz – w stosownych przypadkach – innych odpowiednich właściwych organów o wszelkich naruszeniach bezpieczeństwa lub zakłóceniach w świadczeniu usługi lub we wdrażaniu środków, o których mowa w lit. a) ppkt (i), (ii) lub (iii), które mają znaczący wpływ na świadczoną usługę zaufania lub na przetwarzane w jej ramach dane osobowe, bez zbędnej zwłoki, a w każdym razie nie później niż w terminie 24 godzin po otrzymaniu informacji o wszelkich naruszeniach bezpieczeństwa lub zakłóceniach.

2. Do dnia 21 maja 2025 r. Komisja, w drodze aktów wykonawczych, sporządzi wykaz norm referencyjnych oraz, w razie potrzeby, ustanowi specyfikacje i procedury do celów ust. 1 lit. a) niniejszego artykułu. W przypadku gdy te normy, specyfikacje i procedury są przestrzegane, domniemywa się zgodność z wymogami określonymi w niniejszym artykule. Te akty wykonawcze przyjmuje się zgodnie z procedurą sprawdzającą, o której mowa w art. 48 ust. 2.

▼B

SEKCJA 3

Kwalifikowane usługi zaufania

Artykuł 20

Nadzór nad kwalifikowanymi dostawcami usług zaufania

▼M1

1. Kwalifikowani dostawcy usług zaufania podlegają audytowi, na swój własny koszt, co najmniej raz na 24 miesiące, przeprowadzanemu przez jednostkę oceniającą zgodność. W ramach audytu potwierdza się, czy kwalifikowani dostawcy usług zaufania i świadczone przez nich kwalifikowane usługi zaufania spełniają wymogi określone w niniejszym rozporządzeniu oraz w art. 21 dyrektywy (UE) 2022/2555. Kwalifikowani dostawcy usług zaufania przedkładają organowi nadzoru powstały w wyniku audytu raport z oceny zgodności w terminie trzech dni roboczych od jego otrzymania.

1a. Kwalifikowani dostawcy usług zaufania informują organ nadzoru co najmniej miesiąc przed jakimkolwiek planowanym audytem oraz umożliwiają organowi nadzoru udział w charakterze obserwatora, na jego wniosek.

1b. Państwa członkowskie bez zbędnej zwłoki przekazują Komisji nazwy, adresy i szczegóły akredytacji jednostek oceniających zgodność, o których mowa w ust. 1, oraz wszelkie późniejsze zmiany w tym zakresie. Komisja udostępnia te informacje wszystkim państwom członkowskim.

2. Bez uszczerbku dla ust. 1, organ nadzoru może w dowolnym momencie przeprowadzić audyt lub zwrócić się do jednostki oceniającej zgodność o przeprowadzenie oceny zgodności kwalifikowanych dostawców usług zaufania, na koszt tych dostawców usług zaufania, aby potwierdzić, że dostawcy ci oraz świadczone przez nich kwalifikowane usługi zaufania spełniają wymogi określone w niniejszym rozporządzeniu. W przypadku podejrzenia naruszenia przepisów dotyczących ochrony danych osobowych, organ nadzoru informuje bez zbędnej zwłoki właściwe organy nadzorcze ustanowione zgodnie z art. 51 rozporządzenia (UE) 2016/679.

3. W przypadku gdy kwalifikowany dostawca usług zaufania nie spełnia któregokolwiek z wymogów określonych w niniejszym rozporządzeniu, organ nadzoru nakłada na niego wymóg wyeliminowania, w stosownych przypadkach w ustalonym terminie, niezgodności z tymi wymogami.

W przypadku gdy dostawca ten nie wyeliminuje, w stosownych przypadkach w terminie ustalonym przez organ nadzoru, niezgodności z wymogami, organ nadzoru, jeżeli jest to uzasadnione, biorąc pod uwagę w szczególności zakres, czas trwania i skutki tego niespełnienia wymogów, odbiera status kwalifikowany temu dostawcy lub świadczonej przez niego usłudze, której to dotyczy.

3a. W przypadku gdy właściwe organy wyznaczone lub ustanowione na podstawie art. 8 ust. 1 dyrektywy (UE) 2022/2555 poinformują organ nadzoru, że kwalifikowany dostawca usług zaufania nie spełnia któregokolwiek z wymogów określonych w art. 21 tej dyrektywy, organ nadzoru, jeżeli jest to uzasadnione, biorąc pod uwagę w szczególności zakres, czas trwania i skutki tego niespełnienia wymogów, odbiera status kwalifikowany temu dostawcy lub świadczonej przez niego usłudze, której to dotyczy.

▼M1

3b. W przypadku gdy organy nadzorcze ustanowione zgodnie z art. 51 rozporządzenia (UE) 2016/679 poinformują organ nadzoru, że kwalifikowany dostawca usług zaufania nie spełnia któregokolwiek z wymogów określonych w tym rozporządzeniu, organ nadzoru, jeżeli jest to uzasadnione, biorąc pod uwagę w szczególności zakres, czas trwania i skutki tego niespełnienia wymogów, odbiera status kwalifikowany temu dostawcy lub świadczonej przez niego usłudze, której to dotyczy.

3c. Organ nadzoru informuje kwalifikowanego dostawcę usług zaufania o odebraniu jego statusu kwalifikowanego lub statusu kwalifikowanego danej usługi. Organ nadzoru informuje podmiot zgłoszony na podstawie art. 22 ust. 3 niniejszego rozporządzenia do celów aktualizacji zaufanych list, o których mowa w ust. 1 tego artykułu, oraz właściwy organ wyznaczony lub ustanowiony na podstawie art. 8 ust. 1 dyrektywy (UE) 2022/2555.

4. Do dnia 21 maja 2025 r. Komisja, w drodze aktów wykonawczych, sporządzi wykaz norm referencyjnych oraz, w stosownych przypadkach, ustanowi specyfikacje i procedury w odniesieniu do:

a) akredytacji jednostek oceniających zgodność oraz raportu z oceny zgodności, o którym mowa w ust. 1;

b) wymogów dotyczących audytów, zgodnie z którymi jednostki oceniające zgodność przeprowadzają oceny zgodności, w tym ocenę złożoną, kwalifikowanych dostawców usług zaufania, o których mowa w ust. 1;

c) programów oceny zgodności w zakresie przeprowadzania oceny zgodności kwalifikowanych dostawców usług zaufania przez jednostki oceniające zgodność oraz w odniesieniu do przekazywania raportu, o którym mowa w ust. 1.

Te akty wykonawcze przyjmuje się zgodnie z procedurą sprawdzającą, o której mowa w art. 48 ust. 2.

▼B

Artykuł 21

Inicjowanie kwalifikowanej usługi zaufania

▼M1

1. W przypadku gdy dostawcy usług zaufania zamierzają rozpocząć świadczenie kwalifikowanej usługi zaufania, zgłaszają organowi nadzoru swój zamiar wraz z raportem z oceny zgodności wydanym przez jednostkę oceniającą zgodność potwierdzającym spełnienie wymogów określonych w niniejszym rozporządzeniu oraz w art. 21 dyrektywy (UE) 2022/2555.

2. Organ nadzoru weryfikuje, czy dostawca usług zaufania i świadczone przez niego usługi zaufania spełniają wymogi określone w niniejszym rozporządzeniu, w szczególności wymogi dotyczące kwalifikowanych dostawców usług zaufania oraz świadczonych przez nich kwalifikowanych usług zaufania.

▼M1

W celu zweryfikowania spełnienia przez dostawcę usług zaufania wymogów określonych w art. 21 dyrektywy (UE) 2022/2555 organ nadzoru zwraca się do właściwych organów wyznaczonych lub ustanowionych na podstawie art. 8 ust. 1 tej dyrektywy o przeprowadzenie działań nadzorczych w tym zakresie oraz o udzielenie informacji na temat rezultatu tych działań bez zbędnej zwłoki i w każdym razie nie później niż w terminie dwóch miesięcy od otrzymania tego wniosku. Jeżeli weryfikacja nie została zakończona w terminie dwóch miesięcy od zgłoszenia, te właściwe organy informują o tym organ nadzoru, podając przy tym przyczyny opóźnienia, oraz wskazują termin, w którym weryfikacja ma zostać zakończona.

W przypadku gdy organ nadzoru stwierdzi, że dostawca usług zaufania i świadczone przez niego usługi zaufania spełniają wymogi określone w niniejszym rozporządzeniu, organ nadzoru przyznaje danemu dostawcy usług zaufania status kwalifikowanego dostawcy usług zaufania i status kwalifikowanych usług zaufania świadczonym przez niego usługom oraz informuje podmiot, o którym mowa w art. 22 ust. 3, w celu zaktualizowania przez niego zaufanych list, o których mowa w art. 22 ust. 1, nie później niż trzy miesiące po zgłoszeniu zgodnie z ust. 1 niniejszego artykułu.

W przypadku gdy weryfikacja nie została zakończona w terminie trzech miesięcy od zgłoszenia, organ nadzoru informuje o tym dostawcę usług zaufania, podając przyczyny opóźnienia, oraz wskazuje termin, w którym weryfikacja ma zostać zakończona.

▼B

3. Kwalifikowani dostawcy usług zaufania mogą rozpocząć świadczenie kwalifikowanej usługi zaufania, po tym jak ich kwalifikowany status zostanie wskazany w zaufanych listach, o których mowa w art. 22 ust. 1.

▼M1

4. Do dnia 21 maja 2025 r. Komisja, w drodze aktów wykonawczych, określi formaty i procedury zgłaszania i weryfikacji na potrzeby ust. 1 i 2 niniejszego artykułu. Te akty wykonawcze przyjmuje się zgodnie z procedurą sprawdzającą, o której mowa w art. 48 ust. 2.

▼B

Artykuł 22

Zaufane listy

1. Każde państwo członkowskie sporządza, prowadzi i publikuje zaufane listy zawierające informacje dotyczące kwalifikowanych dostawców usług zaufania, za których jest ono odpowiedzialne, wraz z informacjami dotyczącymi świadczonych przez nich kwalifikowanych usług zaufania.

2. Państwa członkowskie sporządzają, prowadzą i publikują – w zabezpieczony sposób – elektronicznie podpisane lub opatrzone pieczęcią elektroniczną zaufane listy, o których mowa w ust. 1, w postaci dostosowanej do automatycznego przetwarzania.

3. Bez zbędnej zwłoki państwa członkowskie przekazują Komisji informacje o podmiocie odpowiedzialnym za sporządzenie, prowadzenie i publikowanie krajowych zaufanych list wraz ze szczegółowymi informacjami dotyczącymi miejsca publikacji tych list, certyfikatów użytych do podpisania lub opatrzenia pieczęcią zaufanych list i wszelkich zmian, jakie są do nich wprowadzane.

▼B

4. Komisja udostępnia publicznie informacje, o których mowa w ust. 3, w elektronicznie podpisanej lub opatrzonej pieczęcią elektroniczną postaci dostosowanej do automatycznego przetwarzania, używając w tym celu zabezpieczonego kanału komunikacji.

5. Do dnia 18 września 2015 r. Komisja w drodze aktów wykonawczych określi informacje, o których mowa w ust. 1, oraz techniczne specyfikacje i formaty dotyczące zaufanych list mające zastosowanie na użytek ust. 1–4. Te akty wykonawcze przyjmuje się zgodnie z procedurą sprawdzającą, o której mowa w art. 48 ust. 2.

Artykuł 23

Znak zaufania UE dla kwalifikowanych usług zaufania

1. Po tym jak w zaufanej liście, o której mowa w art. 22 ust. 1, wskazany zostanie status kwalifikowany, o którym mowa w art. 21 ust. 2 akapit drugi, kwalifikowani dostawcy usług zaufania mogą używać znaku zaufania UE, aby w prosty, rozpoznawalny i jasny sposób wskazać świadczone przez siebie kwalifikowane usługi zaufania.

2. Gdy kwalifikowani dostawcy usług zaufania używają znaku zaufania UE w odniesieniu do kwalifikowanych usług zaufania, o których mowa w ust. 1, zapewniają, aby na ich witrynie internetowej dostępny był link do odpowiedniej zaufanej listy.

3. Do dnia 1 lipca 2015 r. Komisja w drodze aktów wykonawczych wprowadza specyfikacje dotyczące formy, a w szczególności prezentacji, kompozycji, rozmiaru i wzoru znaku zaufania UE dla kwalifikowanych usług zaufania. Te akty wykonawcze przyjmuje się zgodnie z procedurą sprawdzającą, o której mowa w art. 48 ust. 2.

Artykuł 24

Wymogi dla kwalifikowanych dostawców usług zaufania

▼M1

1. Wydając kwalifikowany certyfikat lub kwalifikowane elektroniczne poświadczenie atrybutów, kwalifikowany dostawca usług zaufania weryfikuje tożsamość oraz, w stosownym przypadku, wszelkie specjalne atrybuty osoby fizycznej lub prawnej, której ma być wydany kwalifikowany certyfikat lub kwalifikowane elektroniczne poświadczenie atrybutów.

1a. Weryfikacji tożsamości, o której mowa w ust. 1, dokonuje kwalifikowany dostawca usług zaufania, za pomocą odpowiednich środków, bezpośrednio albo za pośrednictwem strony trzeciej, w oparciu o jedną z następujących metod lub, w razie potrzeby, ich połączenie, zgodnie z aktami wykonawczymi, o których mowa w ust. 1c:

a) za pomocą europejskiego portfela tożsamości cyfrowej lub notyfikowanego środka identyfikacji elektronicznej, który spełnia wymogi określone w art. 8 w odniesieniu do wysokiego poziomu bezpieczeństwa;

b) za pomocą certyfikatu kwalifikowanego podpisu elektronicznego lub kwalifikowanej pieczęci elektronicznej wydanych zgodnie z lit. a), c) lub d);

▼M1

c) przy użyciu innych metod identyfikacji, które z dużą dozą pewności zapewniają identyfikację osoby i których zgodność jest potwierdzona przez jednostkę oceniającą zgodność;

d) poprzez fizyczną obecność osoby fizycznej lub upoważnionego przedstawiciela osoby prawnej, za pomocą odpowiednich dowodów oraz procedur, zgodnie z prawem krajowym.

1b. Weryfikacji atrybutów, o których mowa w ust. 1, dokonuje kwalifikowany dostawca usług zaufania, za pomocą odpowiednich środków, bezpośrednio albo za pośrednictwem strony trzeciej, w oparciu o jedną z następujących metod lub, w razie potrzeby, ich połączenie, zgodnie z aktami wykonawczymi, o których mowa w ust. 1c:

a) za pomocą europejskiego portfela tożsamości cyfrowej lub notyfikowanego środka identyfikacji elektronicznej, który spełnia wymogi określone w art. 8 w odniesieniu do wysokiego poziomu bezpieczeństwa;

b) za pomocą certyfikatu kwalifikowanego podpisu elektronicznego lub kwalifikowanej pieczęci elektronicznej, wydanych zgodnie z ust. 1a lit. a), c) lub d);

c) za pomocą kwalifikowanego elektronicznego poświadczenia atrybutów;

d) stosując inne metody, które z dużą dozą pewności zapewniają weryfikację atrybutów, i których zgodność jest potwierdzona przez jednostkę oceniającą zgodność;

e) poprzez fizyczną obecność osoby fizycznej lub upoważnionego przedstawiciela osoby prawnej, za pomocą odpowiednich dowodów oraz procedur, zgodnie z prawem krajowym.

1c. Do dnia 21 maja 2025 r. Komisja, w drodze aktów wykonawczych, sporządzi wykaz norm referencyjnych oraz, w razie potrzeby, ustanowi specyfikacje i procedury do celów weryfikacji tożsamości i atrybutów zgodnie z ust. 1, 1a i 1b niniejszego artykułu. Te akty wykonawcze przyjmuje się zgodnie z procedurą sprawdzającą, o której mowa w art. 48 ust. 2.

▼B

2. Dostawca kwalifikowanych usług zaufania świadczący kwalifikowane usługi zaufania:

▼M1

a) informuje organ nadzoru co najmniej miesiąc przed wprowadzeniem jakiejkolwiek zmiany w świadczeniu przez niego kwalifikowanych usług zaufania lub z co najmniej trzymiesięcznym wyprzedzeniem w przypadku zamiaru zaprzestania tej działalności;

▼B

b) zatrudnia pracowników i, w stosownym przypadku, podwykonawców, którzy posiadają niezbędną wiedzę fachową, wiarygodność, doświadczenie i kwalifikacje i którzy przeszli odpowiednie szkolenia na temat przepisów dotyczących bezpieczeństwa i ochrony danych osobowych oraz którzy stosują procedury administracyjne i zarządcze odpowiadające europejskim lub międzynarodowym standardom;

c) w odniesieniu do ryzyka związanego z odpowiedzialnością za szkody zgodnie z art. 13 utrzymuje dostateczne zasoby finansowe lub dysponuje stosownym ubezpieczeniem od odpowiedzialności zgodnie z prawem krajowym;

▼M1

d) przed nawiązaniem stosunku umownego informuje w jasny, kompleksowy i łatwo dostępny sposób, w miejscu publicznie dostępnym oraz indywidualnie wszelkie osoby, które mają zamiar skorzystać z kwalifikowanej usługi zaufania, o dokładnych warunkach korzystania z tej usługi, w tym o wszelkich ograniczeniach korzystania z niej;

e) używa wiarygodnych systemów i produktów, które są chronione przed modyfikacją oraz zapewniają techniczne bezpieczeństwo i wiarygodność procesów przez nie obsługiwanych, w tym przy użyciu odpowiednich technik kryptograficznych;

▼B

f) używa wiarygodnych systemów do przechowywania przekazanych mu danych w sprawdzalnej postaci, tak aby:

(i) dane były publicznie dostępne do wyszukiwania dopiero po uzyskaniu zgody osoby, do której dane się odnoszą;

(ii) tylko upoważnione osoby mogły wprowadzać dane i zmiany w przechowywanych danych;

(iii) można było sprawdzać autentyczność danych;

▼M1

fa) niezależnie od art. 21 dyrektywy (UE) 2022/2555, posiada odpowiednie polityki oraz wprowadza odpowiednie środki w celu zarządzania ryzykiem prawnym, biznesowym, operacyjnym oraz innymi bezpośrednimi lub pośrednimi ryzykami dla świadczenia kwalifikowanej usługi zaufania, w tym co najmniej środki związane z:

(i) procedurami rejestracji i wdrażania w odniesieniu do usługi;

(ii) kontrolami proceduralnymi lub administracyjnymi;

(iii) zarządzaniem usługami zaufania oraz ich wdrażaniem;

fb) bez zbędnej zwłoki, a w każdym razie nie później niż w terminie 24 godzin od incydentu, powiadamia organ nadzoru, możliwe do zidentyfikowania osoby fizyczne, których to dotyczy, a także – w stosownych przypadkach – inne odpowiednie właściwe organy oraz, na wniosek organu nadzoru, opinię publiczną, jeżeli leży to w interesie publicznym, o wszelkich naruszeniach bezpieczeństwa lub zakłóceniach w świadczeniu usługi lub we wdrażaniu środków, o których mowa w lit. fa) ppkt (i), (ii) lub (iii), które mają znaczący wpływ na świadczoną usługę zaufania lub na przetwarzane w ramach tej usługi dane osobowe;

g) wprowadza odpowiednie środki zapobiegające fałszowaniu, kradzieży lub przywłaszczeniu danych, lub nieuprawnionemu usuwaniu, modyfikowaniu lub uniemożliwianiu dostępu do danych;

h) rejestruje i udostępnia tak długo, jak jest to konieczne po zaprzestaniu działalności przez kwalifikowanego dostawcę usług zaufania, wszystkie odpowiednie informacje dotyczące danych wydanych i otrzymanych przez kwalifikowanego dostawcę usług zaufania, do celów przedstawienia dowodów w postępowaniach sądowych do celów zapewnienia ciągłości usług. Rejestracja taka może odbywać się drogą elektroniczną;

▼M1

(i) posiada aktualny plan zakończenia działalności, aby zapewnić ciągłość usług zgodnie z postanowieniami, które zostały zweryfikowane przez organ nadzoru zgodnie z art. 46b ust. 4 lit. i);

_____

▼B

k) w przypadku kwalifikowanych dostawców usług zaufania wydających kwalifikowane certyfikaty – tworzy i aktualizuje bazę danych dotyczącą certyfikatów.

▼M1

Organ nadzoru może zażądać dodatkowych informacji oprócz informacji przekazanych zgodnie z akapitem pierwszym lit. a) lub wyników oceny zgodności oraz może uzależnić udzielenie zezwolenia na wdrożenie planowanych zmian w kwalifikowanych usługach zaufania. Jeżeli weryfikacja nie została zakończona w terminie trzech miesięcy od zgłoszenia, organ nadzoru informuje o tym dostawcę usług zaufania, podając przyczyny opóźnienia, oraz wskazuje termin, w którym weryfikacja ma zostać zakończona.

▼B

3. Jeżeli kwalifikowany dostawca usług zaufania wydający kwalifikowane certyfikaty postanowi unieważnić certyfikat, rejestruje on takie unieważnienie w swojej bazie danych dotyczącej certyfikatów i publikuje informację o statusie unieważnienia certyfikatu w odpowiednim czasie, ale w każdym razie w ciągu 24 godzin po otrzymaniu wniosku. Unieważnienie staje się skuteczne natychmiast po jego opublikowaniu.

4. W odniesieniu do ust. 3 kwalifikowani dostawcy usług zaufania wydający kwalifikowane certyfikaty dostarczają każdej stronie ufającej informacje o statusie ważności lub unieważnienia wydanych przez siebie kwalifikowanych certyfikatów. Informacje te są dostępne co najmniej na poziomie certyfikatu w automatyczny sposób, który jest wiarygodny, nieodpłatny i wydajny, w każdym momencie, także po upływie okresu ważności certyfikatu.

▼M1

4a. Ust. 3 i 4 stosuje się odpowiednio do unieważniania kwalifikowanych elektronicznych poświadczeń atrybutów.

4b. Komisja jest uprawniona do przyjmowania aktów delegowanych, zgodnie z art. 47, ustanawiających dodatkowe środki, o których mowa w ust. 2 lit. fa) niniejszego artykułu.

5. Do dnia 21 maja 2025 r. Komisja, w drodze aktów wykonawczych, sporządzi wykaz norm referencyjnych oraz, w razie potrzeby, ustanowi specyfikacje i procedury w odniesieniu do wymogów, o których mowa w ust. 2 niniejszego artykułu. W przypadku gdy te normy, specyfikacje i procedury są przestrzegane, domniemywa się zgodność z wymogami określonymi w niniejszym ustępie. Te akty wykonawcze przyjmuje się zgodnie z procedurą sprawdzającą, o której mowa w art. 48 ust. 2.

Artykuł 24a

Uznawanie kwalifikowanych usług zaufania

1. Kwalifikowane podpisy elektroniczne oparte na kwalifikowanym certyfikacie wydanym w jednym państwie członkowskim oraz kwalifikowane pieczęcie elektroniczne oparte na kwalifikowanym certyfikacie

▼M1

wydanym w jednym państwie członkowskim uznaje się, odpowiednio, za kwalifikowane podpisy elektroniczne i kwalifikowane pieczęcie elektroniczne we wszystkich pozostałych państwach członkowskich.

2. Kwalifikowane urządzenia do składania podpisu elektronicznego oraz kwalifikowane urządzenia do składania pieczęci elektronicznej certyfikowane w jednym państwie członkowskim uznaje się, odpowiednio, za kwalifikowane urządzenia do składania podpisu elektronicznego i kwalifikowane urządzenia do składania pieczęci elektronicznej we wszystkich pozostałych państwach członkowskich.

3. Kwalifikowany certyfikat podpisów elektronicznych, kwalifikowany certyfikat pieczęci elektronicznych, kwalifikowaną usługę zaufania w zakresie zarządzania kwalifikowanymi urządzeniami do składania podpisu elektronicznego na odległość oraz kwalifikowaną usługę zaufania w zakresie zarządzania urządzeniami do składania kwalifikowanej pieczęci elektronicznej na odległość zapewniane w jednym państwie członkowskim, uznaje się, odpowiednio, za kwalifikowany certyfikat podpisów elektronicznych, kwalifikowany certyfikat pieczęci elektronicznych, kwalifikowaną usługę zaufania w zakresie zarządzania kwalifikowanymi urządzeniami do składania podpisu elektronicznego na odległość oraz kwalifikowaną usługę zaufania w zakresie zarządzania kwalifikowanymi urządzeniami do składania pieczęci elektronicznej na odległość we wszystkich pozostałych państwach członkowskich.

4. Kwalifikowaną usługę walidacji kwalifikowanych podpisów elektronicznych oraz kwalifikowaną usługę walidacji kwalifikowanych pieczęci elektronicznych, świadczone w jednym państwie członkowskim, uznaje się, odpowiednio, za kwalifikowaną usługę walidacji kwalifikowanych podpisów elektronicznych i kwalifikowaną usługę walidacji kwalifikowanych pieczęci elektronicznych we wszystkich pozostałych państwach członkowskich.

5. Kwalifikowaną usługę konserwacji kwalifikowanych podpisów elektronicznych oraz kwalifikowaną usługę konserwacji kwalifikowanych pieczęci elektronicznych, świadczone w jednym państwie członkowskim, uznaje się, odpowiednio, za kwalifikowaną usługę konserwacji kwalifikowanych podpisów elektronicznych i kwalifikowaną usługę konserwacji kwalifikowanych pieczęci elektronicznych we wszystkich pozostałych państwach członkowskich.

6. Kwalifikowany elektroniczny znacznik czasu zapewniany w jednym państwie członkowskim uznaje się za kwalifikowany elektroniczny znacznik czasu we wszystkich pozostałych państwach członkowskich.

7. Kwalifikowany certyfikat uwierzytelniania witryn internetowych wydany w jednym państwie członkowskim uznaje się za kwalifikowany certyfikat uwierzytelniania witryn internetowych we wszystkich pozostałych państwach członkowskich.

8. Kwalifikowaną usługę rejestrowanego doręczenia elektronicznego świadczoną w jednym państwie członkowskim uznaje się za kwalifikowaną usługę rejestrowanego doręczenia elektronicznego we wszystkich pozostałych państwach członkowskich.

9. Kwalifikowane elektroniczne poświadczenie atrybutów wydane w jednym państwie członkowskim uznaje się za kwalifikowane elektroniczne poświadczenie atrybutów we wszystkich pozostałych państwach członkowskich.

10. Kwalifikowane usługi archiwizacji elektronicznej świadczone w jednym państwie członkowskim uznaje się za kwalifikowane usługi archiwizacji elektronicznej we wszystkich pozostałych państwach członkowskich.

▼M1

11. Kwalifikowany rejestr elektroniczny zapewniany w jednym państwie członkowskim uznaje się za kwalifikowany rejestr elektroniczny we wszystkich pozostałych państwach członkowskich.

▼B

SEKCJA 4

Podpisy elektroniczne

Artykuł 25

Skutki prawne podpisów elektronicznych

1. Podpisowi elektronicznemu nie można odmówić skutku prawnego ani dopuszczalności jako dowodu w postępowaniu sądowym wyłącznie z tego powodu, że podpis ten ma postać elektroniczną lub że nie spełnia wymogów dla kwalifikowanych podpisów elektronicznych.

2. Kwalifikowany podpis elektroniczny ma skutek prawny równoważny podpisowi własnoręcznemu.

▼M1

_____

▼B

Artykuł 26

Wymogi dla zaawansowanych podpisów elektronicznych

►M1 1. ◄ Zaawansowany podpis elektroniczny musi spełniać następujące wymogi:

a) jest unikalnie przyporządkowany podpisującemu;

b) umożliwia ustalenie tożsamości podpisującego;

c) jest składany przy użyciu danych służących do składania podpisu elektronicznego, których podpisujący może, z dużą dozą pewności, użyć pod wyłączną swoją kontrolą; oraz

d) jest powiązany z danymi podpisanymi w taki sposób, że każda późniejsza zmiana danych jest rozpoznawalna.

▼M1

2. Do dnia 21 maja 2026 r. Komisja oceni, czy konieczne jest przyjęcie aktów wykonawczych w celu ustanowienia wykazu norm referencyjnych oraz, w razie potrzeby, ustanowienia specyfikacji i procedur w odniesieniu do zaawansowanych podpisów elektronicznych. Komisja może przyjąć takie akty wykonawcze na podstawie tej oceny. W przypadku gdy zaawansowany podpis elektroniczny jest zgodny z tymi normami, specyfikacjami i procedurami, domniemywa się zgodność z wymogami dotyczącymi zaawansowanych podpisów elektronicznych. Te akty wykonawcze przyjmuje się zgodnie z procedurą sprawdzającą, o której mowa w art. 48 ust. 2.

▼B

Artykuł 27

Podpisy elektroniczne w usługach publicznych

1. Jeżeli państwo członkowskie wymaga zaawansowanego podpisu elektronicznego do korzystania z usługi *online* oferowanej przez podmiot sektora publicznego lub w jego imieniu, to państwo członkowskie uznaje

▼B

zaawansowane podpisy elektroniczne, zaawansowane podpisy elektroniczne oparte na kwalifikowanym certyfikacie podpisów elektronicznych oraz kwalifikowane podpisy elektroniczne co najmniej w formatach lub wykorzystujące metody określone w aktach wykonawczych, o których mowa w ust. 5.

2. Jeżeli państwo członkowskie wymaga zaawansowanego podpisu elektronicznego opartego na kwalifikowanym certyfikacie do skorzystania z usługi *online* oferowanej przez podmiot sektora publicznego lub w jego imieniu, to państwo członkowskie uznaje zaawansowane podpisy elektroniczne oparte na kwalifikowanym certyfikacie i kwalifikowane podpisy elektroniczne co najmniej w formatach lub wykorzystujące metody określone w aktach wykonawczych, o których mowa w ust. 5.

3. W przypadku transgranicznego użycia w usłudze *online* oferowanej przez podmiot sektora publicznego państwa członkowskie nie wymagają podpisu elektronicznego o wyższym poziomie bezpieczeństwa niż kwalifikowany podpis elektroniczny.

▼M1

_____

▼B

5. Do dnia 18 września 2015 r. i przy uwzględnieniu istniejących praktyk, standardów i unijnych aktów prawnych Komisja określa w drodze aktów wykonawczych formaty referencyjne zaawansowanych podpisów elektronicznych lub metody referencyjne, w przypadku gdy używane są formaty alternatywne. Te akty wykonawcze przyjmuje się zgodnie z procedurą sprawdzającą, o której mowa w art. 48 ust. 2.

Artykuł 28

Kwalifikowane certyfikaty podpisów elektronicznych

1. Kwalifikowane certyfikaty podpisów elektronicznych muszą spełniać wymogi określone w załączniku I.

2. Kwalifikowane certyfikaty podpisów elektronicznych nie podlegają żadnym obowiązkowym wymogom wykraczającym poza wymogi określone w załączniku I.

3. Kwalifikowane certyfikaty podpisów elektronicznych mogą zawierać nieobowiązkowe dodatkowe szczególne atrybuty. Atrybuty te nie mogą wpływać na interoperacyjność i uznawanie kwalifikowanych podpisów elektronicznych.

4. Jeżeli kwalifikowany certyfikat podpisów elektronicznych został unieważniony po początkowej aktywacji, traci on ważność od momentu jego unieważnienia i w żadnym przypadku nie można przywrócić jego poprzedniego statusu.

5. Państwa członkowskie mogą ustanawiać przepisy krajowe dotyczące tymczasowego zawieszenia kwalifikowanego certyfikatu podpisu elektronicznego z zastrzeżeniem następujących warunków:

a) jeżeli kwalifikowany certyfikat podpisu elektronicznego został czasowo zawieszony, certyfikat ten traci ważność na okres zawieszenia;

b) okres zawieszenia jest jasno wskazywany w bazie danych dotyczącej certyfikatów i informacja o zawieszeniu jest widoczna, w okresie zawieszenia, na podstawie usługi informawania o statusie certyfikatu.

▼M1

6. Do dnia 21 maja 2025 r. Komisja, w drodze aktów wykonawczych, sporządzi wykaz norm referencyjnych oraz, w razie potrzeby, ustanowi specyfikacje i procedury w odniesieniu do kwalifikowanych certyfikatów podpisów elektronicznych. W przypadku gdy kwalifikowany certyfikat podpisu elektronicznego jest zgodny z tymi normami, specyfikacjami i procedurami, domniemywa się zgodność z wymogami określonymi w załączniku I. Te akty wykonawcze przyjmuje się zgodnie z procedurą sprawdzającą, o której mowa w art. 48 ust. 2.

▼B

Artykuł 29

Wymogi dla kwalifikowanych urządzeń do składania podpisu elektronicznego

1. Kwalifikowane urządzenia do składania podpisu elektronicznego muszą spełniać wymogi określone w załączniku II.

▼M1

1a. Dane służące do składania podpisu elektronicznego mogą być generowane, zarządzane lub kopiowane w celu utworzenia kopii zapasowej wyłącznie w imieniu podpisującego, na jego żądanie, i przez kwalifikowanego dostawcę usług zaufania, który świadczy kwalifikowaną usługę zaufania w zakresie zarządzania kwalifikowanym urządzeniem do składania podpisu elektronicznego na odległość.

▼B

2. Komisja może w drodze aktów wykonawczych podać numery referencyjne norm dotyczących kwalifikowanych urządzeń do składania podpisu elektronicznego. Jeżeli kwalifikowane urządzenie do składania podpisu elektronicznego spełnia te normy, domniemywa się zgodność z wymogami określonymi w załączniku II. Te akty wykonawcze przyjmuje się zgodnie z procedurą sprawdzającą, o której mowa w art. 48 ust. 2.

▼M1

Artykuł 29a

Wymogi dotyczące kwalifikowanej usługi zarządzania kwalifikowanymi urządzeniami do składania podpisu elektronicznego na odległość

1. Zarządzanie kwalifikowanymi urządzeniami do składania podpisu elektronicznego na odległość jako usługę kwalifikowaną może świadczyć wyłącznie kwalifikowany dostawca usług zaufania, który:

a) generuje dane służące do składania podpisu elektronicznego lub zarządza nimi w imieniu podpisującego;

b) niezależnie od pkt 1 lit. d) załącznika II kopiuje dane służące do składania podpisu elektronicznego wyłącznie w celu utworzenia kopii zapasowej, pod warunkiem że spełnione są następujące wymogi:

(i) bezpieczeństwo skopiowanych zbiorów danych musi być na tym samym poziomie co w przypadku oryginalnych zbiorów danych;

(ii) liczba skopiowanych zbiorów danych nie może przekraczać minimum niezbędnego do zapewnienia ciągłości usługi;

▼M1

c) spełnia wszelkie wymogi określone w raporcie z certyfikacji konkretnego kwalifikowanego urządzenia do składania podpisu elektronicznego na odległość, wydanym zgodnie z art. 30.

2. Do dnia 21 maja 2025 r. Komisja, w drodze aktów wykonawczych, ustanowi wykaz norm referencyjnych oraz, w razie potrzeby, specyfikacje i procedury do celów ust. 1 niniejszego artykułu. Te akty wykonawcze przyjmuje się zgodnie z procedurą sprawdzającą, o której mowa w art. 48 ust. 2.

▼B

Artykuł 30

Certyfikacja kwalifikowanych urządzeń do składania podpisu elektronicznego

1. Zgodność kwalifikowanych urządzeń do składania podpisu elektronicznego z wymogami określonymi w załączniku II jest certyfikowana przez odpowiednie publiczne lub prywatne podmioty wyznaczone przez państwa członkowskie.

2. Państwa członkowskie zgłaszają Komisji nazwy i adresy podmiotów publicznych lub prywatnych, o których mowa w ust. 1. Komisja udostępnia te informacje państwom członkowskim.

3. Certyfikacja, o której mowa w ust. 1, opiera się na następujących elementach:

a) procedurze oceny bezpieczeństwa, przeprowadzanej zgodnie z jedną z norm dotyczących oceny bezpieczeństwa produktów informatycznych uwzględnionych na liście sporządzonej zgodnie z akapitem drugim; lub

b) procedurze innej niż procedura, o której mowa w lit. a), pod warunkiem że w procedurze tej stosuje się porównywalne poziomy bezpieczeństwa i podmiot publiczny lub prywatny, o którym mowa w ust. 1, zgłosi tę procedurę Komisji. Procedura ta może zostać zastosowana wyłącznie w razie braku norm, o których mowa w lit. a), lub gdy procedura oceny bezpieczeństwa, o której mowa w lit. a), wciąż trwa.

Komisja sporządza w drodze aktów wykonawczych listę norm dotyczących oceny bezpieczeństwa produktów informatycznych, o których mowa w lit. a). Te akty wykonawcze przyjmuje się zgodnie z procedurą sprawdzającą, o której mowa w art. 48 ust. 2

▼M1

3a. Ważność certyfikacji, o której mowa w ust. 1, nie może przekraczać pięciu lat, pod warunkiem że co dwa lata przeprowadza się ocenę podatności na zagrożenia. W przypadku gdy zostaną stwierdzone podatności na zagrożenia i nie zostaną one wyeliminowane, certyfikacja zostaje odwołana.

▼B

4. Komisja jest uprawniona do przyjmowania aktów delegowanych, zgodnie z art. 47, dotyczących ustanowienia specjalnych kryteriów, które muszą spełniać wyznaczone podmioty, o których mowa w ust. 1 niniejszego artykułu.

▼B

Artykuł 31

Publikacja listy certyfikowanych kwalifikowanych urządzeń do składania podpisu elektronicznego

1. Bez zbędnej zwłoki i nie później niż jeden miesiąc po zakończeniu certyfikacji państwa członkowskie przekazują Komisji informacje o kwalifikowanych urządzeniach do składania podpisu elektronicznego, które uzyskały certyfikaty od podmiotów, o których mowa w art. 30 ust. 1. Bez zbędnej zwłoki i nie później niż jeden miesiąc po odwołaniu certyfikacji państwa członkowskie przekazują również Komisji informacje o urządzeniach do składania podpisu elektronicznego, które nie są już certyfikowane.

2. Na podstawie otrzymanych informacji Komisja sporządza, publikuje i prowadzi listę certyfikowanych kwalifikowanych urządzeń do składania podpisu elektronicznego.

▼M1

3. Do dnia 21 maja 2025 r. Komisja, w drodze aktów wykonawczych, ustanowi formaty i procedury mające zastosowanie do celów ust. 1 niniejszego artykułu. Te akty wykonawcze przyjmuje się zgodnie z procedurą sprawdzającą, o której mowa w art. 48 ust. 2.

▼B

Artykuł 32

Wymogi dla walidacji kwalifikowanych podpisów elektronicznych

1. Proces walidacji kwalifikowanego podpisu elektronicznego potwierdza ważność kwalifikowanego podpisu elektronicznego, pod warunkiem że:

a) certyfikat, który towarzyszy podpisowi, był w momencie składania podpisu kwalifikowanym certyfikatem podpisu elektronicznego zgodnym z załącznikiem I;

b) kwalifikowany certyfikat został wydany przez kwalifikowanego dostawcę usług zaufania i był ważny w momencie składania podpisu;

c) dane służące do walidacji podpisu odpowiadają danym dostarczonym stronie ufającej;

d) unikalny zestaw danych reprezentujących podpisującego umieszczony w certyfikacie jest prawidłowo dostarczony stronie ufającej;

e) jeżeli w momencie składania podpisu użyty został pseudonim, zostaje to wyraźnie wskazane stronie ufającej;

f) podpis elektroniczny został złożony za pomocą kwalifikowanego urządzenia do składania podpisu elektronicznego;

g) integralność podpisanych danych nie została naruszona;

h) wymogi przewidziane w art. 26 zostały spełnione w momencie składania podpisu.

▼M1

W przypadku gdy walidacja kwalifikowanych podpisów elektronicznych jest zgodna z normami, specyfikacjami i procedurami, o których mowa w ust. 3, domniemywa się zgodność z wymogami określonymi w akapicie pierwszym niniejszego ustępu.

▼B

2. System wykorzystany do walidacji kwalifikowanego podpisu elektronicznego zapewnia stronie ufającej prawidłowy wynik procesu walidacji i umożliwia stronie ufającej wykrycie wszelkich problemów związanych z bezpieczeństwem.

▼M1

3. Do dnia 21 maja 2025 r. Komisja, w drodze aktów wykonawczych, sporządzi wykaz norm referencyjnych oraz, w razie potrzeby, ustanowi specyfikacje i procedury do celów walidacji kwalifikowanych podpisów elektronicznych. Te akty wykonawcze przyjmuje się zgodnie z procedurą sprawdzającą, o której mowa w art. 48 ust. 2.

Artykuł 32a

Wymogi dotyczące walidacji zaawansowanych podpisów elektronicznych opartych na kwalifikowanych certyfikatach

1. Proces walidacji zaawansowanego podpisu elektronicznego opartego na kwalifikowanym certyfikacie potwierdza ważność zaawansowanego podpisu elektronicznego opartego na kwalifikowanym certyfikacie, pod warunkiem że:

a) certyfikat, który towarzyszy podpisowi, był w momencie składania podpisu kwalifikowanym certyfikatem podpisu elektronicznego zgodnym z załącznikiem I;

b) kwalifikowany certyfikat został wydany przez kwalifikowanego dostawcę usług zaufania i był ważny w momencie składania podpisu;

c) dane służące do walidacji podpisu odpowiadają danym dostarczonym stronie ufającej;

d) niepowtarzalny zestaw danych reprezentujących podpisującego umieszczony w certyfikacie jest prawidłowo dostarczony stronie ufającej;

e) jeżeli w momencie składania podpisu użyty został pseudonim, zostaje to wyraźnie wskazane stronie ufającej;

f) integralność podpisanych danych nie została skompromitowana;

g) wymogi przewidziane w art. 26 zostały spełnione w momencie składania podpisu.

2. System wykorzystany do walidacji zaawansowanego podpisu elektronicznego opartego na kwalifikowanym certyfikacie musi zapewniać stronie ufającej prawidłowy wynik procesu walidacji oraz umożliwiać stronie ufającej wykrycie wszelkich problemów związanych z bezpieczeństwem.

3. Do dnia 21 maja 2025 r. Komisja, w drodze aktów wykonawczych, sporządzi wykaz norm referencyjnych oraz, w razie potrzeby, ustanowi specyfikacje i procedury w odniesieniu do walidacji zaawansowanych podpisów elektronicznych opartych na kwalifikowanych certyfikatach. W przypadku gdy walidacja zaawansowanych podpisów elektronicznych opartych na kwalifikowanych certyfikatach jest zgodna z tymi normami, specyfikacjami i procedurami, domniemywa się zgodność z wymogami określonymi w ust. 1 niniejszego artykułu. Te akty wykonawcze przyjmuje się zgodnie z procedurą sprawdzającą, o której mowa w art. 48 ust. 2.

▼B

Artykuł 33

Kwalifikowana usługa walidacji kwalifikowanych podpisów elektronicznych

1. Kwalifikowaną usługę walidacji kwalifikowanych podpisów elektronicznych może świadczyć wyłącznie kwalifikowany dostawca usług zaufania, który:

a) zapewnia walidację zgodnie z art. 32 ust. 1; oraz

b) umożliwia stronom ufającym otrzymanie wyniku procesu walidacji w automatyczny, wiarygodny i skuteczny sposób oraz przy użyciu zaawansowanego podpisu elektronicznego lub zaawansowanej pieczęci elektronicznej dostawcy kwalifikowanej usługi walidacji.

▼M1

2. Do dnia 21 maja 2025 r. Komisja, w drodze aktów wykonawczych, sporządzi wykaz norm referencyjnych oraz, w razie potrzeby, ustanowi specyfikacje i procedury w odniesieniu do kwalifikowanej usługi walidacji, o której mowa w ust. 1 niniejszego artykułu. W przypadku gdy kwalifikowana usługa walidacji kwalifikowanych podpisów elektronicznych jest zgodna z tymi normami, specyfikacjami i procedurami, domniemywa się zgodność z wymogami określonymi w ust. 1 niniejszego artykułu. Te akty wykonawcze przyjmuje się zgodnie z procedurą sprawdzającą, o której mowa w art. 48 ust. 2.

▼B

Artykuł 34

Kwalifikowana usługa konserwacji kwalifikowanych podpisów elektronicznych

1. Kwalifikowaną usługę konserwacji kwalifikowanych podpisów elektronicznych może świadczyć wyłącznie kwalifikowany dostawca usług zaufania, który stosuje procedury i technologie umożliwiające przedłużenie wiarygodności kwalifikowanego podpisu elektronicznego poza techniczny okres ważności.

▼M1

1a. W przypadku gdy ustalenia w zakresie kwalifikowanej usługi konserwacji kwalifikowanych podpisów elektronicznych są zgodne z normami, specyfikacjami i procedurami, o których mowa w ust. 2, domniemywa się zgodność z wymogami określonymi w ust. 1.

2. Do dnia 21 maja 2025 r. Komisja, w drodze aktów wykonawczych, sporządzi wykaz norm referencyjnych oraz, w razie potrzeby, ustanowi specyfikacje i procedury do celów kwalifikowanej usługi konserwacji kwalifikowanych podpisów elektronicznych. Te akty wykonawcze przyjmuje się zgodnie z procedurą sprawdzającą, o której mowa w art. 48 ust. 2.

▼B

SEKCJA 5

Pieczęcie elektroniczne

Artykuł 35

Skutki prawne pieczęci elektronicznych

1. Pieczęci elektronicznej nie można odmówić skutku prawnego ani dopuszczalności jako dowodu w postępowaniu sądowym wyłącznie z tego powodu, że pieczęć ta ma postać elektroniczną lub że nie spełnia wymogów dla kwalifikowanych pieczęci elektronicznych.

2. Kwalifikowana pieczęć elektroniczna korzysta z domniemania integralności danych i autentyczności pochodzenia tych danych, z którymi kwalifikowana pieczęć elektroniczna jest powiązana.

▼M1

_____

▼B

Artykuł 36

Wymogi dla zaawansowanych pieczęci elektronicznych

►M1 1. ◄ Zaawansowana pieczęć elektroniczna musi spełniać następujące wymogi:

a) jest unikalnie przyporządkowana podmiotowi składającemu pieczęć;

b) umożliwia ustalenie tożsamości podmiotu składającego pieczęć;

c) jest składana przy użyciu danych służących do składania pieczęci elektronicznej, które podmiot składający pieczęć może, mając je z dużą dozą pewności pod swoją kontrolą, użyć do złożenia pieczęci elektronicznej; oraz

d) jest powiązana z danymi, do których się odnosi, w taki sposób, że każda późniejsza zmiana danych jest rozpoznawalna.

▼M1

2. Do dnia 21 maja 2026 r. Komisja oceni, czy należy konieczne jest przyjęcie aktów wykonawczych w celu sporządzenia wykazu norm referencyjnych oraz, w razie potrzeby, ustanowienia specyfikacji i procedur w odniesieniu do zaawansowanych pieczęci elektronicznych. Komisja może przyjąć takie akty wykonawcze na podstawie tej oceny. W przypadku gdy zaawansowane pieczęcie elektroniczne są zgodne z tymi normami, specyfikacjami i procedurami, domniemywa się zgodność z wymogami dotyczącymi zaawansowanych pieczęci elektronicznych. Te akty wykonawcze przyjmuje się zgodnie z procedurą sprawdzającą, o której mowa w art. 48 ust. 2.

▼B

Artykuł 37

Pieczęcie elektroniczne w usługach publicznych

1. Jeżeli państwo członkowskie wymaga zaawansowanej pieczęci elektronicznej do skorzystania z usługi *online* oferowanej przez podmiot sektora publicznego lub w jego imieniu, to państwo członkowskie uznaje zaawansowane pieczęcie elektroniczne, zaawansowane pieczęcie elektroniczne oparte na kwalifikowanym certyfikacie pieczęci elektronicznych i kwalifikowane pieczęcie elektroniczne co najmniej w formatach lub wykorzystujące metody określone w aktach wykonawczych, o których mowa w ust. 5.

▼B

2. Jeżeli państwo członkowskie wymaga zaawansowanej pieczęci elektronicznej opartej na kwalifikowanym certyfikacie do skorzystania z usługi *online* oferowanej przez podmiot sektora publicznego lub w jego imieniu, to państwo członkowskie uznaje zaawansowane pieczęcie elektroniczne oparte na kwalifikowanym certyfikacie i kwalifikowane pieczęcie elektroniczne co najmniej w formatach lub wykorzystujące metody określone w aktach wykonawczych, o których mowa w ust. 5.

3. W przypadku transgranicznego użycia w usłudze *online* oferowanej przez podmiot sektora publicznego państwa członkowskie nie wymagają pieczęci elektronicznej o wyższym poziomie bezpieczeństwa niż kwalifikowana pieczęć elektroniczna.

▼M1

_____

▼B

5. Do dnia 18 września 2015 r. i przy uwzględnieniu istniejących praktyk, standardów i aktów prawnych Unii Komisja określa w drodze aktów wykonawczych formaty referencyjne zaawansowanych pieczęci elektronicznych lub metody referencyjne, w przypadku gdy używane są formaty alternatywne. Te akty wykonawcze przyjmuje się zgodnie z procedurą sprawdzającą, o której mowa w art. 48 ust. 2.

Artykuł 38

Kwalifikowane certyfikaty pieczęci elektronicznej

1. Kwalifikowane certyfikaty pieczęci elektronicznych muszą spełniać wymogi określone w załączniku III.

2. Kwalifikowane certyfikaty pieczęci elektronicznych nie podlegają żadnym obowiązkowym wymogom wykraczającym poza wymogi określone w załączniku III.

3. Kwalifikowane certyfikaty pieczęci elektronicznych mogą zawierać nieobowiązkowe dodatkowe szczególne atrybuty. Atrybuty te nie mogą wpływać na interoperacyjność i uznawanie kwalifikowanych pieczęci elektronicznych.

4. Jeżeli kwalifikowany certyfikat pieczęci elektronicznej został unieważniony po początkowej aktywacji, traci on ważność od momentu jego unieważnienia i w żadnym przypadku nie można przywrócić jego poprzedniego statusu.

5. Państwa członkowskie mogą ustanawiać przepisy krajowe dotyczące tymczasowego zawieszenia kwalifikowanych certyfikatów pieczęci elektronicznych z zastrzeżeniem następujących warunków:

a) jeżeli kwalifikowany certyfikat pieczęci elektronicznej został czasowo zawieszony, certyfikat ten traci ważność na okres zawieszenia;

b) okres zawieszenia jest jasno wskazywany w bazie danych dotyczącej certyfikatów i podmiot udzielający informacji o statusie certyfikatu zapewnia widoczność statusu zawieszenia podczas okresu zawieszenia.

▼M1

6. Do dnia 21 maja 2025 r. Komisja, w drodze aktów wykonawczych, sporządzi wykaz norm referencyjnych oraz, w razie potrzeby, ustanowi specyfikacje i procedury w odniesieniu do kwalifikowanych certyfikatów pieczęci elektronicznych. W przypadku gdy kwalifikowany certyfikat pieczęci elektronicznej jest zgodny z tymi normami, specyfikacjami i procedurami, domniemywa się zgodność z wymogami określonymi w załączniku III. Te akty wykonawcze przyjmuje się zgodnie z procedurą sprawdzającą, o której mowa w art. 48 ust. 2.

▼B

Artykuł 39

Kwalifikowane urządzenia do składania pieczęci elektronicznej

1. Art. 29 stosuje się odpowiednio do wymogów dotyczących kwalifikowanych urządzeń do składania pieczęci elektronicznej.

2. Art. 30 stosuje się odpowiednio do certyfikacji kwalifikowanych urządzeń do składania pieczęci elektronicznej.

3. Art. 31 stosuje się odpowiednio do publikacji listy certyfikowanych kwalifikowanych urządzeń do składania pieczęci elektronicznej.

▼M1

Artykuł 39a

Wymogi dotyczące kwalifikowanej usługi zarządzania kwalifikowanymi urządzeniami do składania pieczęci elektronicznej na odległość

Art. 29a stosuje się odpowiednio do kwalifikowanej usługi zarządzania kwalifikowanymi urządzeniami do składania pieczęci elektronicznej na odległość.

▼B

Artykuł 40

Walidacja i konserwacja kwalifikowanych pieczęci elektronicznych

Art. 32, 33 i 34 stosuje się odpowiednio do walidacji i konserwacji kwalifikowanych pieczęci elektronicznych.

▼M1

Artykuł 40a

Wymogi dotyczące walidacji zaawansowanych pieczęci elektronicznych opartych na kwalifikowanych certyfikatach

Art. 32a stosuje się odpowiednio do walidacji zaawansowanych pieczęci elektronicznych opartych na kwalifikowanych certyfikatach.

▼B

SEKCJA 6

Elektroniczne znaczniki czasu

Artykuł 41

Skutki prawne elektronicznych znaczników czasu

1. Nie jest kwestionowany prawny skutek elektronicznego znacznika czasu ani jego dopuszczalność jako dowodu w postępowaniu sądowym wyłącznie z tego powodu, że znacznik ten ma postać elektroniczną lub że nie spełnia wymogów kwalifikowanego elektronicznego znacznika czasu.

2. Kwalifikowany elektroniczny znacznik czasu korzysta z domniemania dokładności daty i czasu, jakie wskazuje, oraz integralności danych, z którymi wskazywane data i czas są połączone.

▼M1

———————

▼B

Artykuł 42

Wymogi dla kwalifikowanych elektronicznych znaczników czasu

1. Kwalifikowany elektroniczny znacznik czasu musi spełniać następujące wymogi:

a) wiąże on datę i czas z danymi tak, aby w wystarczający sposób wykluczyć możliwość niewykrywalnej zmiany danych;

b) oparty jest na precyzyjnym źródle czasu powiązanym z uniwersalnym czasem koordynowanym; oraz

c) jest podpisany przy użyciu zaawansowanego podpisu elektronicznego lub opatrzony zaawansowaną pieczęcią elektroniczną kwalifikowanego dostawcy usług zaufania lub w inny równoważny sposób.

▼M1

1a. W przypadku gdy powiązanie daty i czasu z danymi oraz precyzyjność źródła czasu są zgodne z normami, specyfikacjami i procedurami, o których mowa w ust. 2, domniemywa się zgodność z wymogami określonymi w ust. 1.

2. Do dnia 21 maja 2025 r. Komisja, w drodze aktów wykonawczych, sporządzi wykaz norm referencyjnych oraz, w razie potrzeby, ustanowi specyfikacje i procedury dotyczące powiązania daty i czasu z danymi oraz precyzyjnych źródeł czasu. Te akty wykonawcze przyjmuje się zgodnie z procedurą sprawdzającą, o której mowa w art. 48 ust. 2.

▼B

SEKCJA 7

Usługi rejestrowanego doręczenia elektronicznego

Artykuł 43

Skutek prawny usługi rejestrowanego doręczenia elektronicznego

1. Nie jest kwestionowany skutek prawny danych wysłanych i otrzymanych przy użyciu usługi rejestrowanego doręczenia elektronicznego ani ich dopuszczalność jako dowodu w postępowaniu sądowym wyłącznie z tego powodu, że dane te mają postać elektroniczną lub że nie spełniają wszystkich wymogów kwalifikowanej usługi rejestrowanego doręczenia elektronicznego.

2. Dane wysłane i otrzymane przy użyciu kwalifikowanej usługi rejestrowanego doręczenia elektronicznego korzystają z domniemania integralności danych, wysłania tych danych przez zidentyfikowanego nadawcę i otrzymania ich przez zidentyfikowanego adresata oraz dokładności daty i czasu wysłania i otrzymania wskazanych przez kwalifikowaną usługę rejestrowanego doręczenia elektronicznego.

Artykuł 44

Wymogi dla kwalifikowanych usług rejestrowanego doręczenia elektronicznego

1. Kwalifikowane usługi rejestrowanego doręczenia elektronicznego muszą spełniają następujące wymogi:

▼B

a) są świadczone przez co najmniej jednego kwalifikowanego dostawcę usług zaufania;

b) z dużą dozą pewności zapewniają identyfikację nadawcy;

c) zapewniają identyfikację adresata przed dostarczeniem danych;

d) wysłanie i otrzymanie danych jest zabezpieczone zaawansowanym podpisem elektronicznym lub zaawansowaną pieczęcią elektroniczną kwalifikowanego dostawcy usług zaufania w taki sposób, by wykluczyć możliwość niewykrywalnej zmiany danych;

e) każda zmiana danych niezbędna do celów wysłania lub otrzymania danych jest wyraźnie wskazana nadawcy i adresatowi danych;

f) data i czas wysłania, otrzymania i wszelkiej zmiany danych są wskazane za pomocą kwalifikowanego elektronicznego znacznika czasu.

W przypadku przesyłania danych między co najmniej dwoma kwalifikowanymi dostawcami usług zaufania wymogi określone w lit. a)–f) mają zastosowanie do wszystkich kwalifikowanych dostawców usług zaufania.

▼M1

1a. W przypadku gdy proces wysyłania i otrzymywania danych jest zgodny z normami, specyfikacjami i procedurami, o których mowa w ust. 2, domniemywa się zgodność z wymogami określonymi w ust. 1.

2. Do dnia 21 maja 2025 r. Komisja, w drodze aktów wykonawczych, sporządzi wykaz norm referencyjnych oraz, w razie potrzeby, ustanowi specyfikacje i procedury dotyczące procesu wysyłania i otrzymywania danych. Te akty wykonawcze przyjmuje się zgodnie z procedurą sprawdzającą, o której mowa w art. 48 ust. 2.

2a. Dostawcy kwalifikowanych usług rejestrowanego doręczenia elektronicznego mogą uzgodnić interoperacyjność świadczonych przez nich kwalifikowanych usług rejestrowanego doręczenia elektronicznego. Takie ramy interoperacyjności muszą być zgodne z wymogami określonymi w ust. 1, a zgodność ta musi zostać potwierdzona przez jednostkę oceniającą zgodność.

2b. Komisja może, w drodze aktów wykonawczych, sporządzić wykaz norm referencyjnych oraz, w razie potrzeby, ustanowić specyfikacje i procedury dotyczące ram interoperacyjności, o których mowa w ust. 2a niniejszego artykułu. Specyfikacje techniczne i treść norm muszą być efektywne kosztowo i proporcjonalne. Te akty wykonawcze przyjmuje się zgodnie z procedurą sprawdzającą, o której mowa w art. 48 ust. 2.

▼B

SEKCJA 8

Uwierzytelnianie witryn internetowych

▼M1

Artykuł 45

Wymogi dla kwalifikowanych certyfikatów uwierzytelniania witryn internetowych

1. Kwalifikowane certyfikaty uwierzytelniania witryn internetowych muszą spełniać wymogi określone w załączniku IV. Ocenę zgodności z tymi wymogami przeprowadza się zgodnie z normami, specyfikacjami i procedurami, o których mowa w ust. 2 niniejszego artykułu.

1a. Kwalifikowane certyfikaty uwierzytelniania witryn internetowych wydane zgodnie z ust. 1 niniejszego artykułu, muszą być rozpoznawane przez dostawców przeglądarek internetowych. Dostawcy przeglądarek internetowych muszą zapewniać, aby dane dotyczące tożsamości poświadczone w certyfikacie oraz dodatkowe poświadczone atrybuty były wyświetlane w sposób przyjazny dla użytkownika. Dostawcy przeglądarek internetowych zapewniają obsługę kwalifikowanych certyfikatów uwierzytelniania witryn internetowych, o których mowa w ust. 1 niniejszego artykułu, oraz interoperacyjność z tymi certyfikatami, z wyjątkiem mikroprzedsiębiorstw lub małych przedsiębiorstw zdefiniowanych w art. 2 załącznika do zalecenia Komisji 2003/361/WE, w ciągu pierwszych pięciu lat ich działalności w charakterze dostawców usług przeglądania stron internetowych.

1b. Kwalifikowane certyfikaty uwierzytelniania witryn internetowych nie podlegają jakimkolwiek obowiązkowym wymogom innym niż wymogi określone w ust. 1.

2. Do dnia 21 maja 2025 r. Komisja, w drodze aktów wykonawczych, sporządzi wykaz norm referencyjnych oraz, w razie potrzeby, ustanowi specyfikacje i procedury w odniesieniu do kwalifikowanych certyfikatów uwierzytelniania witryn internetowych, o których mowa w ust. 1 niniejszego artykułu. Te akty wykonawcze przyjmuje się zgodnie z procedurą sprawdzającą, o której mowa w art. 48 ust. 2.

Artykuł 45a

Środki zapobiegawcze w zakresie cyberbezpieczeństwa

1. Dostawcy przeglądarek internetowych nie mogą wprowadzać jakichkolwiek środków sprzecznych z ich obowiązkami określonymi w art. 45, w szczególności wymogów uznawania kwalifikowanych certyfikatów uwierzytelniania witryn internetowych oraz wyświetlania dostarczonych danych dotyczących tożsamości w sposób przyjazny dla użytkownika.

2. Na zasadzie odstępstwa od ust. 1 oraz jedynie w przypadku uzasadnionych podejrzeń związanych z naruszeniem bezpieczeństwa lub utratą integralności konkretnego certyfikatu lub zestawu certyfikatów, dostawcy przeglądarek internetowych mogą wprowadzać środki zapobiegawcze w odniesieniu do tego certyfikatu lub zestawu certyfikatów.

3. W przypadku gdy dostawca przeglądarki internetowej wprowadza takie środki zapobiegawcze na podstawie ust. 2, bez zbędnej zwłoki zgłasza swoje podejrzenia na piśmie – wraz z opisem środków wprowadzonych w reakcji na te podejrzenia – Komisji, właściwemu organowi nadzorczemu, podmiotowi, któremu wydano dany certyfikat, oraz

▼M1

kwalifikowanemu dostawcy usług zaufania, który wydał dany certyfikat lub zestaw certyfikatów. Po otrzymaniu takiego zgłoszenia właściwy organ nadzorczy wydaje danemu dostawcy przeglądarki internetowej potwierdzenie otrzymania.

4. Właściwy organ nadzoru bada kwestie zawarte w zgłoszeniu zgodnie z art. 46b ust. 4 lit. k). W przypadku gdy w wyniku tego dochodzenia nie odebrano statusu certyfikatu kwalifikowanego, organ nadzoru informuje o tym odpowiednio danego dostawcę przeglądarki internetowej oraz zwraca się do tego dostawcy o zakończenie środków zapobiegawczych, o których mowa w ust. 2 niniejszego artykułu.

SEKCJA 9

elektroniczne poświadczenie atrybutów

Artykuł 45b

Skutki prawne elektronicznego poświadczenia atrybutów

1. Elektronicznemu poświadczeniu atrybutów nie można odmówić skutku prawnego ani dopuszczalności jako dowodu w postępowaniu sądowym wyłącznie z tego powodu, że ma postać elektroniczną lub że nie spełnia wymogów dotyczących kwalifikowanych elektronicznych poświadczeń atrybutów.

2. Kwalifikowane elektroniczne poświadczenie atrybutów oraz poświadczenia atrybutów wydane przez podmiot sektora publicznego odpowiedzialny za źródło autentyczne lub w jego imieniu ma taki sam skutek prawny jak poświadczenia wydane zgodnie z prawem w postaci papierowej.

3. Poświadczenie atrybutów wydane przez podmiot sektora publicznego odpowiedzialny za źródło autentyczne lub w jego imieniu w jednym z państw członkowskich uznaje się za poświadczenie atrybutów wydane przez podmiot sektora publicznego odpowiedzialny za źródło autentyczne lub w jego imieniu we wszystkich państwach członkowskich.

Artykuł 45c

Elektroniczne poświadczenie atrybutów w usługach publicznych

W przypadku gdy zgodnie z prawem krajowym dostęp do usługi online świadczonej przez podmiot sektora publicznego wymaga identyfikacji elektronicznej przy użyciu środka identyfikacji elektronicznej oraz uwierzytelnienia, dane identyfikujące osobę w elektronicznym poświadczeniu atrybutów nie zastępują identyfikacji elektronicznej przy użyciu środków identyfikacji elektronicznej i uwierzytelniania przy identyfikacji elektronicznej, chyba że państwo członkowskie wyraźnie na to zezwoli. W takim przypadku akceptuje się również kwalifikowane elektroniczne poświadczenia atrybutów wydane w innych państwach członkowskich.

Artykuł 45d

Wymogi dotyczące kwalifikowanego elektronicznego poświadczenia atrybutów

1. Kwalifikowane elektroniczne poświadczenie atrybutów musi spełniać wymogi określone w załączniku V.

▼M1

2. Ocenę zgodności z wymogami określonymi w załączniku V przeprowadza się zgodnie z normami, specyfikacjami i procedurami, o których mowa w ust. 5 niniejszego artykułu.

3. Kwalifikowane elektroniczne poświadczenia atrybutów nie podlegają jakimkolwiek obowiązkowym wymogom oprócz wymogów określonych w załączniku V.

4. W przypadku gdy kwalifikowane elektroniczne poświadczenie atrybutów zostało unieważnione po wydaniu, traci ono ważność z chwilą jego unieważnienia i w żadnym przypadku nie można przywrócić jego poprzedniego statusu.

5. Do dnia 21 listopada 2024 r. Komisja, w drodze aktów wykonawczych, sporządzi wykaz norm referencyjnych oraz, w razie potrzeby, ustanowi specyfikacje i procedury dotyczące kwalifikowanych elektronicznych poświadczeń atrybutów. Te akty wykonawcze muszą być spójne z aktami wykonawczymi, o których mowa w art. 5a ust. 23, dotyczącymi wdrożenia europejskiego portfela tożsamości cyfrowej. Przyjmuje się je zgodnie z procedurą sprawdzającą, o której mowa w art. 48 ust. 2.

Artykuł 45e

Weryfikacja atrybutów na podstawie źródeł autentycznych

1. Państwa członkowskie zapewniają, w terminie 24 miesięcy od dnia wejścia w życie aktów wykonawczych, o których mowa w art. 5a ust. 23 i art. 5c ust. 6, aby przynajmniej w odniesieniu do atrybutów wymienionych w załączniku VI, w przypadku gdy atrybuty te polegają na źródłach autentycznych w sektorze publicznym, wprowadzono środki umożliwiające kwalifikowanym dostawcom usług zaufania, którzy dostarczają kwalifikowane elektroniczne poświadczenia atrybutów, weryfikację tych atrybutów drogą elektroniczną, na żądanie użytkownika, zgodnie z prawem Unii lub prawem krajowym.

2. Do dnia 21 listopada 2024 r. Komisja, uwzględniając odpowiednie normy międzynarodowe, sporządzi, w drodze aktów wykonawczych, wykaz norm referencyjnych oraz, w razie potrzeby, ustanowi specyfikacje i procedury w odniesieniu do katalogu atrybutów, a także systemów poświadczania atrybutów i procedur weryfikacji kwalifikowanych elektronicznych poświadczeń atrybutów do celów ust. 1 niniejszego artykułu. Te akty wykonawcze muszą być spójne z aktami wykonawczymi, o których mowa w art. 5a ust. 23, dotyczącymi wdrożenia europejskich portfeli tożsamości cyfrowej. Te akty wykonawcze przyjmuje się zgodnie z procedurą sprawdzającą, o której mowa w art. 48 ust. 2.

Artykuł 45f

Wymogi dotyczące elektronicznego poświadczenia atrybutów wydanego przez podmiot sektora publicznego odpowiedzialny za źródło autentyczne lub w jego imieniu

1. Elektroniczne poświadczenie atrybutów wydane przez podmiot sektora publicznego odpowiedzialny za źródło autentyczne lub w jego imieniu musi spełniać następujące wymogi:

a) wymogi określone w załączniku VII;

▼M1

b) kwalifikowany certyfikat towarzyszący kwalifikowanemu podpisowi elektronicznemu lub kwalifikowanej pieczęci elektronicznej podmiotu sektora publicznego, o którym mowa w art. 3 pkt 46, zidentyfikowanego jako wydawca, o którym mowa w załączniku VII lit. b), zawiera określony zestaw certyfikowanych atrybutów w formie nadającej się do automatycznego przetwarzania oraz:

(i) wskazanie, że podmiot wydający został ustanowiony zgodnie z prawem Unii lub prawem krajowym jako podmiot odpowiedzialny za źródło autentyczne, na podstawie którego wydawane jest elektroniczne poświadczenie atrybutów, lub jako podmiot wyznaczony do działania w jego imieniu;

(ii) dostarczenie zestawu danych jednoznacznie reprezentujących źródło autentyczne, o którym mowa w ppkt (i); oraz

(iii) wskazanie prawa Unii lub prawa krajowego, o którym mowa w ppkt (i).

2. Państwo członkowskie, w którym mają siedzibę podmioty sektora publicznego, o których mowa w art. 3 pkt 46, zapewnia, aby podmioty sektora publicznego, które wydają elektroniczne poświadczenia atrybutów, zapewniały poziom rzetelności i wiarygodności równoważny kwalifikowanym dostawcom usług zaufania zgodnie z art. 24.

3. Państwa członkowskie notyfikują Komisji podmioty sektora publicznego, o których mowa w art. 3 pkt 46. Notyfikacja ta obejmuje raport z oceny zgodności wydany przez jednostkę oceniającą zgodność, potwierdzający spełnienie wymogów określonych w ust. 1, 2 i 6 niniejszego artykułu. Komisja – przy użyciu zabezpieczonego kanału komunikacji – udostępnia publicznie wykaz podmiotów sektora publicznego, o których mowa w ust. 3 pkt 46, w postaci pozwalającej na automatyczne przetwarzanie, elektronicznie podpisany lub opatrzony pieczęcią elektroniczną.

4. W przypadku gdy elektroniczne poświadczenie atrybutów wydane przez podmiot sektora publicznego odpowiedzialny za źródło autentyczne lub w jego imieniu zostało unieważnione po wydaniu, traci ono ważność od momentu jego unieważnienia i nie można przywrócić jego poprzedniego statusu.

5. Elektroniczne poświadczenie atrybutów wydane przez podmiot sektora publicznego odpowiedzialny za źródło autentyczne lub w jego imieniu uznaje się za zgodne z wymogami określonymi w ust. 1, w przypadku gdy przestrzega ono norm, specyfikacji i procedur, o których mowa w ust. 6.

6. Do dnia 21 listopada 2024 r. Komisja, w drodze aktów wykonawczych, sporządzi wykaz norm referencyjnych oraz, w razie potrzeby, ustanowi specyfikacje i procedury w odniesieniu do elektronicznego poświadczania atrybutów wydawanego przez podmiot sektora publicznego odpowiedzialny za źródło autentyczne lub w jego imieniu. Te akty wykonawcze muszą być spójne z aktami wykonawczymi, o których mowa w art. 5a ust. 23, dotyczącymi wdrożenia europejskiego portfela tożsamości cyfrowej. Przyjmuje się je zgodnie z procedurą sprawdzającą, o której mowa w art. 48 ust. 2.

▼M1

7. Do dnia 21 listopada 2024 r. Komisja, w drodze aktów wykonawczych, sporządzi wykaz norm referencyjnych oraz, w razie potrzeby, ustanowi specyfikacje i procedury do celów ust. 3 niniejszego artykułu. Te akty wykonawcze muszą być spójne z aktami wykonawczymi, o których mowa w art. 5a ust. 23, dotyczącymi wdrożenia europejskiego portfela tożsamości cyfrowej. Przyjmuje się je zgodnie z procedurą sprawdzającą, o której mowa w art. 48 ust. 2.

8. Podmioty sektora publicznego, o których mowa w art. 3 pkt 46, wydające elektroniczne poświadczenie atrybutów zapewniają interfejs z europejskimi portfelami tożsamości cyfrowej, które są zapewniane zgodnie z art. 5a.

Artykuł 45g

Wydawanie elektronicznych poświadczeń atrybutów do europejskich portfeli tożsamości cyfrowej

1. Dostawcy elektronicznych poświadczeń atrybutów zapewniają użytkownikom europejskiego portfela tożsamości cyfrowej możliwość żądania, otrzymywania i przechowywania elektronicznego poświadczenia atrybutów, a także zarządzania nim, niezależnie od państwa członkowskiego, w którym zapewniany jest europejski portfel tożsamości cyfrowej.

2. Dostawcy kwalifikowanych elektronicznych poświadczeń atrybutów zapewniają interfejs z europejskimi portfelami tożsamości cyfrowej, które są zapewniane zgodnie z art. 5a.

Artykuł 45h

Dodatkowe przepisy w odniesieniu do świadczenia usług elektronicznego poświadczania atrybutów

1. Dostawcy kwalifikowanych i niekwalifikowanych usług elektronicznego poświadczania atrybutów nie mogą łączyć danych osobowych związanych ze świadczeniem tych usług z danymi osobowymi pochodzącymi z jakichkolwiek innych usług oferowanych przez nich lub przez ich partnerów handlowych.

2. Dane osobowe związane ze świadczeniem usług elektronicznego poświadczania atrybutów muszą być logicznie oddzielone od wszelkich innych danych przechowywanych przez dostawcę elektronicznego poświadczenia atrybutów.

3. Dostawcy usług kwalifikowanych elektronicznego poświadczania atrybutów wdrażają świadczenie takich kwalifikowanych usług zaufania w sposób, który jest funkcjonalnie oddzielony od innych świadczonych przez nich usług.

SEKCJA 10

usługi archiwizacji elektronicznej

Artykuł 45i

Skutki prawne usług archiwizacji elektronicznej

1. Danym elektronicznym oraz elektronicznym dokumentom przechowywanym przy użyciu usługi archiwizacji elektronicznej nie można odmówić skutku prawnego ani dopuszczalności jako dowodu

▼M1

w postępowaniu sądowym wyłącznie z tego powodu, że dane te mają postać elektroniczną lub że nie są przechowywane przy użyciu kwalifikowanej usługi archiwizacji elektronicznej.

2. Dane elektroniczne oraz elektroniczne dokumenty przechowywane przy użyciu kwalifikowanej usługi archiwizacji elektronicznej korzystają z domniemania ich integralności i pochodzenia przez cały okres przechowywania przez kwalifikowanego dostawcę usług zaufania.

Artykuł 45j

Wymogi dotyczące kwalifikowanych usług archiwizacji elektronicznej

1. Kwalifikowane usługi archiwizacji elektronicznej muszą spełniać następujące wymogi:

a) są świadczone przez kwalifikowanych dostawców usług zaufania;

b) wykorzystują procedury i technologie umożliwiające zapewnienie trwałości i czytelności danych elektronicznych i dokumentów elektronicznych poza technologiczny okres ważności i co najmniej na cały okres prawnego lub umownego okresu przechowywania, przy jednoczesnym zachowaniu ich integralności i autentyczności pochodzenia;

c) zapewniają przechowywanie tych danych elektronicznych i dokumentów elektronicznych w taki sposób, aby były zabezpieczone przed utratą i modyfikacją, z wyjątkiem zmian dotyczących ich nośnika lub formatu elektronicznego;

d) umożliwiają one upoważnionym stronom ufającym otrzymanie w automatyczny sposób raportu potwierdzającego, że dane elektroniczne i dokumenty elektroniczne pobrane z kwalifikowanego archiwum elektronicznego korzystają z domniemania integralności danych od początku okresu przechowywania do momentu pobrania.

Raport, o którym mowa w lit. d) akapitu pierwszego, musi być przekazywany w sposób niezawodny i efektywny oraz opatrzony kwalifikowanym podpisem elektronicznym lub kwalifikowaną pieczęcią elektroniczną dostawcy kwalifikowanej usługi archiwizacji elektronicznej.

2. Do dnia 21 maja 2025 r. Komisja, w drodze aktów wykonawczych, sporządzi wykaz norm referencyjnych oraz, w razie potrzeby, ustanowi specyfikacje i procedury w odniesieniu do kwalifikowanych usług archiwizacji elektronicznej. W przypadku gdy kwalifikowana usługa archiwizacji elektronicznej spełnia wymogi tych norm, specyfikacji i procedur, domniemywa się zgodność z wymogami dotyczącymi kwalifikowanych usług archiwizacji elektronicznej. Te akty wykonawcze przyjmuje się zgodnie z procedurą sprawdzającą, o której mowa w art. 48 ust. 2.

SEKCJA 11

rejestry elektroniczne

Artykuł 45k

Skutki prawne rejestrów elektronicznych

1. Rejestrowi elektronicznemu nie można odmówić skutku prawnego ani dopuszczalności jako dowodu w postępowaniu sądowym wyłącznie z tego powodu, że rejestr ten ma postać elektroniczną lub że nie spełnia wymogów dla kwalifikowanych rejestrów elektronicznych.

▼M1

2. Wpisy danych zawarte w kwalifikowanym rejestrze elektronicznym korzystają z domniemania ich niepowtarzalnego i dokładnego sekwencyjnego uporządkowania chronologicznego oraz ich integralności.

Artykuł 45l

Wymogi dotyczące kwalifikowanych rejestrów elektronicznych

1. Kwalifikowane rejestry elektroniczne muszą spełniać następujące wymogi:

a) są tworzone i zarządzane przez co najmniej jednego kwalifikowanego dostawcę usług zaufania;

b) ustalają pochodzenie wpisów danych w rejestrze;

c) zapewniają niepowtarzalne sekwencyjne uporządkowanie chronologiczne wpisów danych w rejestrze;

d) rejestrują dane w taki sposób, że każda późniejsza zmiana danych jest natychmiast wykrywalna, co zapewnia ich integralność w czasie.

2. W przypadku gdy rejestr elektroniczny przestrzega norm, specyfikacji i procedur, o których mowa w ust. 3, domniemywa się zgodność z wymogami określonymi w ust. 1.

3. Do dnia 21 maja 2025 r. Komisja, w drodze aktów wykonawczych, sporządzi wykaz norm referencyjnych oraz, w razie potrzeby, ustanowi specyfikacje i procedury w odniesieniu do wymogów określonych w ust. 1 niniejszego artykułu. Te akty wykonawcze przyjmuje się zgodnie z procedurą sprawdzającą, o której mowa w art. 48 ust. 2.

▼B

ROZDZIAŁ IV

DOKUMENTY ELEKTRONICZNE

Artykuł 46

Skutki prawne dokumentów elektronicznych

Nie jest kwestionowany skutek prawny dokumentu elektronicznego ani jego dopuszczalność jako dowodu w postępowaniu sądowym wyłącznie z tego powodu, że dokument ten ma postać elektroniczną.

▼M1

ROZDZIAŁ IVa

RAMY ZARZĄDZANIA

Artykuł 46a

Nadzór nad ramami dla europejskiego portfela tożsamości cyfrowej

1. Państwa członkowskie wyznaczają na swoim terytorium jeden lub większą liczbę organów nadzoru.

Organy nadzoru wyznaczone zgodnie z akapitem pierwszym muszą otrzymać niezbędne uprawnienia i odpowiednie zasoby do wykonywania swoich zadań w sposób skuteczny, efektywny i niezależny.

▼M1

2. Państwa członkowskie przekazują Komisji nazwy i adresy swoich organów nadzoru wyznaczonych zgodnie z ust. 1, oraz informacje o wszelkich późniejszych zmianach w tym zakresie. Komisja publikuje wykaz zgłoszonych organów nadzoru.

3. Organy nadzoru wyznaczone zgodnie z ust. 1 spełniają następującą rolę:

a) sprawują nadzór nad dostawcami europejskich portfeli tożsamości cyfrowej mającymi siedzibę na terytorium wyznaczającego państwa członkowskiego oraz zapewniają – za pomocą działań nadzorczych *ex ante* i *ex post* – aby ci dostawcy i dostarczane przez nich europejskie portfele tożsamości cyfrowej spełniały wymogi określone w niniejszym rozporządzeniu;

b) podejmują w razie potrzeby działania – za pomocą działań nadzorczych ex post – w odniesieniu do mających siedzibę na terytorium wyznaczającego państwa członkowskiego dostawców europejskich portfeli tożsamości cyfrowej po otrzymaniu informacji, że dostawcy lub europejskie portfele tożsamości cyfrowej, dostarczane przez tych dostawców, naruszają niniejsze rozporządzenie.

4. Zadania organów nadzoru wyznaczonych zgodnie z ust. 1 obejmują w szczególności:

a) współpracę z innymi organami nadzoru oraz udzielanie im pomocy zgodnie z art. 46c i 46e;

b) żądanie informacji niezbędnych do monitorowania zgodności z niniejszym rozporządzeniem;

c) informowanie odpowiednich właściwych organów wyznaczonych lub ustanowionych w danym państwie członkowskim zgodnie z art. 8 ust. 1 dyrektywy (UE) 2022/2555 o wszelkich poważnych naruszeniach bezpieczeństwa lub utracie integralności, o których dowiedziały się w trakcie wykonywania swoich zadań oraz – w przypadku gdy poważne naruszenie lub utrata integralności dotyczą innych państw członkowskich – informowanie pojedynczego punktu kontaktowego wyznaczonego lub ustanowionego w danym państwie członkowskim zgodnie z art. 8 ust. 3 dyrektywy (UE) 2022/2555 oraz pojedynczych punktów kontaktowych wyznaczonych w innych państwach członkowskich zgodnie z art. 46c ust. 1 niniejszego rozporządzenia, a także informowanie opinii publicznej lub zobowiązanie do tego dostawców europejskiego portfela tożsamości cyfrowej, w przypadku gdy organ nadzoru stwierdzi, że ujawnienie naruszenia bezpieczeństwa lub utraty integralności leży w interesie publicznym;

d) prowadzenie kontroli na miejscu i nadzoru zdalnego;

e) zobowiązywanie dostawców europejskich portfeli tożsamości cyfrowej do wyeliminowania wszelkich przypadków niespełnienia wymogów określonych w niniejszym rozporządzeniu;

f) zawieszanie lub cofnięcie rejestracji oraz włączenia stron ufających do mechanizmu, o którym mowa w art. 5b ust. 7, w przypadku niezgodnego z prawem lub oszukańczego korzystania z europejskiego portfela tożsamości cyfrowej;

g) współpracę z właściwymi organami nadzorczymi ustanowionymi na podstawie art. 51 rozporządzenia (UE) 2016/679, w szczególności poprzez informowanie ich, bez zbędnej zwłoki, w przypadku podejrzenia naruszenia przepisów dotyczących ochrony danych osobowych, a także informowanie ich o naruszeniach bezpieczeństwa, które przypuszczalnie stanowią naruszenie ochrony danych osobowych.

▼M1

5. W przypadku gdy organ nadzoru wyznaczony zgodnie z ust. 1 zobowiązuje dostawcę europejskiego portfela tożsamości cyfrowej do wyeliminowania wszelkich przypadków niespełnienia wymogów wynikających z niniejszego rozporządzenia zgodnie z ust. 4 lit. e), a dostawca ten nie podejmuje odpowiednich działań, ani – w stosownych przypadkach – nie podejmuje ich w terminie wyznaczonym przez ten organ nadzoru, organ nadzoru wyznaczony zgodnie z ust. 1 może, mając na uwadze w szczególności zakres, czas trwania oraz skutki takiego niespełniania wymogów, nakazać temu dostawcy zawieszenie lub zaprzestanie dostarczania europejskiego portfela tożsamości cyfrowej. Organ nadzoru bez zbędnej zwłoki informuje organy nadzoru z pozostałych państw członkowskich, Komisję, strony ufające oraz użytkowników europejskiego portfela tożsamości cyfrowej o decyzji nakazującej zawieszenie lub zaprzestanie dostarczania europejskiego portfela tożsamości cyfrowej.

6. Do dnia 31 marca każdego roku każdy organ nadzoru wyznaczony zgodnie z ust. 1 przedkłada Komisji sprawozdanie ze swoich głównych działań w poprzednim roku kalendarzowym. Komisja udostępnia te coroczne sprawozdania Parlamentowi Europejskiemu i Radzie.

7. Do dnia 21 maja 2025 r. Komisja, w drodze aktów wykonawczych, określi formaty i procedury w odniesieniu do sprawozdania, o którym mowa w ust. 6 niniejszego artykułu. Te akty wykonawcze przyjmuje się zgodnie z procedurą sprawdzającą, o której mowa w art. 48 ust. 2.

Artykuł 46b

Nadzór nad usługami zaufania

1. Państwa członkowskie wyznaczają organ nadzoru ustanowiony na ich terytorium lub wyznaczają – za obopólnym porozumieniem z innym państwem członkowskim – organ nadzoru z siedzibą w tym innym państwie członkowskim. Ten organ nadzoru odpowiedzialny jest za zadania nadzoru w wyznaczającym państwie członkowskim w odniesieniu do usług zaufania.

Organy nadzoru wyznaczone zgodnie z akapitem pierwszym muszą otrzymać niezbędne uprawnienia i odpowiednie zasoby do wykonywania swoich zadań.

2. Państwa członkowskie przekazują Komisji nazwy i adresy swoich organów nadzoru wyznaczonych zgodnie z ust. 1, oraz informacje o wszelkich późniejszych zmianach w tym zakresie. Komisja publikuje wykaz zgłoszonych organów nadzoru.

3. Rolą organów nadzoru wyznaczonych zgodnie z ust. 1 jest:

a) sprawowanie nadzoru nad kwalifikowanymi dostawcami usług zaufania z siedzibą na terytorium wyznaczającego państwa członkowskiego oraz zapewnianie – za pomocą działań nadzorczych ex ante i ex post – aby określone w niniejszym rozporządzeniu wymogi były spełniane przez tych kwalifikowanych dostawców usług zaufania oraz przez świadczone przez nich kwalifikowane usługi zaufania;

b) podejmowanie, w razie potrzeby, działań w odniesieniu do niekwalifikowanych dostawców usług zaufania mających siedzibę na terytorium wyznaczającego państwa członkowskiego – za pomocą działań nadzorczych *ex post* – gdy dowiedzą się, że niekwalifikowani dostawcy usług zaufania lub świadczone przez nich usługi zaufania przypuszczalnie nie spełniają wymogów określonych w niniejszym rozporządzeniu.

▼M1

4. Zadania organu nadzoru wyznaczonego zgodnie z ust. 1 obejmują w szczególności:

a) informowanie odpowiednich właściwych organów wyznaczonych lub ustanowionych w danym państwie członkowskim zgodnie z art. 8 ust. 1 dyrektywy (UE) 2022/2555 o wszelkich poważnych naruszeniach bezpieczeństwa lub utracie integralności, o których dowiedział się w trakcie wykonywania swoich zadań oraz – w przypadku gdy poważne naruszenie lub utrata integralności dotyczą innych państw członkowskich – informowanie pojedynczego punktu kontaktowego wyznaczonego lub ustanowionego w danym państwie członkowskim zgodnie z art. 8 ust. 3 dyrektywy (UE) 2022/2555 oraz pojedynczych punktów kontaktowych wyznaczonych w innych państwach członkowskich zgodnie z art. 46c ust. 1 niniejszego rozporządzenia, a także informowanie opinii publicznej lub zobowiązanie do tego dostawcy usług zaufania, w przypadku gdy organ nadzoru stwierdzi, że ujawnienie naruszenia bezpieczeństwa lub utraty integralności leży w interesie publicznym;

b) współpracę z innymi organami nadzoru oraz udzielanie im pomocy zgodnie z art. 46c i 46e;

c) analizowanie raportów z oceny zgodności, o których mowa w art. 20 ust. 1 i art. 21 ust. 1;

d) składanie sprawozdań Komisji na temat swoich głównych działań zgodnie z ust. 6 niniejszego artykułu;

e) przeprowadzanie audytów lub zwracanie się do jednostki oceniającej zgodność o przeprowadzenie oceny zgodności kwalifikowanych dostawców usług zaufania zgodnie z art. 20 ust. 2;

f) współpracę z właściwymi organami nadzoru ustanowionymi zgodnie z art. 51 rozporządzenia (UE) 2016/679, w szczególności poprzez informowanie ich, bez zbędnej zwłoki, w przypadku podejrzenia naruszenia przepisów dotyczących ochrony danych osobowych, a także informowanie ich o naruszeniach bezpieczeństwa, które przypuszczalnie stanowią naruszenie ochrony danych osobowych;

g) przyznawanie dostawcom usług zaufania i świadczonym przez nich usługom statusu kwalifikowanego dostawcy usług zaufania i kwalifikowanych usług, a także odebranie tego statusu zgodnie z art. 20 i 21;

h) informowanie organu odpowiedzialnego za krajową zaufaną listę, o której mowa w art. 22 ust. 3, o swoich decyzjach o przyznaniu lub odebraniu statusu kwalifikowanego, chyba że organ ten jest również organem nadzoru wyznaczonym zgodnie z ust. 1 niniejszego artykułu;

(i) sprawdzanie istnienia i prawidłowego stosowania postanowień dotyczących planów zakończenia działalności w przypadkach, gdy kwalifikowany dostawca usług zaufania zaprzestaje działalności, w tym sposobu, w jaki zapewnia się dalszą dostępność informacji zgodnie z art. 24 ust. 2 lit. h);

j) zobowiązywanie dostawców usług zaufania do wyeliminowania wszelkich przypadków niespełnienia wymogów określonych w niniejszym rozporządzeniu;

▼M1

k) rozpatrywanie zgłoszeń wnoszonych przez dostawców przeglądarek internetowych zgodnie z art. 45a oraz w razie potrzeby podejmowanie działań.

5. Państwa członkowskie mogą wymagać, aby organ nadzoru wyznaczony zgodnie z ust. 1 utworzył, utrzymywał i aktualizował infrastrukturę zaufania zgodnie z prawem krajowym.

6. Do dnia 31 marca każdego roku każdy organ nadzoru wyznaczony zgodnie z ust. 1 przedkłada Komisji sprawozdanie ze swoich głównych działań w poprzednim roku kalendarzowym. Komisja udostępnia te coroczne sprawozdania Parlamentowi Europejskiemu i Radzie.

7. Do dnia 21 maja 2025 r. Komisja przyjmie wytyczne dotyczące wykonywania przez organy nadzoru wyznaczone zgodnie z ust. 1 zadań, o których mowa w ust. 4 niniejszego artykułu, oraz – w drodze aktów wykonawczych – określi formaty i procedury w odniesieniu do sprawozdania, o którym mowa w ust. 6 niniejszego artykułu. Te akty wykonawcze przyjmuje się zgodnie z procedurą sprawdzającą, o której mowa w art. 48 ust. 2.

Artykuł 46c

Pojedyncze punkty kontaktowe

1. Każde państwo członkowskie wyznacza pojedynczy punkt kontaktowy ds. usług zaufania, europejskich portfeli tożsamości cyfrowej i notyfikowanych systemów identyfikacji elektronicznej.

2. Każdy pojedynczy punkt kontaktowy pełni funkcję łącznikową w celu ułatwienia współpracy transgranicznej między organami nadzoru dla dostawców usług zaufania oraz między organami nadzoru dla dostawców europejskich portfeli tożsamości cyfrowej, a także, w stosownych przypadkach, z Komisją oraz Agencją Unii Europejskiej ds. Cyberbezpieczeństwa (ENISA) oraz z innymi właściwymi organami w swoim państwie członkowskim.

3. Każde państwo członkowskie podaje do wiadomości publicznej oraz bez zbędnej zwłoki przekazuje Komisji nazwy i adresy pojedynczego punktu kontaktowego wyznaczonego zgodnie z ust. 1, oraz informacje o wszelkich późniejszych zmianach w tym zakresie.

4. Komisja publikuje wykaz pojedynczych punktów kontaktowych zgłoszonych zgodnie z ust. 3.

Artykuł 46d

Wzajemna pomoc

1. W celu ułatwienia nadzoru i egzekwowania obowiązków wynikających z niniejszego rozporządzenia organy nadzoru wyznaczone zgodnie z art. 46a ust. 1 i art. 46b ust. 1 mogą zwracać się, w tym za pośrednictwem grupy współpracy ustanowionej na podstawie art. 46e ust. 1, o wzajemną pomoc do organów nadzoru w innym państwie członkowskim, w którym ma siedzibę dany dostawca europejskiego portfela tożsamości cyfrowej lub dany dostawca usług zaufania, lub w którym znajdują się jego sieć i systemy informatyczne lub świadczone są jego usługi.

2. Wzajemna pomoc oznacza co najmniej, że:

▼M1

a) organ nadzoru stosujący środki nadzoru i egzekwowania w jednym państwie członkowskim informuje organ nadzoru w innym zainteresowanym państwie członkowskim oraz prowadzi z nim konsultacje;

b) organ nadzoru może zwrócić się do organu nadzoru innego zainteresowanego państwa członkowskiego o wprowadzenie środków nadzoru lub egzekwowania, w tym – na przykład – może zwrócić się z wnioskiem o przeprowadzenie kontroli dotyczących raportów z oceny zgodności, o których mowa w art. 20 i 21, w odniesieniu do świadczenia usług zaufania;

c) w stosownych przypadkach organy nadzoru mogą prowadzić wspólne dochodzenia z organami nadzoru z innych państw członkowskich.

Ustalenia i procedury dotyczące wspólnych działań, o których mowa w akapicie pierwszym, są uzgadniane i określane przez zainteresowane państwa członkowskie zgodnie z ich prawem krajowym.

3. Organ nadzoru, do którego kierowany jest wniosek o pomoc, może odrzucić ten wniosek z któregokolwiek z poniższych względów:

a) pomoc, o którą się zwrócono, nie jest proporcjonalna do działań nadzorczych organu nadzoru prowadzonych zgodnie z art. 46a i 46b;

b) organ nadzoru nie jest właściwy do udzielenia pomocy, której dotyczy wniosek;

c) udzielenie pomocy, której dotyczy wniosek, byłoby niezgodne z niniejszym rozporządzeniem.

4. Do dnia 21 maja 2025 r., a następnie co dwa lata grupa współpracy ustanowiona na podstawie art. 46e ust. 1 wydaje wytyczne dotyczące aspektów organizacyjnych i procedur wzajemnej pomocy, o której mowa w ust. 1 i 2 niniejszego artykułu.

Artykuł 46e

Grupa Współpracy na rzecz Europejskiej Tożsamości Cyfrowej

1. W celu wspierania i ułatwiania transgranicznej współpracy państw członkowskich oraz wymiany informacji dotyczących usług zaufania, europejskich portfeli tożsamości cyfrowej i notyfikowanych systemów identyfikacji elektronicznej Komisja ustanawia Grupę Współpracy na rzecz Europejskiej Tożsamości Cyfrowej (zwaną dalej „grupą współpracy”).

2. Grupa współpracy składa się z przedstawicieli mianowanych przez państwa członkowskie oraz przez Komisję. Grupie współpracy przewodniczy Komisja., Komisja zapewnia również obsługę sekretariatu grupy współpracy.

3. Do udziału w posiedzeniach grupy współpracy i uczestnictwa w jej pracach w charakterze obserwatorów mogą być zapraszani – na zasadzie ad hoc – przedstawiciele odpowiednich zainteresowanych stron.

4. Do udziału w pracach grupy współpracy w charakterze obserwatora zapraszana jest ENISA, gdy grupa współpracy przeprowadza wymianę poglądów, najlepszych praktyk i informacji w odniesieniu do istotnych aspektów cyberbezpieczeństwa, takich jak zgłaszanie przypadków naruszenia bezpieczeństwa, a także gdy rozpatrywane są kwestie stosowania certyfikatów lub norm cyberbezpieczeństwa.

5. Grupa współpracy ma następujące zadania:

▼M1

a) wymiana porad oraz współpraca z Komisją w zakresie nowych inicjatyw politycznych w dziedzinie portfeli tożsamości cyfrowej, środków identyfikacji elektronicznej i usług zaufania;

b) doradzanie Komisji, w stosownych przypadkach, na wczesnym etapie przygotowywania projektów aktów wykonawczych i delegowanych, które mają zostać przyjęte na podstawie niniejszego rozporządzenia;

c) w celu wspierania organów nadzoru w wykonywaniu przepisów niniejszego rozporządzenia:

(i) wymiana najlepszych praktyk i informacji dotyczących wykonywania przepisów niniejszego rozporządzenia;

(ii) ocena istotnych zmian w obszarach portfela tożsamości cyfrowej, identyfikacji elektronicznej i usług zaufania;

(iii) organizowanie regularnych wspólnych spotkań z odpowiednimi zainteresowanymi stronami z całej Unii, aby dyskutować na temat działań prowadzonych przez grupę współpracy oraz zbierać informacje o nowych wyzwaniach politycznych;

(iv) wymiana poglądów, najlepszych praktyk i informacji na temat odpowiednich aspektów cyberbezpieczeństwa europejskich portfeli tożsamości cyfrowej, systemów identyfikacji elektronicznej oraz usług zaufania – przy wsparciu ze strony ENISA;

(v) wymiana najlepszych praktyk w odniesieniu do opracowywania i wdrażania polityki zgłaszania naruszeń bezpieczeństwa, o których mowa w art. 5e i 10;

(vi) organizacja wspólnych spotkań z grupą współpracy ds. bezpieczeństwa sieci i informacji ustanowioną zgodnie z art. 14 ust. 1 dyrektywy (UE) 2022/2555 w celu wymiany istotnych informacji dotyczących usług zaufania i identyfikacji elektronicznej powiązanych cyberzagrożeń, incydentów, podatności na zagrożenia, inicjatyw na rzecz podnoszenia świadomości, szkoleń, ćwiczeń i umiejętności, budowania zdolności w zakresie norm i specyfikacji technicznych, a także norm i specyfikacji technicznych;

(vii) dyskutowanie, na wniosek organu nadzoru, na temat konkretnych wniosków o pomoc wzajemną, o której mowa w art. 46d;

(viii) ułatwianie wymiany informacji między organami nadzoru poprzez udzielanie wskazówek dotyczących aspektów organizacyjnych i procedur wzajemnej pomocy, o której mowa w art. 46d;

d) organizacja wzajemnej oceny systemów identyfikacji elektronicznej podlegających notyfikacji zgodnie z niniejszym rozporządzeniem.

6. Państwa członkowskie zapewniają skuteczną i efektywną współpracę swoich wyznaczonych przedstawicieli w grupie współpracy.

▼M1

7. Do dnia 21 maja 2025 r. Komisja, w drodze aktów wykonawczych, ustanowi niezbędne ustalenia proceduralne w celu ułatwienia współpracy między państwami członkowskimi, o której mowa w ust. 5 lit. d) niniejszego artykułu. Te akty wykonawcze przyjmuje się zgodnie z procedurą sprawdzającą, o której mowa w art. 48 ust. 2.

▼B

ROZDZIAŁ V

PRZEKAZANIE UPRAWNIEŃ I PRZEPISY WYKONAWCZE

Artykuł 47

Wykonywanie przekazanych uprawnień

1. Powierzenie Komisji uprawnień do przyjmowania aktów delegowanych podlega warunkom określonym w niniejszym artykule.

▼M1

2. Uprawnienia do przyjmowania aktów delegowanych, o których mowa w art. 5c ust. 7, art. 24 ust. 4b i art. 30 ust. 4, powierza się Komisji na czas nieokreślony od dnia 17 września 2014 r.

3. Przekazanie uprawnień, o których mowa w art. 5c ust. 7, art. 24 ust. 4b i art. 30 ust. 4, może zostać w dowolnym momencie odwołane przez Parlament Europejski lub przez Radę. Decyzja o odwołaniu kończy przekazanie określonych w niej uprawnień. Decyzja o odwołaniu staje się skuteczna następnego dnia po jej opublikowaniu w *Dzienniku Urzędowym Unii Europejskiej* lub w późniejszym terminie określonym w tej decyzji. Nie wpływa ona na ważność już obowiązujących aktów delegowanych.

▼B

4. Niezwłocznie po przyjęciu aktu delegowanego Komisja przekazuje go równocześnie Parlamentowi Europejskiemu i Radzie.

▼M1

5. Akt delegowany przyjęty na podstawie art. 6c ust. 7, art. 24 ust. 4b lub art. 30 ust. 4 wchodzi w życie tylko wówczas, gdy ani Parlament Europejski, ani Rada nie wyraziły sprzeciwu w terminie dwóch miesięcy od przekazania tego aktu Parlamentowi Europejskiemu i Radzie, lub gdy, przed upływem tego terminu, zarówno Parlament Europejski, jak i Rada poinformowały Komisję, że nie wniosą sprzeciwu. Termin ten przedłuża się o dwa miesiące z inicjatywy Parlamentu Europejskiego lub Rady.

▼B

Artykuł 48

Procedura komitetowa

1. Komisję wspomaga komitet. Komitet ten jest komitetem w rozumieniu rozporządzenia (UE) nr 182/2011.

2. W przypadku odesłania do niniejszego ustępu stosuje się art. 5 rozporządzenia (UE) nr 182/2011.

▼B

ROZDZIAŁ VI

PRZEPISY KOŃCOWE

▼M1

Artykuł 48a

Wymogi dotyczące sprawozdawczości

1. Państwa członkowskie zapewniają zbieranie danych statystycznych dotyczących funkcjonowania europejskich portfeli tożsamości cyfrowej oraz kwalifikowanych usług zaufania dostarczanych lub świadczonych na ich terytorium.

2. Dane statystyczne zbierane zgodnie z ust. 1 obejmują następujące elementy:

a) liczbę osób fizycznych i prawnych posiadających ważny europejski portfel tożsamości cyfrowej;

b) rodzaj i liczbę usług akceptujących używanie europejskiego portfela tożsamości cyfrowej;

c) liczbę skarg użytkowników i incydentów związanych z ochroną konsumentów lub ochroną danych w odniesieniu do stron ufających i kwalifikowanych usług zaufania;

d) zestawienie zawierające dane dotyczące incydentów uniemożliwiających używanie europejskiego portfela tożsamości cyfrowej;

e) podsumowanie poważnych incydentów związanych z bezpieczeństwem, naruszeń ochrony danych i użytkowników europejskich portfeli tożsamości cyfrowej lub kwalifikowanych usług zaufania, których to dotyczy.

3. Dane statystyczne, o których mowa w ust. 2, udostępnia się publicznie w otwartym i powszechnie używanym formacie nadającym się do odczytu maszynowego.

4. Do dnia 31 marca każdego roku państwa członkowskie przedkładają Komisji sprawozdanie dotyczące danych statystycznych zebranych zgodnie z ust. 2.

Artykuł 49

Przegląd

1. Komisja dokonuje przeglądu stosowania niniejszego rozporządzenia i do dnia 21 maja 2026 r. przedłoży sprawozdanie Parlamentowi Europejskiemu i Radzie. W sprawozdaniu tym Komisja oceni w szczególności, czy należy zmienić zakres stosowania niniejszego rozporządzenia lub jego poszczególnych przepisów, w tym – w szczególności – przepisów zawartych w art. 5c ust. 5, biorąc pod uwagę doświadczenia zdobyte przy stosowaniu niniejszego rozporządzenia, a także rozwój technologiczny, sytuację rynkową i prawną. W razie potrzeby do sprawozdania dołącza się wniosek dotyczący zmiany niniejszego rozporządzenia.

2. Sprawozdanie, o którym mowa w ust. 1, obejmuje ocenę dostępności, bezpieczeństwa i użyteczności notyfikowanych środków identyfikacji elektronicznej oraz europejskich portfeli tożsamości cyfrowej objętych zakresem stosowania niniejszego rozporządzenia, oraz ocenę,

▼M1

czy wszyscy prywatni dostawcy usług online korzystający z usług identyfikacji elektronicznej świadczonych przez strony trzecie do celów uwierzytelniania użytkowników muszą zostać zobowiązani do akceptowania wykorzystywania notyfikowanych środków identyfikacji elektronicznej i europejskiego portfela tożsamości cyfrowej.

3. Do dnia 21 maja 2030 r., a następnie co cztery lata Komisja przedkłada Parlamentowi Europejskiemu i Radzie sprawozdanie z postępów w osiąganiu celów niniejszego rozporządzenia.

▼B

Artykuł 50

Uchylenie

1. Dyrektywę 1999/93/WE uchyla się z dniem 1 lipca 2016 r.

2. Odesłania do uchylonej dyrektywy odczytuje się jako odesłania do niniejszego rozporządzenia.

▼M1

Artykuł 51

Środki przejściowe

1. Bezpieczne urządzenia do składania podpisu, których zgodność ustalono zgodnie z art. 3 ust. 4 dyrektywy 1999/93/WE, w dalszym ciągu uznaje się za kwalifikowane urządzenia do składania podpisu elektronicznego na podstawie niniejszego rozporządzenia do dnia 21 maja 2027 r.

2. Kwalifikowane certyfikaty wydane osobom fizycznym na podstawie dyrektywy 1999/93/WE w dalszym ciągu uznaje się za kwalifikowane certyfikaty podpisów elektronicznych na podstawie niniejszego rozporządzenia do dnia 21 maja 2026 r.

3. Zarządzanie kwalifikowanymi urządzeniami do składania podpisów i pieczęci elektronicznych na odległość przez kwalifikowanych dostawców usług zaufania, innych niż kwalifikowani dostawcy usług zaufania świadczący kwalifikowane usługi zaufania na potrzeby zarządzania kwalifikowanymi urządzeniami do składania podpisów i pieczęci elektronicznych na odległość zgodnie z art. 29a i 39a, może być prowadzone, bez konieczności uzyskania statusu kwalifikowanego do celów świadczenia tych usług zarządzania, do dnia 21 maja 2026 r.

4. Kwalifikowani dostawcy usług zaufania, którym na podstawie niniejszego rozporządzenia przyznano status kwalifikowany przed dniem 20 maja 2024 r., przedkładają organowi nadzoru raport z oceny zgodności potwierdzający zgodność z art. 24 ust. 1, 1a i 1b najszybciej jak to możliwe, nie później jednak niż w dniu 21 May 2026 r.

▼B

Artykuł 52

Wejście w życie

1. Niniejsze rozporządzenie wchodzi w życie dwudziestego dnia po jego opublikowaniu w *Dzienniku Urzędowym Unii Europejskiej*.

2. Niniejsze rozporządzenie stosuje się od dnia 1 lipca 2016 r., z wyjątkiem następujących przepisów:

▼B

a) art. 8 ust. 3, art. 9 ust. 5, art. 12 ust. 2–9, art. 17 ust. 8, art. 19 ust. 4, art. 20 ust. 4, art. 21 ust. 4, art. 22 ust. 5, art. 23 ust. 3, art. 24 ust. 5, art. 27 ust. 4 i 5, art. 28 ust. 6, art. 29 ust. 2, art. 30 ust. 3 i 4, art. 31 ust. 3, art. 32 ust. 3, art. 33 ust. 2, art. 34 ust. 2, art. 37 ust. 4 i 5, art. 38 ust. 6, art. 42 ust. 2, art. 44 ust. 2, art. 45 ust. 2, art. 47 i 48 mają zastosowanie od dnia 17 września 2014 r.;

b) art. 7, art. 8 ust. 1 i 2, art. 9, 10, 11 i art. 12 ust. 1 mają zastosowanie od dnia rozpoczęcia stosowania aktów wykonawczych, o których mowa w art. 8 ust. 3 i art. 12 ust. 8;

c) art. 6 ma zastosowanie od dnia przypadającego trzy lata od dnia rozpoczęcia stosowania aktów wykonawczych, o których mowa w art. 8 ust. 3 i art. 12 ust. 8.

3. W przypadku gdy notyfikowany system identyfikacji elektronicznej został umieszczony w wykazie publikowanym przez Komisję na podstawie art. 9 przed dniem, o którym mowa w ust. 2 lit. c) niniejszego artykułu, uznanie środka identyfikacji elektronicznej w ramach tego systemu na mocy art. 6 następuje nie później niż 12 miesięcy po opublikowaniu tego systemu, ale nie wcześniej niż w dniu, o którym mowa w ust. 2 lit. c) niniejszego artykułu.

4. Niezależnie od ust. 2 lit. c) niniejszego artykułu państwo członkowskie może postanowić, że środki identyfikacji elektronicznej w ramach systemu identyfikacji elektronicznej notyfikowanego na podstawie art. 9 ust. 1 przez inne państwo członkowskie są uznawane w pierwszym państwie członkowskim z dniem rozpoczęcia stosowania aktów wykonawczych, o których mowa w art. 8 ust. 3 i art. 12 ust. 8. Zainteresowane państwa członkowskie informują o tym Komisję. Komisja podaje te informacje do wiadomości publicznej.

Niniejsze rozporządzenie wiąże w całości i jest bezpośrednio stosowane we wszystkich państwach członkowskich.

▼B

ZAŁĄCZNIK I

WYMOGI DLA KWALIFIKOWANYCH CERTYFIKATÓW PODPISÓW ELEKTRONICZNYCH

Kwalifikowane certyfikaty podpisów elektronicznych zawierają następujące informacje:

a) wskazanie – co najmniej w postaci pozwalającej na automatyczne przetwarzanie – że dany certyfikat został wydany jako kwalifikowany certyfikat podpisu elektronicznego;

b) zestaw danych jednoznacznie reprezentujących kwalifikowanego dostawcę usług zaufania wydającego kwalifikowane certyfikaty, obejmujący co najmniej państwo członkowskie, w którym dostawca ma siedzibę, oraz

— w odniesieniu do osoby prawnej: nazwę i, w stosownym przypadku, numer rejestrowy zgodnie z oficjalnym rejestrem,

— w odniesieniu do osoby fizycznej: imię i nazwisko tej osoby;

c) co najmniej imię i nazwisko podpisującego lub jego pseudonim; jeżeli używany jest pseudonim, fakt ten jest jasno wskazany;

d) dane służące do walidacji podpisu elektronicznego, które odpowiadają danym służącym do składania podpisu elektronicznego;

e) dane dotyczące początku i końca okresu ważności certyfikatu;

f) kod identyfikacyjny certyfikatu, który musi być niepowtarzalny dla kwalifikowanego dostawcy usług zaufania;

g) zaawansowany podpis elektroniczny lub zaawansowaną pieczęć elektroniczną wydającego kwalifikowanego dostawcy usług zaufania;

h) miejsce, w którym nieodpłatnie dostępny jest certyfikat towarzyszący zaawansowanemu podpisowi elektronicznemu lub zaawansowanej pieczęci elektronicznej, o których mowa w lit. g);

▼M1

i) informacje na temat statusu ważności kwalifikowanego certyfikatu lub miejsce usług, w którym można dowiedzieć się o statusie ważności kwalifikowanego certyfikatu;

▼B

j) w przypadku gdy dane służące do składania podpisu elektronicznego powiązane z danymi służącymi do walidacji podpisu elektronicznego znajdują się w kwalifikowanym urządzeniu do składania podpisu elektronicznego, odpowiednie wskazanie tego faktu co najmniej w postaci pozwalającej na automatyczne przetwarzanie.

▼B

ZAŁĄCZNIK II

WYMOGI DLA KWALIFIKOWANYCH URZĄDZEŃ DO SKŁADANIA PODPISU ELEKTRONICZNEGO

1. Kwalifikowane urządzenia do składania podpisu elektronicznego zapewniają dzięki właściwym środkom technicznym i proceduralnym co najmniej:

   a) zagwarantowanie w racjonalny sposób poufności danych służących do składania podpisu elektronicznego użytych do złożenia podpisu elektronicznego;

   b) w praktyce tylko jednorazowe wystąpienie danych służących do składania podpisu elektronicznego użytych do złożenia podpisu elektronicznego;

   c) uniemożliwienie, z racjonalną dozą pewności, pozyskania danych służących do składania podpisu elektronicznego użytych do złożenia podpisu elektronicznego oraz skuteczną ochronę podpisu elektronicznego przed sfałszowaniem za pomocą aktualnie dostępnych technologii;

   d) możliwość skutecznej ochrony, przez osobę uprawnioną do składania podpisu, danych służących do składania podpisu elektronicznego użytych do złożenia podpisu elektronicznego, przed użyciem ich przez innych.

2. Kwalifikowane urządzenia do składania podpisu elektronicznego nie zmieniają danych, które mają być podpisane, ani nie uniemożliwiają przedstawienia tych danych podpisującemu przed złożeniem podpisu.

▼M1

_____

▼B

ZAŁĄCZNIK III

WYMOGI DLA KWALIFIKOWANYCH CERTYFIKATÓW PIECZĘCI ELEKTRONICZNYCH

Kwalifikowane certyfikaty pieczęci elektronicznych zawierają:

a) wskazanie – co najmniej w postaci pozwalającej na automatyczne przetwarzanie – że dany certyfikat został wydany jako kwalifikowany certyfikat pieczęci elektronicznej;

b) zestaw danych jednoznacznie reprezentujących kwalifikowanego dostawcę usług zaufania wydającego kwalifikowane certyfikaty, obejmujący co najmniej państwo członkowskie, w którym dostawca ma siedzibę, oraz

— w odniesieniu do osoby prawnej: nazwę i, w stosownym przypadku, numer rejestrowy zgodnie z oficjalnym rejestrem,

— w odniesieniu do osoby fizycznej: imię i nazwisko tej osoby;

c) co najmniej nazwę podmiotu składającego pieczęć i, w stosownym przypadku, numer rejestrowy zgodnie z oficjalnym rejestrem;

d) dane służące do walidacji pieczęci elektronicznej, które odpowiadają danym służącym do składania pieczęci elektronicznej;

e) dane dotyczące początku i końca okresu ważności certyfikatu;

f) kod identyfikacyjny certyfikatu, który musi być niepowtarzalny dla kwalifikowanego dostawcy usług zaufania;

g) zaawansowany podpis elektroniczny lub zaawansowaną pieczęć elektroniczną wydającego kwalifikowanego dostawcy usług zaufania;

h) miejsce, w którym nieodpłatnie dostępny jest certyfikat towarzyszący zaawansowanemu podpisowi elektronicznemu lub zaawansowanej pieczęci elektronicznej, o których mowa w lit. g);

▼M1

i) informacje na temat statusu ważności kwalifikowanego certyfikatu lub miejsce usług, w którym można dowiedzieć się o statusie ważności kwalifikowanego certyfikatu;

▼B

j) jeżeli dane służące do składania pieczęci elektronicznej powiązane z danymi służącymi do walidacji pieczęci elektronicznej znajdują się w kwalifikowanym urządzeniu do składania pieczęci elektronicznej, odpowiednie wskazanie tego faktu co najmniej w postaci pozwalającej na automatyczne przetwarzanie.

▼B

ZAŁĄCZNIK IV

WYMOGI DLA KWALIFIKOWANYCH CERTYFIKATÓW UWIERZYTELNIANIA WITRYN INTERNETOWYCH

Kwalifikowane certyfikaty uwierzytelniania witryn internetowych zawierają:

a) wskazanie – co najmniej w postaci pozwalającej na automatyczne przetwarzanie – że dany certyfikat został wydany jako kwalifikowany certyfikat uwierzytelniania witryn internetowych;

b) zestaw danych jednoznacznie reprezentujących kwalifikowanego dostawcę usług zaufania wydającego kwalifikowane certyfikaty, obejmujący co najmniej państwo członkowskie, w którym dostawca ma siedzibę, oraz

— w odniesieniu do osoby prawnej: nazwę i, w stosownym przypadku, numer rejestrowy zgodnie z oficjalnym rejestrem,

— w odniesieniu do osoby fizycznej: imię i nazwisko tej osoby;

▼M1

c) w odniesieniu do osób fizycznych: co najmniej imię i nazwisko osoby, której wydano certyfikat, lub pseudonim; w przypadku gdy używany jest pseudonim, musi to być wyraźnie wskazane;

ca) w odniesieniu do osób prawnych: niepowtarzalny zestaw danych jednoznacznie reprezentujących osobę prawną, której wydano certyfikat, zawierający co najmniej nazwę osoby prawnej, której wydawany jest certyfikat oraz – w stosownych przypadkach – numer rejestrowy zgodnie z oficjalnym rejestrem;

▼B

d) elementy adresu, w tym co najmniej miasto i państwo, osoby fizycznej lub prawnej, którym wydano certyfikat, i, w stosownym przypadku, zgodnie z oficjalnym rejestrem;

e) nazwę(-y) domen, którymi posługuje się osoba fizyczna lub prawna, której wydano certyfikat;

f) dane dotyczące początku i końca okresu ważności certyfikatu;

g) kod identyfikacyjny certyfikatu, który musi być niepowtarzalny dla kwalifikowanego dostawcy usług zaufania;

h) zaawansowany podpis elektroniczny lub zaawansowaną pieczęć elektroniczną wydającego kwalifikowanego dostawcy usług zaufania;

i) miejsce, w którym nieodpłatnie dostępny jest certyfikat towarzyszący zaawansowanemu podpisowi elektronicznemu lub zaawansowanej pieczęci elektronicznej, o których mowa w lit. h);

▼M1

j) informacje na temat statusu ważności kwalifikowanego certyfikatu lub miejsce usług statusu ważności certyfikatu, w którym można dowiedzieć się o statusie ważności kwalifikowanego certyfikatu.

▼M1

ZAŁĄCZNIK V

WYMOGI DOTYCZĄCE KWALIFIKOWANEGO ELEKTRONICZNEGO POŚWIADCZENIA ATRYBUTÓW

Kwalifikowane elektroniczne poświadczenie atrybutów musi zawierać:

a) wskazanie – co najmniej w formie nadającej się do automatycznego przetwarzania – że dane poświadczenie zostało wydane jako kwalifikowane elektroniczne poświadczenie atrybutów;

b) zestaw danych jednoznacznie reprezentujących kwalifikowanego dostawcę usług zaufania wydającego kwalifikowane elektroniczne poświadczenia atrybutów, obejmujący co najmniej państwo członkowskie, w którym dostawca ma siedzibę, oraz:

   (i) w odniesieniu do osoby prawnej: nazwę oraz – w stosownym przypadku – numer rejestrowy zgodnie z oficjalnym rejestrem,

   (ii) w odniesieniu do osoby fizycznej: imię i nazwisko tej osoby;

c) zestaw danych jednoznacznie reprezentujących podmiot, do którego poświadczone atrybuty się odnoszą; w przypadku gdy używany jest pseudonim, musi to być wyraźnie wskazane;

d) poświadczony atrybut lub poświadczone atrybuty, w tym – w stosownych przypadkach – informacje niezbędne do określenia zakresu tych atrybutów;

e) szczegółowe dane dotyczące początku i końca okresu ważności poświadczenia;

f) kod identyfikacyjny poświadczenia, który musi być niepowtarzalny dla kwalifikowanego dostawcy usług zaufania, oraz – w stosownych przypadkach – wskazanie systemu poświadczeń, którego częścią jest dane poświadczenie atrybutów;

g) kwalifikowany podpis elektroniczny lub kwalifikowaną pieczęć elektroniczną wydającego kwalifikowanego dostawcy usług zaufania;

h) miejsce, w którym nieodpłatnie dostępny jest certyfikat towarzyszący kwalifikowanemu podpisowi elektronicznemu lub kwalifikowanej pieczęci elektronicznej, o których mowa w lit. g);

i) informacje na temat statusu ważności kwalifikowanego poświadczenia lub miejsce usług, w którym można dowiedzieć się o statusie ważności kwalifikowanego poświadczenia.

▼M1

ZAŁĄCZNIK VI

MINIMALNY WYKAZ ATRYBUTÓW

Zgodnie z art. 45e państwa członkowskie zapewniają, aby wprowadzono środki umożliwiające kwalifikowanym dostawcom usług zaufania, którzy dostarczają kwalifikowane elektroniczne poświadczenia atrybutów weryfikację drogą elektroniczną, na żądanie użytkownika, autentyczności następujących atrybutów w zestawieniu z odpowiednim źródłem autentycznym na poziomie krajowym lub poprzez wyznaczonych pośredników uznanych na poziomie krajowym zgodnie z prawem Unii lub prawem krajowym oraz w przypadku gdy atrybuty te polegają na źródłach autentycznych w sektorze publicznym:

1) adres;

2) wiek;

3) płeć;

4) stan cywilny;

5) skład rodziny;

6) narodowość lub obywatelstwo;

7) wykształcenie, tytuły i licencje;

8) kwalifikacje zawodowe, tytuły i licencje;

9) pełnomocnictwa i upoważnienia do reprezentowania osób fizycznych lub prawnych;

10) publicznoprawne zezwolenia i licencje;

11) w odniesieniu do osób prawnych – dane finansowe i dane dotyczące przedsiębiorstwa.

▼M1

ZAŁĄCZNIK VII

WYMOGI DOTYCZĄCE ELEKTRONICZNEGO POŚWIADCZENIA ATRYBUTÓW WYDAWANEGO PRZEZ PODMIOT PUBLICZNY ODPOWIEDZIALNY ZA ŹRÓDŁO AUTENTYCZNE LUB W JEGO IMIENIU

Elektroniczne poświadczenie atrybutów wydawane przez podmiot publiczny odpowiedzialny za źródło autentyczne lub w jego imieniu musi zawierać:

a) wskazanie – co najmniej w formie nadającej się do automatycznego przetwarzania– że poświadczenie zostało wydane jako elektroniczne poświadczenie atrybutów wydawane przez podmiot publiczny odpowiedzialny za źródło autentyczne lub w jego imieniu;

b) zestaw danych jednoznacznie reprezentujących podmiot publiczny wydający elektroniczne poświadczenie atrybutów, w tym co najmniej państwo członkowskie, w którym ten podmiot publiczny ma siedzibę, oraz nazwę podmiotu oraz, w stosownych przypadkach, jego numer rejestrowy zgodnie z oficjalnym rejestrem;

c) zestaw danych jednoznacznie reprezentujących podmiot, do którego poświadczone atrybuty się odnoszą; w przypadku gdy używany jest pseudonim, musi to być wyraźnie wskazane;

d) poświadczony atrybut lub poświadczone atrybuty, w tym – w stosownych przypadkach – informacje niezbędne do określenia zakresu tych atrybutów;

e) szczegółowe dane dotyczące początku i końca okresu ważności poświadczenia;

f) kod identyfikacyjny poświadczenia, który musi być niepowtarzalny dla wydającego podmiotu publicznego, oraz – w stosownych przypadkach – wskazanie systemu poświadczeń, którego częścią jest dane poświadczenie atrybutów;

g) kwalifikowany podpis elektroniczny lub kwalifikowaną pieczęć elektroniczną wydającego podmiotu;

h) miejsce, w którym nieodpłatnie dostępny jest certyfikat towarzyszący kwalifikowanemu podpisowi elektronicznemu lub kwalifikowanej pieczęci elektronicznej, o których mowa w lit. g);

(i) informacje na temat statusu ważności poświadczenia lub miejsce usług, w którym można dowiedzieć się o statusie ważności poświadczenia.