2024/1183

30.4.2024

ROZPORZĄDZENIE PARLAMENTU EUROPEJSKIEGO I RADY (UE) 2024/1183

z dnia 11 kwietnia 2024 r.

w sprawie zmiany rozporządzenia (UE) nr 910/2014 w odniesieniu do ustanowienia europejskich ram tożsamości cyfrowej

PARLAMENT EUROPEJSKI I RADA UNII EUROPEJSKIEJ,

uwzględniając Traktat o funkcjonowaniu Unii Europejskiej, w szczególności jego art. 114,

uwzględniając wniosek Komisji Europejskiej,

po przekazaniu projektu aktu ustawodawczego parlamentom narodowym,

uwzględniając opinię Europejskiego Komitetu Ekonomiczno-Społecznego ([1]),

uwzględniając opinię Komitetu Regionów ([2]),

stanowiąc zgodnie ze zwykłą procedurą ustawodawczą ([3]),

a także mając na uwadze, co następuje:

(1) W komunikacie Komisji z dnia 19 lutego 2020 r., zatytułowanym „Kształtowanie cyfrowej przyszłości Europy", zapowiedziano przegląd rozporządzenia Parlamentu Europejskiego i Rady (UE) nr 910/2014 ([4]) w celu poprawy jego skuteczności, rozszerzenia wynikających z niego korzyści na sektor prywatny oraz promowania zaufanych tożsamości cyfrowych dla wszystkich Europejczyków.

(2) W konkluzjach z dnia 1–2 października 2020 r. Rada Europejska wezwała Komisję do przedstawienia wniosku w sprawie opracowania ogólnounijnych ram bezpiecznej publicznej identyfikacji elektronicznej, w tym interoperacyjnych podpisów cyfrowych, aby zapewnić obywatelom kontrolę nad ich tożsamością i danymi w internecie, a także umożliwić dostęp do publicznych, prywatnych i transgranicznych usług cyfrowych.

(3) W programie polityki „Droga ku cyfrowej dekadzie" do 2030 r., ustanowionym decyzją Parlamentu Europejskiego i Rady (UE) 2022/2481 ([5]), określono założenia i cyfrowe cele unijnych ram, które do 2030 r. mają zapewnić wprowadzenie na szeroką skalę zaufanej, dobrowolnej i kontrolowanej przez użytkownika tożsamości cyfrowej, uznawanej w całej Unii oraz umożliwiającej każdemu użytkownikowi kontrolowanie swoich danych w interakcjach online.

(4) W „Europejskiej deklaracji praw i zasad cyfrowych w cyfrowej dekadzie", proklamowanej przez Parlament Europejski, Radę i Komisję ([6]) (zwanej dalej „deklaracją"), podkreślono prawo każdego do dostępu do technologii, produktów i usług cyfrowych, które z założenia są bezpieczne i chronione oraz strzegą prywatności. Obejmuje to zapewnienie, aby wszyscy ludzie mieszkający w Unii mogli korzystać z dostępnej, bezpiecznej i zaufanej tożsamości cyfrowej, która umożliwia dostęp do szerokiego wachlarza usług online i offline, zapewniając ochronę przed ryzykiem w cyberprzestrzeni i przed cyberprzestępczością, w tym naruszeniami ochrony danych i kradzieżą tożsamości lub manipulowaniem tożsamością. W deklaracji stwierdzono również, że każdy ma prawo do ochrony swoich danych osobowych. Prawo to obejmuje także kontrolę tego, jak dane są wykorzystywane i komu są udostępniane.

([1]) Dz.U. C 105 z 4.3.2022, s. 81.
([2]) Dz.U. C 61 z 4.2.2022, s. 42.
([3]) Stanowisko Parlamentu Europejskiego z dnia 29 lutego 2024 r. (dotychczas nieopublikowane w Dzienniku Urzędowym) oraz decyzja Rady z dnia 26 marca 2024 r.
([4]) 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).
([5]) Decyzja Parlamentu Europejskiego i Rady (UE) 2022/2481 z dnia 14 grudnia 2022 r. ustanawiająca program polityki „Droga ku cyfrowej dekadzie" do 2030 r. (Dz.U. L 323 z 19.12.2022, s. 4).
([6]) Dz.U. C 23 z 23.1.2023, s. 1.

(5) Obywatele i rezydenci Unii powinni mieć prawo do tożsamości cyfrowej, która jest pod ich wyłączną kontrolą i która pozwala im na wykonywanie ich praw w środowisku cyfrowym oraz uczestnictwo w gospodarce cyfrowej. Aby osiągnąć ten cel, należy ustanowić europejskie ramy tożsamości cyfrowej umożliwiające obywatelom i rezydentom Unii dostęp do publicznych i prywatnych usług online i offline w całej Unii.

(6) Zharmonizowane ramy tożsamości cyfrowej powinny przyczyniać się do tworzenia bardziej zintegrowanej cyfrowo Unii poprzez zmniejszanie barier cyfrowych między państwami członkowskimi oraz umożliwienie obywatelom i rezydentom Unii czerpania korzyści z cyfryzacji, przy jednoczesnym zwiększeniu przejrzystości i ochrony ich praw.

(7) Bardziej zharmonizowane podejście do identyfikacji elektronicznej powinno zmniejszyć ryzyko i koszty wynikające z obecnej fragmentacji spowodowanej stosowaniem rozbieżnych rozwiązań krajowych lub – w niektórych państwach członkowskich – brakiem takich rozwiązań w zakresie identyfikacji elektronicznej. Takie podejście powinno wzmocnić rynek wewnętrzny, umożliwiając obywatelom i rezydentom Unii, określonym w prawie krajowym, oraz przedsiębiorstwom identyfikowanie się i uwierzytelnianie swojej tożsamości online i offline w sposób bezpieczny, godny zaufania, przyjazny dla użytkownika, wygodny, dostępny i zharmonizowany w całej Unii. Europejski portfel tożsamości cyfrowej powinien zapewnić osobom fizycznym i prawnym w całej Unii zharmonizowany środek identyfikacji elektronicznej umożliwiający im uwierzytelnianie i udostępnianie danych związanych z ich tożsamością. Każdy powinien mieć możliwość bezpiecznego dostępu do usług publicznych i prywatnych, za pomocą ulepszonego systemu usług zaufania i zweryfikowanych dowodów potwierdzających tożsamość oraz elektronicznych poświadczeń atrybutów, takich jak kwalifikacje akademickie, w tym dyplomy ukończenia studiów wyższych, lub inne uprawnienia edukacyjne lub zawodowe. Europejskie ramy tożsamości cyfrowej mają na celu przejście od polegania wyłącznie na krajowych rozwiązaniach w zakresie tożsamości cyfrowej do zapewnienia elektronicznych poświadczeń atrybutów, które są ważne i prawnie uznawane w całej Unii. Dostawcy elektronicznych poświadczeń atrybutów powinni skorzystać na jasnym i jednolitym zestawie przepisów, natomiast administracje publiczne powinny mieć możliwość polegania na dokumentach elektronicznych w określonym formacie.

(8) Szereg państw członkowskich wdrożyło i stosuje środki identyfikacji elektronicznej, które są akceptowane przez dostawców usług w Unii. Ponadto na podstawie rozporządzenia (UE) nr 910/2014 dokonano inwestycji zarówno w rozwiązania krajowe, jak i transgraniczne, w tym w interoperacyjność notyfikowanych systemów identyfikacji elektronicznej zgodnie z tym rozporządzeniem. Aby zapewnić komplementarność i szybkie przyjęcie europejskich portfeli tożsamości cyfrowej przez obecnych użytkowników notyfikowanych środków identyfikacji elektronicznej oraz zminimalizować wpływ na istniejących dostawców usług, oczekuje się, że w ramach europejskich portfeli tożsamości cyfrowej wykorzystane zostaną doświadczenia zdobyte w związku z istniejącymi środkami identyfikacji elektronicznej, a także infrastruktura notyfikowanych systemów identyfikacji elektronicznej wdrożona na poziomie unijnym i krajowym.

(9) Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2016/679 ([7]) oraz – w stosownych przypadkach – dyrektywa 2002/58/WE Parlamentu Europejskiego i Rady ([8]) mają zastosowanie do wszystkich czynności przetwarzania danych osobowych na podstawie rozporządzenia (UE) nr 910/2014. Rozwiązania wynikające z ram interoperacyjności przewidziane w niniejszym rozporządzeniu również są zgodne z tymi przepisami. Prawo Unii dotyczące ochrony danych przewiduje zasady ochrony danych, takie jak zasada minimalizacji danych i zasada celowości, oraz obowiązki, takie jak uwzględnienie ochrony danych na etapie projektowania i domyślna ochrona danych.

(10) Aby wspierać konkurencyjność unijnych przedsiębiorstw, dostawcy zarówno usług online, jak i offline powinni móc polegać na rozwiązaniach w zakresie tożsamości cyfrowej uznawanych w całej Unii, niezależnie od państwa członkowskiego, w którym rozwiązania te zostały zapewnione, a tym samym czerpać korzyści ze zharmonizowanego unijnego podejścia do zaufania, bezpieczeństwa i interoperacyjności. Zarówno użytkownicy, jak i dostawcy usług powinni mieć możliwość korzystania z przyznania elektronicznym poświadczeniom atrybutów takiej samej wartości prawnej w całej Unii. Zharmonizowane ramy tożsamości cyfrowej mają tworzyć wartość gospodarczą poprzez zapewnianie łatwiejszego dostępu do towarów i usług oraz poprzez znaczące zmniejszenie kosztów operacyjnych związanych z procedurami elektronicznej identyfikacji i elektronicznego uwierzytelniania, na przykład podczas rejestracji nowych klientów, poprzez zmniejszenie ryzyka potencjalnych cyberprzestępstw, takich jak kradzież tożsamości, kradzież danych i oszustwa internetowe, wspierając tym samym wzrost efektywności oraz bezpieczną transformację cyfrową mikroprzedsiębiorstw oraz małych i średnich przedsiębiorstw (MŚP) w Unii.

([7]) 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).

([8]) Dyrektywa 2002/58/WE Parlamentu Europejskiego i Rady z dnia 12 lipca 2002 r. dotycząca przetwarzania danych osobowych i ochrony prywatności w sektorze łączności elektronicznej (dyrektywa o prywatności i łączności elektronicznej) (Dz.U. L 201 z 31.7.2002, s. 37).

(11) Europejskie portfele tożsamości cyfrowej powinny ułatwiać stosowanie zasady jednorazowości i tym samym zmniejszać obciążenie administracyjne oraz wspierać transgraniczną mobilność obywateli i rezydentów Unii oraz przedsiębiorstw w całej Unii, a także sprzyjać rozwojowi interoperacyjnych usług administracji elektronicznej w całej Unii.

(12) W ramach wykonywania niniejszego rozporządzenia, do przetwarzania danych osobowych zastosowanie mają rozporządzenie (UE) 2016/679 i rozporządzenie Parlamentu Europejskiego i Rady (UE) 2018/1725 ([9]) oraz dyrektywa 2002/58/WE. W związku z tym w niniejszym rozporządzeniu należy ustanowić szczególne zabezpieczenia uniemożliwiające dostawcom środków identyfikacji elektronicznej i elektronicznych poświadczeń atrybutów łączenie danych osobowych uzyskanych w ramach świadczenia innych usług z danymi osobowymi przetwarzanymi w celu świadczenia usług objętych zakresem stosowania niniejszego rozporządzenia. Dane osobowe związane z dostarczaniem europejskich portfeli tożsamości cyfrowej powinny być logicznie oddzielone od wszelkich innych danych będących w posiadaniu dostawcy europejskiego portfela tożsamości cyfrowej. Niniejsze rozporządzenie nie powinno uniemożliwiać dostawcom europejskich portfeli tożsamości cyfrowej stosowania dodatkowych środków technicznych przyczyniających się do ochrony danych osobowych, takich jak fizyczne oddzielenie danych osobowych związanych z dostarczaniem europejskich portfeli tożsamości cyfrowej od wszelkich innych danych będących w posiadaniu dostawcy. Bez uszczerbku dla rozporządzenia (UE) 2016/679, niniejsze rozporządzenie doprecyzowuje stosowanie zasady celowości, zasady minimalizacji danych oraz uwzględniania ochrony danych na etapie projektowania i domyślnej ochrony danych.

(13) Europejskie portfele tożsamości cyfrowej powinny mieć wbudowaną funkcję wspólnego panelu zarządzania, aby zapewnić wyższy stopień przejrzystości, prywatności i kontroli użytkowników nad ich danymi osobowymi. Funkcja ta powinna zapewniać łatwy i przyjazny dla użytkownika interfejs wraz z przeglądem wszystkich stron ufających, którym użytkownik udostępnia dane, w tym atrybuty, oraz rodzaju danych udostępnionych każdej ze stron ufających. Powinna ona umożliwiać użytkownikom śledzenie wszystkich transakcji przeprowadzonych za pośrednictwem europejskiego portfela tożsamości cyfrowej za pomocą co najmniej następujących danych: czas i data transakcji, identyfikacja drugiej strony, żądane dane osobowe i dane udostępnione. Informacje te powinny być przechowywane, nawet jeżeli transakcja nie została zawarta. Nie powinna istnieć możliwość podważenia autentyczności informacji zawartych w historii transakcji. Taka funkcja powinna być domyślnie aktywna. Powinna ona umożliwiać użytkownikom łatwe zażądanie natychmiastowego usunięcia przez stronę ufającą danych osobowych zgodnie z art. 17 rozporządzenia (UE) 2016/679 oraz łatwe zgłoszenie strony ufającej właściwemu krajowemu organowi ochrony danych w przypadku otrzymania przypuszczalnie niezgodnego z prawem lub podejrzanego żądania danych osobowych, bezpośrednio poprzez europejski portfel tożsamości cyfrowej.

(14) Państwa członkowskie powinny włączyć do europejskiego portfela tożsamości cyfrowej różne technologie chroniące prywatność, takie jak dowód z wiedzą zerową. Te metody kryptograficzne powinny umożliwiać stronie ufającej zweryfikowanie, czy dane stwierdzenie oparte na danych identyfikujących osobę i poświadczeniu atrybutów jest prawdziwe, bez ujawniania jakichkolwiek danych, na których opiera się to stwierdzenie, chroniąc tym samym prywatność użytkownika.

(15) Niniejsze rozporządzenie określa zharmonizowane warunki ustanowienia ram dla europejskich portfeli tożsamości cyfrowej, które mają być zapewniane przez państwa członkowskie. Wszyscy obywatele i rezydenci Unii określeni w prawie krajowym powinni być uprawnieni do bezpiecznego żądania, wybierania, łączenia, przechowywania, usuwania, udostępniania i prezentacji danych dotyczących swojej tożsamości oraz żądania usunięcia swoich danych osobowych w przyjazny dla użytkownika i wygodny sposób, pod wyłączną kontrolą użytkownika, przy jednoczesnej możliwości selektywnego ujawniania danych osobowych. Niniejsze rozporządzenie odzwierciedla wspólne wartości europejskie oraz przestrzega praw podstawowych, gwarancji prawnych i zasady odpowiedzialności, chroniąc w ten sposób społeczeństwa demokratyczne, obywateli i rezydentów Unii. Należy rozwijać technologie wykorzystywane do osiągnięcia tych celów, dążąc do zapewnienia najwyższego poziomu bezpieczeństwa, prywatności, wygody użytkowników, dostępności, szerokiej używalności oraz niezakłóconej interoperacyjności. Państwa członkowskie powinny zapewniać równy dostęp do identyfikacji elektronicznej wszystkim swoim obywatelom i rezydentom. Państwa członkowskie nie powinny – bezpośrednio ani pośrednio – ograniczać dostępu do usług publicznych lub prywatnych osobom fizycznym lub prawnym, które nie zdecydują się na używanie europejskich portfeli tożsamości cyfrowej, oraz powinny udostępniać odpowiednie rozwiązania alternatywne.

([9]) Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2018/1725 z dnia 23 października 2018 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych przez instytucje, organy i jednostki organizacyjne Unii i swobodnego przepływu takich danych oraz uchylenia rozporządzenia (WE) nr 45/2001 i decyzji nr 1247/2002/WE (Dz.U. L 295 z 21.11.2018, s. 39).

(16) Państwa członkowskie powinny korzystać z możliwości oferowanych przez niniejsze rozporządzenie w celu zapewniania, w ramach swojej odpowiedzialności, europejskich portfeli tożsamości cyfrowej do użytku przez osoby fizyczne i prawne mające miejsce zamieszkania lub siedzibę na ich terytorium. Aby zapewnić państwom członkowskim elastyczność oraz wykorzystać najnowocześniejszą technologię, niniejsze rozporządzenie powinno umożliwiać zapewnianie europejskich portfeli tożsamości cyfrowej bezpośrednio przez państwo członkowskie, na podstawie upoważnienia od państwa członkowskiego, lub niezależnie od państwa członkowskiego, lecz przy uznaniu przez to państwo członkowskie.

(17) Do celów rejestracji strony ufające powinny przekazywać informacje niezbędne do umożliwienia ich elektronicznej identyfikacji i elektronicznego uwierzytelniania w europejskich portfelach tożsamości cyfrowej. Deklarując swoje zamierzone wykorzystanie europejskiego portfela tożsamości cyfrowej, strony ufające powinny podać informacje dotyczące danych, których będą ewentualnie żądać w celu świadczenia swoich usług, oraz podać uzasadnienie tego żądania. Rejestracja strony ufającej ułatwia weryfikację przez państwa członkowskie zgodności z prawem działalności stron ufających zgodnie z prawem Unii. Obowiązek rejestracji przewidziany w niniejszym rozporządzeniu powinien pozostawać bez uszczerbku dla obowiązków określonych w innych przepisach prawa Unii lub prawa krajowego, takich jak obowiązki dotyczące informacji, które mają być przekazywane osobom, których dane dotyczą, zgodnie z rozporządzeniem (UE) 2016/679. Strony ufające powinny stosować zabezpieczenia przewidziane w art. 35 i 36 tego rozporządzenia, w szczególności dokonując oceny skutków dla ochrony danych oraz konsultując się z właściwymi organami ochrony danych przed przetwarzaniem danych, w przypadku gdy oceny skutków dla ochrony danych wskazują, że przetwarzanie powodowałoby wysokie ryzyko. Takie zabezpieczenia powinny wspierać zgodne z prawem przetwarzanie danych osobowych przez strony ufające, w szczególności w odniesieniu do szczególnych kategorii danych, takich jak dane dotyczące zdrowia. Rejestracja stron ufających ma na celu zwiększenie przejrzystości i zaufania w zakresie korzystania z europejskich portfeli tożsamości cyfrowej. Aby zapewnić jej upowszechnienie wśród usługodawców, rejestracja powinna być efektywna kosztowo oraz proporcjonalna względem odnośnych zagrożeń. W tym kontekście rejestracja powinna przewidywać stosowanie zautomatyzowanych procedur, w tym poleganie na istniejących rejestrach i korzystanie z nich przez państwa członkowskie, oraz nie powinna wiązać się z procesem uzyskiwania wstępnego zezwolenia. Proces rejestracji powinien umożliwiać szereg przypadków użycia, które mogą różnić się pod względem trybu działania – online lub w trybie offline – lub pod względem wymogu uwierzytelnienia urządzeń do celów połączenia z europejskim portfelem tożsamości cyfrowej. Rejestracja powinna mieć zastosowanie wyłącznie do stron ufających świadczących usługi za pośrednictwem interakcji cyfrowych.

(18) Ochrona obywateli i rezydentów Unii przed nieuprawnionym lub oszukańczym używaniem europejskich portfeli tożsamości cyfrowej ma duże znaczenie dla zapewnienia zaufania do europejskich portfeli tożsamości cyfrowej i ich szerokiego upowszechnienia. Należy zapewnić użytkownikom skuteczną ochronę przed takim niewłaściwym używaniem. W szczególności, jeżeli w kontekście innej procedury krajowej organy sądowe ustalą stan faktyczny będący podstawą stwierdzenia oszustwa lub innego niezgodnego z prawem używania europejskiego portfela tożsamości cyfrowej, organy nadzoru odpowiedzialne za dostawców europejskich portfeli tożsamości cyfrowej powinny, po otrzymaniu powiadomienia, podjąć niezbędne środki w celu zapewnienia cofnięcia lub zawieszenia rejestracji strony ufającej oraz cofnięcia lub zawieszenia włączenia stron ufających do mechanizmu uwierzytelniania, do czasu potwierdzenia przez organ notyfikujący, że stwierdzone nieprawidłowości zostały wyeliminowane.

(19) Wszystkie europejskie portfele tożsamości cyfrowej powinny umożliwiać użytkownikom elektroniczne identyfikowanie się i uwierzytelnianie online i w trybie offline w kontekście transgranicznym na potrzeby dostępu do szerokiego zakresu usług publicznych i prywatnych. Bez uszczerbku dla prerogatyw państw członkowskich w zakresie identyfikacji ich obywateli i rezydentów, europejskie portfele tożsamości cyfrowej mogą również zaspokajać potrzeby instytucjonalne administracji publicznych, organizacji międzynarodowych oraz instytucji, organów i jednostek organizacyjnych Unii. Uwierzytelnianie offline byłoby ważne w wielu sektorach, w tym w sektorze zdrowia, w którym usługi są często świadczone w ramach kontaktu osobistego, a w przypadku recept elektronicznych powinna istnieć możliwość stosowania kodów QR lub podobnych technologii do weryfikacji autentyczności. W oparciu o wysoki poziom bezpieczeństwa dla systemów identyfikacji elektronicznej, europejskie portfele tożsamości cyfrowej powinny wykorzystywać potencjał, jaki oferują rozwiązania zabezpieczające przed manipulacją, takie jak bezpieczne elementy (ang. secure elements), w celu zapewnienia zgodności z wymogami bezpieczeństwa wynikającymi z niniejszego rozporządzenia. Europejskie portfele tożsamości cyfrowej powinny również umożliwiać użytkownikom tworzenie i używanie kwalifikowanych podpisów i pieczęci elektronicznych akceptowanych w całej Unii. Po zarejestrowaniu się w europejskim portfelu tożsamości cyfrowej osoby fizyczne powinny mieć możliwość używania go do składania kwalifikowanych podpisów elektronicznych, domyślnie i nieodpłatnie, bez konieczności przechodzenia przez jakiekolwiek dodatkowe procedury administracyjne. Użytkownicy powinni mieć możliwość podpisywania lub opatrywania pieczęcią przygotowanych przez siebie potwierdzeń lub atrybutów. Aby zapewnić obywatelom i przedsiębiorstwom w całej Unii korzyści w zakresie uproszczeń i zmniejszenia kosztów, w tym poprzez umożliwienie korzystania z upoważnień i pełnomocnictw elektronicznych, państwa członkowskie powinny zapewniać europejskie portfele tożsamości cyfrowej oparte na wspólnych normach i specyfikacjach technicznych w celu zapewnienia niezakłóconej interoperacyjności oraz odpowiedniego podniesienia bezpieczeństwa informatycznego, wzmocnienia odporności na cyberataki, a tym samym znaczącego zmniejszenia potencjalnego ryzyka związanego z postępującą cyfryzacją dla obywateli

i rezydentów Unii oraz dla przedsiębiorstw. Wyłącznie właściwe organy państw członkowskich mogą zapewnić dużą dozę pewności przy ustalaniu tożsamości danej osoby, zapewniając tym samym, że osoba podająca daną tożsamość jest faktycznie osobą, za którą się podaje. Dla zapewnienia europejskich portfeli tożsamości cyfrowej niezbędne jest zatem poleganie na oficjalnej tożsamości obywateli i rezydentów Unii lub osób prawnych. Poleganie na oficjalnej tożsamości nie powinno utrudniać użytkownikom europejskich portfeli tożsamości cyfrowej dostępu do usług z użyciem pseudonimu w przypadku gdy prawo nie wymaga podania oficjalnej tożsamości w celu uwierzytelnienia. Zaufanie do europejskich portfeli tożsamości cyfrowej zwiększyłoby się, gdyby podmioty je wydające i nimi zarządzające były zobowiązane do wdrożenia odpowiednich środków technicznych i organizacyjnych w celu zapewnienia najwyższego poziomu bezpieczeństwa, jaki jest współmierny do stwarzanego ryzyka dla praw i wolności osób fizycznych zgodnie z rozporządzeniem (UE) 2016/679.

(20) Użycie kwalifikowanego podpisu elektronicznego powinno być nieodpłatne dla wszystkich osób fizycznych do celów innych niż profesjonalne. Państwa członkowskie powinny móc ustanowić środki zapobiegające nieodpłatnemu użyciu kwalifikowanych podpisów elektronicznych przez osoby fizyczne do celów profesjonalnych, przy jednoczesnym zapewnieniu, aby wszelkie takie środki były proporcjonalne do zidentyfikowanego ryzyka oraz uzasadnione.

(21) Korzystne jest ułatwienie upowszechnienia i używania europejskich portfeli tożsamości cyfrowej poprzez niezakłócone zintegrowanie ich z już wdrożonym na poziomie krajowym, lokalnym lub regionalnym ekosystemem publicznych i prywatnych usług cyfrowych. Z myślą o osiągnięciu tego celu państwa członkowskie powinny móc przewidzieć środki prawne i organizacyjne, aby zwiększyć elastyczność dla dostawców europejskich portfeli tożsamości cyfrowej oraz umożliwić wprowadzenie dodatkowych funkcji europejskich portfeli tożsamości cyfrowej oprócz tych, które przewidziano w niniejszym rozporządzeniu, w tym poprzez zwiększoną interoperacyjność z istniejącymi krajowymi środkami identyfikacji elektronicznej. Takie dodatkowe funkcje nie powinny w żadnym razie szkodzić zapewnieniu podstawowych funkcji europejskich portfeli tożsamości cyfrowej przewidzianych w niniejszym rozporządzeniu ani prowadzić do promowania istniejących rozwiązań krajowych kosztem europejskich portfeli tożsamości cyfrowej. Ponieważ takie dodatkowe funkcje wykraczają poza zakres stosowania niniejszego rozporządzenia, nie podlegają one określonym w niniejszym rozporządzeniu przepisom dotyczącym transgranicznego używania europejskich portfeli tożsamości cyfrowej.

(22) Europejskie portfele tożsamości cyfrowej powinny zawierać funkcję generowania pseudonimów wybranych i zarządzanych przez użytkownika, służących do uwierzytelniania podczas dostępu do usług online.

(23) W celu zapewnienia wysokiego poziomu bezpieczeństwa i zaufania, w niniejszym rozporządzeniu ustanawia się wymogi dotyczące europejskich portfeli tożsamości cyfrowej. Zgodność europejskich portfeli tożsamości cyfrowej z tymi wymogami powinna być certyfikowana przez akredytowane jednostki oceniające zgodność wyznaczone przez państwa członkowskie.

(24) W celu uniknięcia rozbieżnych podejść oraz harmonizacji wdrażania wymogów określonych w niniejszym rozporządzeniu, Komisja powinna – do celów certyfikacji europejskich portfeli tożsamości cyfrowej – przyjmować akty wykonawcze, aby ustanowić wykaz norm referencyjnych oraz, w razie potrzeby, ustanowić specyfikacje i procedury w celu przedstawienia szczegółowych specyfikacji technicznych tych wymogów. W zakresie, w jakim certyfikacja zgodności europejskich portfeli tożsamości cyfrowej z odpowiednimi wymogami związanymi z cyberbezpieczeństwem nie jest objęta istniejącymi programami certyfikacji cyberbezpieczeństwa, o których mowa w niniejszym rozporządzeniu, oraz w odniesieniu do wymogów niezwiązanych z cyberbezpieczeństwem istotnych dla europejskich portfeli tożsamości cyfrowej, państwa członkowskie powinny ustanowić krajowe programy certyfikacji zgodnie ze zharmonizowanymi wymogami określonymi w niniejszym rozporządzeniu oraz przyjętymi na jego podstawie. Państwa członkowskie powinny przekazywać swoje projekty krajowych systemów certyfikacji Grupie Współpracy na rzecz Europejskiej Tożsamości Cyfrowej, która powinna mieć możliwość wydawania opinii i zaleceń.

(25) Certyfikacja zgodności z wymogami związanymi z cyberbezpieczeństwem określonymi w niniejszym rozporządzeniu powinna opierać się – jeżeli są dostępne – na odpowiednich europejskich programach certyfikacji cyberbezpieczeństwa ustanowionych na podstawie rozporządzenia Parlamentu Europejskiego i Rady (UE) 2019/881 ([10]), które ustanawia dobrowolne europejskie ramy certyfikacji cyberbezpieczeństwa produktów, procesów i usług ICT.

([10]) 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).

(26) Aby stale oceniać i ograniczać ryzyko związane z bezpieczeństwem, certyfikowane europejskie portfele tożsamości cyfrowej powinny podlegać regularnym ocenom podatności na zagrożenia, mającym na celu wykrywanie wszelkich podatności na zagrożenia certyfikowanych elementów związanych z produktem, certyfikowanych elementów związanych z procesem oraz certyfikowanych elementów związanych z usługami europejskiego portfela tożsamości cyfrowej.

(27) Zapewniając ochronę użytkowników i przedsiębiorstw przed zagrożeniami w cyberprzestrzeni, zasadnicze wymogi związane z cyberbezpieczeństwem określone w niniejszym rozporządzeniu przyczyniają się również do zwiększenia ochrony danych osobowych oraz prywatności osób fizycznych. Należy rozważyć możliwości synergii zarówno w obszarze normalizacji, jak i certyfikacji w zakresie aspektów cyberbezpieczeństwa, poprzez współpracę między Komisją, europejskimi organizacjami normalizacyjnymi, Agencją Unii Europejskiej ds. Cyberbezpieczeństwa (ENISA), Europejską Radą Ochrony Danych ustanowioną rozporządzeniem (UE) 2016/679 oraz krajowymi organami nadzorczymi odpowiedzialnymi za ochronę danych.

(28) Należy ułatwić rejestrację obywateli i rezydentów Unii w europejskim portfelu tożsamości cyfrowej z użyciem środków identyfikacji elektronicznej na wysokim poziomie bezpieczeństwa. Na środkach identyfikacji elektronicznej wydanych na średnim poziomie bezpieczeństwa należy polegać wyłącznie w przypadkach, gdy zharmonizowane specyfikacje techniczne i procedury wykorzystujące środki identyfikacji elektronicznej wydane na średnim poziomie bezpieczeństwa, w połączeniu ze środkami uzupełniającymi weryfikację tożsamości, umożliwią spełnienie wymogów określonych w niniejszym rozporządzeniu w odniesieniu do wysokiego poziomu bezpieczeństwa. Takie środki uzupełniające powinny być niezawodne i łatwe w użyciu i mogłyby opierać się na możliwości korzystania z procedur zdalnej rejestracji, kwalifikowanych certyfikatów podpisu elektronicznego, kwalifikowanych elektronicznych poświadczeń atrybutów lub połączenia tych opcji. Aby zapewnić wystarczające upowszechnienie europejskich portfeli tożsamości cyfrowej, należy określić w aktach wykonawczych zharmonizowane specyfikacje techniczne i procedury dotyczące rejestracji użytkowników przy użyciu środków identyfikacji elektronicznej, w tym wydanych na średnim poziomie bezpieczeństwa.

(29) Celem niniejszego rozporządzenia jest zapewnienie użytkownikowi w pełni mobilnego, bezpiecznego i przyjaznego dla użytkownika europejskiego portfela tożsamości cyfrowej. Jako środek przejściowy – dopóki nie staną się dostępne certyfikowane rozwiązania zabezpieczające przed manipulacją, takie jak bezpieczne elementy w urządzeniach użytkowników – europejskie portfele tożsamości cyfrowej powinny opierać się na certyfikowanych zewnętrznych bezpiecznych elementach w celu ochrony materiału kryptograficznego i innych danych wrażliwych lub na notyfikowanych środkach identyfikacji elektronicznej na wysokim poziomie bezpieczeństwa w celu wykazania zgodności z odpowiednimi wymogami niniejszego rozporządzenia w odniesieniu do poziomu bezpieczeństwa europejskiego portfela tożsamości cyfrowej. Niniejsze rozporządzenie powinno pozostawać bez uszczerbku dla krajowych warunków w zakresie wydawania i stosowania certyfikowanego zewnętrznego bezpiecznego elementu, w przypadku gdy zastosowanie środka przejściowego zależy od tego bezpiecznego elementu.

(30) Europejskie portfele tożsamości cyfrowej powinny zapewniać najwyższy poziom ochrony danych i bezpieczeństwa na potrzeby identyfikacji elektronicznej i uwierzytelniania w celu ułatwienia dostępu do usług publicznych i prywatnych online, niezależnie od tego, czy takie dane są przechowywane lokalnie, czy przy użyciu rozwiązań opartych na chmurze, z należytym uwzględnieniem różnych poziomów ryzyka.

(31) Bezpieczeństwo europejskich portfeli tożsamości cyfrowej powinno być zapewnione już na etapie projektowania i powinny one wdrażać zaawansowane zabezpieczenia służące ochronie przed kradzieżą tożsamości i innymi rodzajami kradzieży danych, atakami prowadzącymi do odmowy usługi (ang. denial of service) oraz wszelkimi innymi zagrożeniami cyberbezpieczeństwa. Takie bezpieczeństwo powinno obejmować najnowocześniejsze metody szyfrowania i przechowywania danych, które dostępne są wyłącznie dla użytkownika i możliwe do odszyfrowania tylko przez niego, i które oparte są na pełnym szyfrowaniu komunikacji z innymi europejskimi portfelami tożsamości cyfrowej i stronami ufającymi. Ponadto europejskie portfele tożsamości cyfrowej powinny wymagać bezpiecznego, wyraźnego i aktywnego potwierdzenia przez użytkownika operacji wykonywanych za pośrednictwem europejskich portfeli tożsamości cyfrowej.

(32) Nieodpłatne używanie europejskich portfeli tożsamości cyfrowej nie powinno skutkować przetwarzaniem danych wykraczającym poza dane, które są niezbędne do świadczenia usług europejskiego portfela tożsamości cyfrowej. Niniejsze rozporządzenie nie powinno zezwalać na przetwarzanie danych osobowych – przechowywanych w europejskim portfelu tożsamości cyfrowej lub będących wynikiem używania go – przez dostawcę europejskiego portfela tożsamości cyfrowej do celów innych niż świadczenie usług europejskiego portfela tożsamości cyfrowej. Aby zapewnić prywatność, dostawcy europejskich portfeli tożsamości cyfrowej powinni zapewnić nieobserwowalność, nie zbierając danych i nie posiadając wglądu w transakcje użytkowników europejskiego portfela tożsamości cyfrowej. Taka nieobserwowalność oznacza, że dostawcy nie mają możliwości zapoznania się ze szczegółami transakcji dokonywanych przez użytkownika. Jednakże w szczególnych przypadkach, na podstawie wcześniejszej wyraźnej zgody użytkownika w każdym z tych szczególnych przypadków oraz w pełnej zgodności z rozporządzeniem (UE) 2016/679 dostawcy europejskich portfeli tożsamości cyfrowej mogliby uzyskać dostęp

do informacji niezbędnych do świadczenia konkretnej usługi związanej z europejskimi portfelami tożsamości cyfrowej.

(33) Przejrzystość funkcjonowania europejskich portfeli tożsamości cyfrowej oraz rozliczalność ich dostawców to kluczowe elementy pozwalające budować zaufanie społeczne oraz sprawić, aby ramy te były akceptowane. Dlatego funkcjonowanie europejskich portfeli tożsamości cyfrowej powinno być przejrzyste oraz, w szczególności, powinno umożliwiać weryfikowalne przetwarzanie danych osobowych. Aby to osiągnąć, państwa członkowskie powinny ujawniać kod źródłowy komponentów oprogramowania użytkownika europejskich portfeli tożsamości cyfrowej, w tym tych, które są związane z przetwarzaniem danych osobowych i danych osób prawnych. Publikacja tego kodu źródłowego w ramach licencji otwartego oprogramowania powinna umożliwić społeczeństwu, w tym użytkownikom i programistom, zrozumienie jego funkcjonowania, audyt i przegląd kodu. Zwiększyłoby to również zaufanie użytkowników do systemu oraz – poprzez umożliwienie każdemu zgłaszania słabych punktów i błędów w kodzie – przyczyniłoby się do zwiększenia bezpieczeństwa europejskich portfeli tożsamości cyfrowej. Ogólnie rzecz biorąc, powinno to stanowić zachętę dla dostawców do dostarczania i utrzymywania wysoce bezpiecznego produktu. Jednakże w niektórych przypadkach ujawnienie kodu źródłowego wykorzystywanych bibliotek programistycznych, kanału komunikacji lub innych elementów, które nie są przechowywane na urządzeniu użytkownika, mogłoby zostać ograniczone przez państwa członkowskie z należycie uzasadnionych powodów, zwłaszcza ze względu na bezpieczeństwo publiczne.

(34) Używanie europejskich portfeli tożsamości cyfrowej, a także zaprzestanie ich używania powinno stanowić wyłączne prawo i wyłączny wybór użytkowników. Państwa członkowskie powinny opracować proste i bezpieczne procedury umożliwiające użytkownikom żądanie natychmiastowego unieważnienia europejskich portfeli tożsamości cyfrowej, w tym w przypadku utraty lub kradzieży. Należy ustanowić mechanizm, który po śmierci użytkownika lub zaprzestaniu działalności przez osobę prawną pozwoli organowi odpowiedzialnemu za rozstrzyganie w sprawie dziedziczenia po osobie fizycznej lub w kwestiach majątkowych osoby prawnej zażądać natychmiastowego unieważnienia europejskich portfeli tożsamości cyfrowej.

(35) Aby promować upowszechnienie europejskich portfeli tożsamości cyfrowej oraz szersze stosowanie tożsamości cyfrowych, państwa członkowskie powinny nie tylko promować korzyści płynące z odpowiednich usług, ale powinny także – we współpracy z sektorem prywatnym, naukowcami i środowiskiem akademickim – opracowywać programy szkoleniowe mające na celu wzmocnienie umiejętności cyfrowych swoich obywateli i rezydentów, w szczególności grup szczególnie wrażliwych, takich jak osoby z niepełnosprawnościami i osoby starsze. Państwa członkowskie powinny także upowszechniać wiedzę na temat korzyści i zagrożeń związanych z europejskimi portfelami tożsamości cyfrowej za pomocą kampanii informacyjnych.

(36) Aby zapewnić otwartość europejskich ram tożsamości cyfrowej na innowacje i rozwój technologiczny oraz aby ramy te wytrzymywały próbę czasu, zachęca się państwa członkowskie, wspólnie, do tworzenia piaskownic do testowania innowacyjnych rozwiązań w kontrolowanym i bezpiecznym środowisku, w szczególności w celu poprawy funkcjonalności, ochrony danych osobowych, bezpieczeństwa i interoperacyjności rozwiązań oraz w celu uzyskiwania informacji na potrzeby przyszłego aktualizowania technicznych dokumentów referencyjnych i wymogów prawnych. Środowisko to powinno sprzyjać włączeniu MŚP, przedsiębiorstw typu start-up oraz indywidualnych innowatorów i badaczy, a także odpowiednich zainteresowanych stron z branży. Takie inicjatywy powinny przyczyniać się do osiągnięcia oraz powodować wzmocnienie zgodności regulacyjnej i odporności technicznej europejskich portfeli tożsamości cyfrowej, które mają być zapewniane obywatelom i rezydentom Unii, a tym samym zapobiegać opracowywaniu rozwiązań, które nie są zgodne z prawem Unii dotyczącym ochrony danych lub zawierają luki w zakresie bezpieczeństwa.

(37) Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2019/1157 ([11]) zwiększa bezpieczeństwo dowodów osobistych z ulepszonymi zabezpieczeniami do sierpnia 2021 r. Państwa członkowskie powinny rozważyć, czy mogą notyfikować te dowody w ramach systemów identyfikacji elektronicznej, aby zwiększyć transgraniczną dostępność środków identyfikacji elektronicznej.

(38) Proces notyfikacji systemów identyfikacji elektronicznej należy uprościć i przyspieszyć, aby promować dostęp do wygodnych, zaufanych, bezpiecznych i innowacyjnych rozwiązań w zakresie uwierzytelniania i identyfikacji oraz, w stosownych przypadkach, zachęcać prywatnych dostawców usług w zakresie tożsamości do oferowania organom państw członkowskich systemów identyfikacji elektronicznej do notyfikacji jako krajowe systemy identyfikacji elektronicznej na podstawie rozporządzenia (UE) nr 910/2014.

([11]) Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2019/1157 z dnia 20 czerwca 2019 r. w sprawie poprawy zabezpieczeń dowodów osobistych obywateli Unii i dokumentów pobytowych wydawanych obywatelom Unii i członkom ich rodzin korzystającym z prawa do swobodnego przemieszczania się (Dz.U. L 188 z 12.7.2019, s. 67).

(39) Usprawnienie obecnych procedur notyfikacji i wzajemnej oceny zapobiegnie niejednorodnemu podejściu do oceny różnych notyfikowanych systemów identyfikacji elektronicznej oraz ułatwi budowanie zaufania między państwami członkowskimi. Nowe, uproszczone mechanizmy mają na celu sprzyjanie współpracy państw członkowskich w zakresie bezpieczeństwa i interoperacyjności ich notyfikowanych systemów identyfikacji elektronicznej.

(40) Państwa członkowskie powinny skorzystać na nowych, elastycznych narzędziach służących do zapewniania zgodności z wymogami niniejszego rozporządzenia oraz odpowiednich aktów wykonawczych przyjętych na jego podstawie. Niniejsze rozporządzenie powinno umożliwiać państwom członkowskim korzystanie ze sprawozdań i ocen sporządzonych przez akredytowane jednostki oceniające zgodność, jak przewidziano w kontekście programów certyfikacji, które mają zostać ustanowione na poziomie Unii na podstawie rozporządzenia (UE) 2019/881, na poparcie ich wniosków dotyczących dostosowania systemów lub ich części do rozporządzenia (UE) nr 910/2014.

(41) Dostawcy usług publicznych wykorzystują dane identyfikujące osobę dostępne ze środków identyfikacji elektronicznej zgodnie z rozporządzeniem (UE) nr 910/2014, aby dopasować tożsamość elektroniczną użytkowników z innych państw członkowskich do danych identyfikujących osobę wydanych tym użytkownikom w państwie członkowskim przeprowadzającym transgraniczne dopasowywanie tożsamości. Jednakże w wielu przypadkach, pomimo stosowania minimalnego zbioru danych udostępnianego w ramach notyfikowanych systemów identyfikacji elektronicznej, zapewnienie dokładnego dopasowania tożsamości, gdy państwa członkowskie działają jako strony ufające, wymaga dodatkowych informacji na temat użytkownika oraz szczególnych uzupełniających procedur jednoznacznej identyfikacji, które należy przeprowadzić na poziomie krajowym. W celu dalszego wspomagania użyteczności środków identyfikacji elektronicznej, świadczenia lepszych usług publicznych online oraz zwiększenia pewności prawa w odniesieniu do tożsamości elektronicznej użytkowników, w rozporządzeniu (UE) nr 910/2014 należy zobowiązać państwa członkowskie do wprowadzenia szczególnych środków online w celu zapewnienia jednoznacznego dopasowywania tożsamości, gdy użytkownicy zamierzają uzyskać dostęp do transgranicznych usług publicznych online.

(42) Podczas prac nad europejskimi portfelami tożsamości cyfrowej niezbędne jest uwzględnienie potrzeb użytkowników. Dostępne powinny być istotne zastosowania i usługi online wykorzystujące europejskie portfele tożsamości cyfrowej. Dla wygody użytkowników oraz aby zapewnić transgraniczną dostępność takich usług, ważne jest podjęcie działań w celu ułatwienia zastosowania podobnego podejścia do projektowania, rozwijania i wdrażania usług online we wszystkich państwach członkowskich. Użytecznym narzędziem umożliwiającym osiągnięcie tego celu mogą być niewiążące wytyczne dotyczące sposobu projektowania, rozwijania i wdrażania usług online wykorzystujących europejskie portfele tożsamości cyfrowej. Takie wytyczne należy przygotować z uwzględnieniem unijnych ram interoperacyjności. Państwa członkowskie powinny odgrywać wiodącą rolę w przyjmowaniu tych wytycznych.

(43) Zgodnie z dyrektywą Parlamentu Europejskiego i Rady (UE) 2019/882 ([12]) osoby z niepełnosprawnościami powinny móc używać europejskie portfele tożsamości cyfrowej, usługi zaufania oraz produkty przeznaczone dla użytkownika końcowego wykorzystywane do świadczenia tych usług na równi z innymi użytkownikami.

(44) Aby zapewnić skuteczne egzekwowanie niniejszego rozporządzenia, należy ustanowić minimalny poziom maksymalnych administracyjnych kar pieniężnych zarówno dla kwalifikowanych, jak i niekwalifikowanych dostawców usług zaufania. Państwa członkowskie powinny ustanowić skuteczne, proporcjonalne i odstraszające kary. Przy określaniu kar należy odpowiednio uwzględnić wielkość podmiotów, których to dotyczy, ich modele biznesowe oraz wagę naruszeń.

(45) Państwa członkowskie powinny ustanowić przepisy dotyczące kar za naruszenia, takie jak bezpośrednie lub pośrednie praktyki prowadzące do wprowadzenia w błąd w zakresie odróżniania niekwalifikowanych usług zaufania od kwalifikowanych usług zaufania, lub prowadzące do nadużywania unijnego znaku zaufania przez niekwalifikowanych dostawców usług zaufania. Unijny znak zaufania nie powinien być używany na warunkach, które bezpośrednio lub pośrednio prowadzą do przekonania, że jakiekolwiek niekwalifikowane usługi zaufania oferowane przez tych dostawców są usługami kwalifikowanymi.

(46) Niniejsze rozporządzenie nie powinno obejmować aspektów związanych z zawieraniem i ważnością umów lub innych zobowiązań prawnych, w przypadku gdy istnieją wymogi dotyczące formy ustanowione w prawie Unii lub prawie krajowym. Dodatkowo nie powinno ono mieć wpływu na krajowe wymogi w zakresie formy dotyczące rejestrów publicznych, w szczególności rejestrów handlowych i rejestrów gruntów.

([12]) 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).

(47) Świadczenie usług zaufania i korzystanie z nich oraz korzyści pod względem wygody i pewności prawa w kontekście transakcji transgranicznych, w szczególności w przypadku korzystania z kwalifikowanych usług zaufania, stają się coraz ważniejsze dla handlu międzynarodowego i współpracy międzynarodowej. Partnerzy międzynarodowi Unii tworzą ramy zaufania wzorowane na rozporządzeniu (UE) nr 910/2014. Aby w związku z tym ułatwić uznawanie takich kwalifikowanych usług zaufania i ich dostawców, Komisja może przyjmować akty wykonawcze określające warunki, na których ramy zaufania państw trzecich można uznać za równoważne określonym w niniejszym rozporządzeniu ramom zaufania dotyczącym kwalifikowanych usług zaufania i kwalifikowanych dostawców tych usług. Takie podejście powinno być uzupełnieniem możliwości wzajemnego uznawania usług zaufania i dostawców tych usług mających siedzibę w Unii i w państwach trzecich zgodnie z art. 218 Traktatu o funkcjonowaniu Unii Europejskiej (TFEU). Określając warunki, na jakich ramy zaufania państw trzecich można uznać za równoważne ramom zaufania dotyczącym kwalifikowanych usług zaufania i kwalifikowanych dostawców tych usług na podstawie rozporządzenia (UE) nr 910/2014, należy również zapewnić zgodność z odpowiednimi przepisami dyrektywy Parlamentu Europejskiego i Rady (UE) 2022/2555 ([13]) i rozporządzenia (UE) 2016/679, a także wykorzystanie zaufanych list jako istotnych elementów budowania zaufania.

(48) Niniejsze rozporządzenie powinno sprzyjać możliwości dokonywania wyboru między europejskimi portfelami tożsamości cyfrowej oraz ich zmiany, w przypadku gdy państwo członkowskie zatwierdziło na swoim terytorium więcej niż jedno rozwiązanie w zakresie europejskiego portfela tożsamości cyfrowej. Aby uniknąć w takich sytuacjach efektu uzależnienia od dostawcy, dostawcy europejskich portfeli tożsamości cyfrowej powinni – w przypadku gdy jest to technicznie wykonalne – zapewnić skuteczną możliwość przenoszenia danych na żądanie użytkowników europejskiego portfela tożsamości cyfrowej oraz nie powinni mieć prawa do stosowania barier umownych, ekonomicznych lub technicznych w celu uniemożliwienia skutecznej zmiany europejskiego portfela tożsamości cyfrowej na inny lub w celu zniechęcania do takiej zmiany.

(49) Aby zapewnić właściwe funkcjonowanie europejskich portfeli tożsamości cyfrowej, dostawcy europejskich portfeli tożsamości cyfrowej potrzebują skutecznej interoperacyjności oraz sprawiedliwych, rozsądnych i niedyskryminujących warunków dostępu europejskich portfeli tożsamości cyfrowej do określonych funkcji sprzętu i oprogramowania urządzeń mobilnych. Elementy te mogłyby obejmować w szczególności anteny komunikacji zbliżeniowej (ang. near field communication) i bezpieczne elementy, w tym uniwersalne karty elektroniczne (ang. Universal Integrated Circuit Cards), wbudowane bezpieczne elementy (ang. embedded secure elements), karty mikroSD i Bluetooth o niskim zużyciu energii (ang. Bluetooth Low Energy). Dostęp do tych elementów mógłby podlegać kontroli operatorów sieci mobilnych i producentów sprzętu. W związku z tym, w przypadku gdy jest to konieczne do świadczenia usług związanych z europejskimi portfelami tożsamości cyfrowej, producenci oryginalnego sprzętu urządzeń mobilnych lub dostawcy usług łączności elektronicznej nie powinni odmawiać dostępu do takich komponentów. Ponadto przedsiębiorstwa wskazane jako strażnicy dostępu w odniesieniu do podstawowych usług platformowych, wymienione przez Komisję na podstawie rozporządzenia Parlamentu Europejskiego i Rady (UE) 2022/1925 ([14]), powinny nadal podlegać przepisom szczegółowym tego rozporządzenia, w oparciu o jego art. 6 ust. 7.

(50) Aby usprawnić spełnianie obowiązków w zakresie cyberbezpieczeństwa nałożone na dostawców usług zaufania, a także umożliwić tym dostawcom i ich odpowiednim właściwym organom korzystanie z ram prawnych ustanowionych dyrektywą (UE) 2022/2555, dostawcy usług zaufania zobowiązani są do wprowadzenia odpowiednich środków technicznych i organizacyjnych na podstawie tej dyrektywy, takich jak środki służące przeciwdziałaniu awariom systemu, błędom ludzkim, szkodliwym działaniom lub zjawiskom naturalnym, w celu zarządzania ryzykiem w zakresie bezpieczeństwa sieci i systemów informatycznych, z których dostawcy ci korzystają przy świadczeniu swoich usług, a także w celu zgłaszania poważnych incydentów i zagrożeń cyberbezpieczeństwa zgodnie z tą dyrektywą. Jeżeli chodzi o zgłaszanie incydentów, dostawcy usług zaufania powinni zgłaszać wszelkie incydenty mające znaczący wpływ na świadczenie ich usług, w tym incydenty spowodowane kradzieżą, utratą urządzeń lub uszkodzeniem kabli sieciowych lub incydenty występujące w kontekście identyfikacji osób. Wymogi w zakresie zarządzania ryzykiem w cyberprzestrzeni oraz obowiązki w zakresie zgłaszania incydentów określone w dyrektywie (UE) 2022/2555 należy uznać za uzupełniające w stosunku do wymogów nałożonych na podstawie niniejszego rozporządzenia na dostawców usług zaufania. W stosownych przypadkach właściwe organy wyznaczone na podstawie dyrektywy (UE) 2022/2555 powinny nadal stosować ustalone praktyki lub wytyczne krajowe dotyczące wdrażania wymogów w zakresie bezpieczeństwa i sprawozdawczości oraz nadzoru nad zgodnością z takimi wymogami na podstawie rozporządzenia (UE) nr 910/2014. Niniejsze rozporządzenie nie ma wpływu na obowiązek zgłaszania naruszeń ochrony danych osobowych zgodnie z rozporządzeniem (UE) 2016/679.

([13]) 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).

([14]) 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).

(51) Należy zwrócić należytą uwagę na zapewnienie skutecznej współpracy między organami nadzoru wyznaczonymi na podstawie art. 46b rozporządzenia (UE) nr 910/2014 a właściwymi organami wyznaczonymi lub ustanowionymi na podstawie art. 8 ust. 1 dyrektywy (UE) 2022/2555. W przypadku gdy organ nadzoru nie jest jednocześnie właściwym organem, organ nadzoru i właściwy organ powinny ściśle i terminowo współpracować poprzez wymianę odpowiednich informacji, aby zapewnić skuteczny nadzór nad dostawcami usług zaufania oraz przestrzeganie przez nich wymogów określonych w rozporządzeniu (UE) nr 910/2014 i w dyrektywie (UE) 2022/2555. W szczególności, organy nadzoru wyznaczone na podstawie rozporządzenia (UE) nr 910/2014 powinny być uprawnione do zwracania się do właściwych organów wyznaczonych lub ustanowionych na podstawie dyrektywy (UE) 2022/2555 o udzielenie odpowiednich informacji potrzebnych do przyznania statusu kwalifikowanego oraz do przeprowadzenia działań nadzorczych w celu zweryfikowania zgodności dostawców usług zaufania z odpowiednimi wymogami określonymi w dyrektywie (UE) 2022/2555 lub zażądania od tych dostawców, aby wyeliminowali niezgodności z tymi wymogami.

(52) Istotne jest ustanowienie ram prawnych służących ułatwieniu transgranicznego uznawania istniejących krajowych rozwiązań prawnych, związanych z usługami rejestrowanego doręczenia elektronicznego. Ramy te mogłyby stworzyć także nowe możliwości rynkowe dla unijnych dostawców usług zaufania w odniesieniu do oferowania nowych ogólnounijnych usług rejestrowanego doręczenia elektronicznego. W celu zapewnienia, aby dane przesyłane za pomocą kwalifikowanej usługi rejestrowanego doręczenia elektronicznego zostały dostarczone do właściwego adresata, kwalifikowane usługi rejestrowanego doręczenia elektronicznego powinny zapewniać z całkowitą pewnością identyfikację adresata, przy czym do identyfikacji nadawcy wystarczyłaby duża doza pewności. Państwa członkowskie powinny zachęcać dostawców kwalifikowanych usług rejestrowanego doręczenia elektronicznego do zapewnienia interoperacyjności ich usług z kwalifikowanymi usługami rejestrowanego doręczenia elektronicznego świadczonymi przez innych kwalifikowanych dostawców usług zaufania w celu łatwego przesyłania rejestrowanych elektronicznie danych między dwoma kwalifikowanymi dostawcami usług zaufania lub większą ich liczbą oraz promowania uczciwych praktyk na rynku wewnętrznym.

(53) W większości przypadków obywatele i rezydenci Unii nie mają możliwości – w sposób bezpieczny oraz z zapewnieniem wysokiego stopnia ochrony danych – dokonywania transgranicznej wymiany informacji cyfrowych związanych z ich tożsamością, takich jak ich adres, wiek, kwalifikacje zawodowe, prawo jazdy i inne zezwolenia oraz dane dotyczące płatności.

(54) Powinna istnieć możliwość wydawania i obsługi wiarygodnych atrybutów elektronicznych oraz przyczynienia się do zmniejszenia obciążenia administracyjnego poprzez umożliwienie obywatelom i rezydentom Unii korzystania z tych atrybutów w transakcjach prywatnych i publicznych. Obywatele i rezydenci Unii powinni móc na przykład wykazać posiadanie ważnego prawa jazdy wydanego przez organ w jednym państwie członkowskim, który to dokument odpowiednie organy w innych państwach członkowskich mogą zweryfikować i na którym mogą polegać, oraz powinni móc korzystać ze swoich uprawnień w zakresie ubezpieczenia społecznego lub z przyszłych cyfrowych dokumentów podróży w kontekście transgranicznym.

(55) Każdy dostawca usług, który wydaje poświadczone atrybuty w formie elektronicznej, takie jak dyplomy, zezwolenia, akty urodzenia lub pełnomocnictwa i upoważnienia do reprezentowania osób fizycznych lub prawnych, lub do działania w ich imieniu, powinien być uznawany za dostawcę usług zaufania w zakresie elektronicznego poświadczenia atrybutów. Nie należy odmawiać skutku prawnego elektronicznemu poświadczeniu atrybutów z tego powodu, że poświadczenie to ma postać elektroniczną lub że nie spełnia wymogów kwalifikowanego elektronicznego poświadczenia atrybutów. Należy ustanowić ogólne wymogi w celu zapewnienia, aby kwalifikowane elektroniczne poświadczenie atrybutów miało skutek prawny równoważny skutkowi prawnemu wystawionych zgodnie z prawem poświadczeń w formie papierowej. Wymogi te powinny jednak mieć zastosowanie bez uszczerbku dla prawa Unii lub prawa krajowego określającego dodatkowe wymogi sektorowe w odniesieniu do formy, której zachowanie wywołuje skutki prawne, a w szczególności – w stosownych przypadkach – do transgranicznego uznawania kwalifikowanego elektronicznego poświadczenia atrybutów.

(56) Szeroka dostępność i użyteczność europejskich portfeli tożsamości cyfrowej powinna prowadzić do większej ich akceptacji oraz zaufania do nich zarówno wśród osób prywatnych, jak i prywatnych dostawców usług. Prywatne strony ufające świadczące usługi na przykład w obszarach transportu, energetyki, bankowości i usług finansowych, zabezpieczenia społecznego, zdrowia, wody pitnej, usług pocztowych, infrastruktury cyfrowej, telekomunikacji lub edukacji, powinny zatem akceptować używanie europejskich portfeli tożsamości cyfrowej na potrzeby świadczenia usług, w przypadku gdy silne uwierzytelnienie użytkownika do celów identyfikacji elektronicznej wymagane jest na podstawie prawa Unii lub prawa krajowego, lub na podstawie zobowiązania umownego. Każdy wniosek strony ufającej o udzielenie informacji od użytkownika europejskiego portfela tożsamości cyfrowej powinien być niezbędny i proporcjonalny do zamierzonego wykorzystania w danym przypadku, powinien być zgodny z zasadą minimalizacji danych oraz powinien zapewniać przejrzystość w odniesieniu do tego, które dane są udostępniane i w jakich celach. Aby ułatwić używanie europejskich portfeli tożsamości cyfrowej oraz ich akceptację, przy ich wprowadzaniu należy uwzględnić powszechnie akceptowane normy i specyfikacje branżowe.

(57) W przypadku gdy bardzo duże platformy internetowe w rozumieniu art. 33 ust. 1 rozporządzenia Parlamentu Europejskiego i Rady (UE) 2022/2065 ([15]) wymagają, aby użytkownicy uwierzytelnili się do celów dostępu do usług online, platformy te powinny być zobowiązane do akceptowania europejskich portfeli tożsamości cyfrowej na dobrowolny wniosek użytkownika. Użytkownicy nie powinni być zobowiązani do używania europejskiego portfela tożsamości cyfrowej w celu uzyskania dostępu do usług prywatnych, a ich dostęp do usług nie powinien być ograniczany ani utrudniany ze względu na to, że nie używają europejskiego portfela tożsamości cyfrowej. Jeżeli jednak użytkownicy wyrażą taką wolę, bardzo duże platformy internetowe powinny akceptować te portfele do tego celu, przy jednoczesnym poszanowaniu zasady minimalizacji danych i prawa użytkowników do używania dowolnie wybranych pseudonimów. Biorąc pod uwagę znaczenie bardzo dużych platform internetowych ze względu na ich zasięg, w szczególności wyrażony liczbą odbiorców usługi i transakcji gospodarczych, obowiązek akceptowania europejskich portfeli tożsamości cyfrowej jest niezbędny, aby zwiększyć ochronę użytkowników przed oszustwami oraz zapewnić wysoki poziom ochrony danych.

(58) Aby przyczynić się do zapewnienia szerokiej dostępności i użyteczności środków identyfikacji elektronicznej, w tym europejskich portfeli tożsamości cyfrowej objętych zakresem stosowania niniejszego rozporządzenia, należy opracować kodeksy postępowania na poziomie Unii. Kodeksy postępowania powinny ułatwiać szeroką akceptację środków identyfikacji elektronicznej, w tym europejskich portfeli tożsamości cyfrowej, przez tych dostawców usług, którzy nie kwalifikują się jako bardzo duże platformy i którzy do celów uwierzytelniania użytkownika polegają na usługach identyfikacji elektronicznej świadczonych przez strony trzecie.

(59) Selektywne ujawnianie polega na umożliwieniu właścicielowi danych ujawniania jedynie niektórych części większego zbioru danych, aby podmiot otrzymujący mógł uzyskać tylko takie informacje, które są niezbędne do świadczenia usługi żądanej przez użytkownika. Europejski portfel tożsamości cyfrowej powinien pod względem technicznym umożliwiać selektywne ujawnianie atrybutów stronom ufającym. Użytkownik powinien mieć techniczną możliwość selektywnego ujawniania atrybutów, w tym z wielu odrębnych poświadczeń elektronicznych, oraz łączyć i prezentować je w sposób niezakłócony stronom ufającym. Funkcja ta powinna stać się jedną z podstawowych cech europejskich portfeli tożsamości cyfrowej, co zwiększy wygodę i ochronę danych osobowych, w tym minimalizację danych.

(60) Nie należy zakazywać dostępu do usług przy użyciu pseudonimu, chyba że przepisy szczególne prawa Unii lub prawa krajowego wymagają od użytkowników zidentyfikowania się.

(61) Atrybuty dostarczane przez kwalifikowanych dostawców usług zaufania w ramach kwalifikowanego poświadczenia atrybutów powinny być weryfikowane względem źródeł autentycznych bezpośrednio przez kwalifikowanego dostawcę usług zaufania albo poprzez wyznaczonych pośredników uznanych na poziomie krajowym zgodnie z prawem Unii lub prawem krajowym do celów bezpiecznej wymiany poświadczonych atrybutów między dostawcami usług w zakresie tożsamości lub dostawcami usług poświadczania atrybutów a stronami ufającymi. Państwa członkowskie powinny ustanowić odpowiednie mechanizmy na poziomie krajowym w celu zapewnienia, aby kwalifikowani dostawcy usług zaufania wydający kwalifikowane elektroniczne poświadczenie atrybutów mogli – za zgodą osoby, której wydano poświadczenie – weryfikować autentyczność atrybutów na podstawie źródeł autentycznych. Powinna istnieć możliwość, aby odpowiednie mechanizmy obejmowały korzystanie – zgodnie z prawem krajowym – z konkretnych pośredników lub rozwiązań technicznych umożliwiających dostęp do źródeł autentycznych. Zapewnienie dostępności mechanizmu, który umożliwia weryfikację atrybutów względem źródeł autentycznych, ma na celu ułatwienie kwalifikowanym dostawcom usług zaufania, którzy dostarczają kwalifikowane elektroniczne poświadczenia atrybutów, przestrzegania ich obowiązków określonych w rozporządzeniu (UE) nr 910/2014. Nowy załącznik do tego rozporządzenia powinien zawierać wykaz kategorii atrybutów, w odniesieniu do których państwa członkowskie mają zapewnić wprowadzenie środków umożliwiających kwalifikowanym dostawcom elektronicznych poświadczeń atrybutów zweryfikowanie drogą elektroniczną, na żądanie użytkownika, ich autentyczności względem odpowiedniego źródła autentycznego.

(62) Bezpieczna identyfikacja elektroniczna oraz dostarczanie poświadczeń atrybutów powinny zapewniać sektorowi usług finansowych dodatkową elastyczność oraz rozwiązania umożliwiające identyfikację klientów i wymianę specjalnych atrybutów niezbędnych do spełnienia, na przykład, wymogów należytej staranności wobec klienta wynikających z przyszłego rozporządzenia ustanawiającego Urząd ds. Przeciwdziałania Praniu Pieniędzy, wymogów dotyczących odpowiedniego zachowania wynikających z przepisów dotyczących ochrony inwestorów lub do spełnienia wymogów silnego uwierzytelniania klienta w odniesieniu do identyfikacji elektronicznej na potrzeby logowania się na konto i inicjowania transakcji w dziedzinie usług płatniczych.

(63) Skutek prawny podpisu elektronicznego nie powinien być kwestionowany na tej podstawie, że podpis ma postać elektroniczną lub nie spełnia wymogów kwalifikowanego podpisu elektronicznego. Skutek prawny podpisów elektronicznych określa się jednak w prawie krajowym, z wyjątkiem wymogów przewidzianych w niniejszym rozporządzeniu, zgodnie z którymi skutek prawny kwalifikowanego podpisu elektronicznego należy uznać za równoważny skutkowi prawnemu podpisu własnoręcznego. Przy określaniu skutków prawnych podpisów elektronicznych, państwa członkowskie powinny uwzględnić zasadę proporcjonalności między mocą prawną podpisywanego dokumentu, poziomem bezpieczeństwa oraz kosztami związanymi z podpisem elektronicznym.

([15]) 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).

Aby zwiększyć dostępność i wykorzystywanie podpisów elektronicznych, zachęca się państwa członkowskie, aby rozważyły wykorzystywanie zaawansowanych podpisów elektronicznych w bieżących transakcjach, w odniesieniu do których zapewniają one dostateczny poziom bezpieczeństwa i zaufania.

(64) Aby zapewnić spójność praktyk certyfikacji w całej Unii, Komisja powinna wydać wytyczne dotyczące certyfikacji i odnowienia certyfikacji kwalifikowanych urządzeń do składania podpisu elektronicznego oraz kwalifikowanych urządzeń do składania pieczęci elektronicznej, w tym ich ważności i ograniczeń w czasie. Niniejsze rozporządzenie nie uniemożliwia podmiotom publicznym lub prywatnym, które posiadają certyfikowane kwalifikowane urządzenia do składania podpisu elektronicznego, czasowego odnowienia certyfikacji takich urządzeń na krótki okres certyfikacji, w oparciu o wyniki poprzedniego procesu certyfikacji, w przypadku gdy takiego odnowienia certyfikacji nie można przeprowadzić w prawnie określonych ramach czasowych z powodu innego niż naruszenie lub incydent bezpieczeństwa, a także bez uszczerbku dla obowiązku przeprowadzenia oceny podatności na zagrożenia oraz bez uszczerbku dla mającej zastosowanie praktyki dotyczącej certyfikacji.

(65) Wydawanie certyfikatów uwierzytelniania witryn internetowych ma na celu zapewnienie użytkownikom dużej dozy pewności co do tożsamości podmiotu stojącego za daną witryną internetową, bez względu na to, jaka platforma jest wykorzystywana do wyświetlenia tej tożsamości. Certyfikaty te powinny przyczyniać się do budowy zaufania do prowadzenia działalności gospodarczej online, ponieważ użytkownicy będą mieli pewność co do witryny internetowej, która została uwierzytelniona. Korzystanie przez witryny internetowe z takich certyfikatów powinno być dobrowolne. Jednakże, aby uwierzytelnianie witryny internetowej stało się środkiem zwiększenia zaufania, zapewnienia użytkownikowi lepszego doświadczenia oraz wspierania wzrostu na rynku wewnętrznym, niniejsze rozporządzenie ustanawia ramy zaufania obejmujące minimalne obowiązki w zakresie bezpieczeństwa i odpowiedzialności dla dostawców kwalifikowanych certyfikatów uwierzytelniania witryn internetowych oraz wymogów dotyczących wydawania tych certyfikatów. Krajowe zaufane listy powinny potwierdzać kwalifikowany status usług uwierzytelniania witryn internetowych i dostawców tych usług zaufania, w tym ich pełną zgodność z wymogami niniejszego rozporządzenia w odniesieniu do wydawania kwalifikowanych certyfikatów uwierzytelniania witryn internetowych. Uznawanie kwalifikowanych certyfikatów uwierzytelniania witryn internetowych oznacza, że dostawcy przeglądarek internetowych nie powinni podważać autentyczności kwalifikowanych certyfikatów uwierzytelniania stron internetowych służących wyłącznie do potwierdzenia związku między nazwą domeny witryny internetowej a osobą fizyczną lub prawną, której wydano certyfikat, lub do potwierdzenia tożsamości tej osoby. Dostawcy przeglądarek internetowych powinni wyświetlać certyfikowane dane dotyczące tożsamości oraz inne poświadczone atrybuty użytkownikowi końcowemu w sposób przyjazny dla użytkownika w środowisku przeglądarki, korzystając z wybranych przez siebie środków technicznych. W tym celu dostawcy przeglądarek internetowych powinni zapewniać obsługę kwalifikowanych certyfikatów uwierzytelniania witryn internetowych wydanych w pełnej zgodności z niniejszym rozporządzeniem oraz interoperacyjność z tymi certyfikatami. Obowiązek uznawania oraz interoperacyjności i obsługi kwalifikowanych certyfikatów uwierzytelniania witryn internetowych nie wpływa na swobodę dostawców przeglądarek internetowych w zakresie zapewniania bezpieczeństwa sieci, uwierzytelniania domen oraz szyfrowania ruchu sieciowego w taki sposób i przy użyciu takich technologii, które uznają za najodpowiedniejsze. Aby przyczynić się do bezpieczeństwa użytkowników końcowych w internecie, dostawcy przeglądarek internetowych powinni – w wyjątkowych okolicznościach – mieć możliwość wprowadzania środków zapobiegawczych, które będą zarówno konieczne, jak i proporcjonalne, w odpowiedzi na uzasadnione podejrzenia dotyczące naruszeń bezpieczeństwa lub utraty integralności określonego certyfikatu lub zestawu certyfikatów. W przypadku wprowadzenia przez nich takich środków zapobiegawczych dostawcy przeglądarek internetowych powinni – bez zbędnej zwłoki – powiadomić Komisję, krajowy organ nadzoru oraz podmiot, któremu wydano dany certyfikat, oraz kwalifikowanego dostawcę usług zaufania, który wydał ten certyfikat lub zestaw certyfikatów, o wszelkich podejrzeniach związanych z takim naruszeniem bezpieczeństwa lub utratą integralności, a także o środkach wprowadzonych w odniesieniu do pojedynczego certyfikatu lub zestawu certyfikatów. Środki te powinny pozostawać bez uszczerbku dla obowiązku dostawców przeglądarek w zakresie uznawania kwalifikowanych certyfikatów uwierzytelniania witryn internetowych zgodnie z krajowymi zaufanymi listami. W celu dalszej ochrony obywateli i rezydentów Unii oraz propagowania korzystania z kwalifikowanych certyfikatów uwierzytelniania witryn internetowych, organy publiczne w państwach członkowskich powinny rozważyć włączenie kwalifikowanych certyfikatów uwierzytelniania witryn internetowych do swoich witryn internetowych. Przewidziane w niniejszym rozporządzeniu środki, których celem jest zapewnienie większej spójności między stosowanymi przez państwa członkowskie rozbieżnymi podejściami i praktykami dotyczącymi procedur nadzorczych, mają przyczynić się do zwiększenia zaufania oraz pewności co do bezpieczeństwa, jakości oraz dostępności kwalifikowanych certyfikatów uwierzytelniania witryn internetowych.

(66) Wiele państw członkowskich wprowadziło krajowe wymogi dotyczące usług zapewniających bezpieczną i wiarygodną archiwizację elektroniczną, aby umożliwić długoterminowe przechowywanie danych i dokumentów elektronicznych oraz powiązanych usług zaufania. Aby zapewnić pewność prawa, zaufanie i harmonizację we wszystkich państwach członkowskich, należy ustanowić ramy prawne dla kwalifikowanych usług archiwizacji elektronicznej, wzorowane na ramach dla innych usług zaufania określonych w niniejszym rozporządzeniu. Ramy prawne kwalifikowanych usług archiwizacji elektronicznej powinny oferować dostawcom usług zaufania i użytkownikom skuteczny zestaw narzędzi obejmujący wymogi funkcjonalne dotyczące usługi archiwizacji elektronicznej, a także jasne skutki prawne w przypadku korzystania z kwalifikowanej usługi archiwizacji elektronicznej. Przepisy te powinny mieć zastosowanie do danych elektronicznych i dokumentów elektronicznych sporządzonych w postaci elektronicznej oraz dokumentów papierowych, które zostały zeskanowane i zdigitalizowane. W razie potrzeby przepisy te powinny pozwalać na przenoszenie przechowywanych danych i dokumentów

elektronicznych na inne nośniki lub formaty w celu przedłużenia ich trwałości i czytelności poza technologiczny okres ważności, przy jednoczesnym zapobieganiu w możliwie największym zakresie stratom i modyfikacji. W przypadku gdy dane i dokumenty elektroniczne przekazywane do usługi archiwizacji elektronicznej zawierają co najmniej jeden kwalifikowany podpis elektroniczny lub kwalifikowaną pieczęć elektroniczną, w ramach usługi należy stosować procedury i technologie, które mogą przedłużyć ich wiarygodność na okres przechowywania takich danych, w miarę możliwości w oparciu o wykorzystanie innych kwalifikowanych usług zaufania ustanowionych na podstawie niniejszego rozporządzenia. W celu tworzenia dowodów konserwacji w przypadku użycia podpisów elektronicznych, pieczęci elektronicznych lub elektronicznych znaczników czasu należy korzystać z kwalifikowanych usług zaufania. W zakresie, w jakim usługi archiwizacji elektronicznej nie są harmonizowane na podstawie niniejszego rozporządzenia, państwa członkowskie powinny mieć możliwość utrzymania lub wprowadzenia, zgodnie z prawem Unii, przepisów krajowych odnoszących się do tych usług, takich jak przepisy szczegółowe dotyczące usług zintegrowanych w ramach danej organizacji i wykorzystywanych wyłącznie do archiwów wewnętrznych tej organizacji. Niniejsze rozporządzenie nie powinno wprowadzać rozróżnienia między danymi elektronicznymi i dokumentami elektronicznymi sporządzonymi w postaci elektronicznej a dokumentami fizycznymi, które zostały zdigitalizowane.

(67) Działalność krajowych archiwów i instytucji pamięci, jako organizacji, które w interesie publicznym zajmują się ochroną dziedzictwa mającego postać dokumentów, uregulowana jest zazwyczaj w prawie krajowym i niekoniecznie obejmuje świadczenie usług zaufania w rozumieniu niniejszego rozporządzenia. W zakresie, w jakim takie instytucje nie świadczą takich usług zaufania, niniejsze rozporządzenie pozostaje bez uszczerbku dla ich funkcjonowania.

(68) Rejestry elektroniczne to sekwencje elektronicznych wpisów danych zapewniające integralność tych wpisów danych oraz dokładność ich chronologicznego uporządkowania. Rejestry elektroniczne powinny ustanawiać chronologiczną sekwencję wpisów danych. W połączeniu z innymi technologiami powinny one przyczyniać się do opracowywania rozwiązań na rzecz bardziej efektywnych i transformacyjnych usług publicznych, takich jak głosowanie elektroniczne, transgraniczna współpraca organów celnych, transgraniczna współpraca instytucji akademickich oraz rejestrowanie własności nieruchomości w zdecentralizowanych rejestrach gruntów. Kwalifikowane rejestry elektroniczne powinny ustanawiać domniemanie prawne dotyczące niepowtarzalnego i dokładnego sekwencyjnego uporządkowania chronologicznego oraz integralności wpisów danych w rejestrze. Z uwagi na ich specyfikę, na przykład sekwencyjne uporządkowanie chronologiczne wpisów danych, rejestry elektroniczne powinny odróżniać się od innych usług zaufania, takich jak elektroniczne znaczniki czasu i usługi rejestrowanego doręczenia elektronicznego. W celu zapewnienia pewności prawa oraz promowania innowacji należy ustanowić ogólnounijne ramy prawne określające transgraniczne uznawanie usług zaufania do celów rejestrowania danych w rejestrach elektronicznych. Powinno to w wystarczającym stopniu zapobiec kopiowaniu i wielokrotnej sprzedaży tych samych aktywów cyfrowych różnym stronom. Proces tworzenia i aktualizacji rejestru elektronicznego zależy od rodzaju wykorzystywanego rejestru, tzn. czy jest on scentralizowany czy rozproszony. Niniejsze rozporządzenie powinno zapewniać neutralność technologiczną, tj. nie powinno faworyzować ani dyskryminować jakiejkolwiek technologii stosowanej przy wdrażaniu nowej usługi zaufania dla rejestrów elektronicznych. Ponadto przy przygotowywaniu aktów wykonawczych określających wymogi dotyczące kwalifikowanych rejestrów elektronicznych Komisja, stosując odpowiednie metodyki, powinna uwzględniać wskaźniki zrównoważonego rozwoju w odniesieniu do wszelkiego niekorzystnego wpływu na klimat lub w odniesieniu do innych niekorzystnych skutków związanych ze środowiskiem.

(69) Rolą dostawców usług zaufania w zakresie rejestrów elektronicznych powinno być potwierdzanie sekwencyjnego rejestrowania danych w rejestrze. Niniejsze rozporządzenie pozostaje bez uszczerbku dla wszelkich obowiązków prawnych użytkowników rejestrów elektronicznych, wynikających z prawa Unii lub prawa krajowego. I tak na przykład zastosowania związane z przetwarzaniem danych osobowych powinny być zgodne z rozporządzeniem (UE) 2016/679, a zastosowania związane z usługami finansowymi powinny być zgodne z odpowiednimi przepisami prawa Unii w zakresie usług finansowych.

(70) Aby uniknąć fragmentacji i barier na rynku wewnętrznym, wynikających z rozbieżnych norm i ograniczeń technicznych, oraz aby zapewnić skoordynowany proces wyeliminowania ich wpływu na wdrożenie europejskich ram tożsamości cyfrowej, potrzebna jest bliska i zorganizowana współpraca między Komisją, państwami członkowskimi, społeczeństwem obywatelskim, środowiskami akademickimi i sektorem prywatnym. Aby osiągnąć ten cel, państwa członkowskie i Komisja powinny współpracować w zakresie ram określonych w zaleceniu Komisji (UE) 2021/946 ([16]) nad określeniem wspólnego unijnego zestawu narzędzi na potrzeby europejskich ram tożsamości cyfrowej. W tym kontekście państwa członkowskie powinny uzgodnić kompleksową architekturę techniczną i ramy odniesienia, zestaw wspólnych norm i technicznych dokumentów referencyjnych, w tym uznane obowiązujące normy, oraz zestaw wytycznych i opisów najlepszych praktyk obejmujące co najmniej wszystkie funkcje i interoperacyjność europejskich portfeli tożsamości cyfrowej, w tym podpisów elektronicznych, oraz dostawców kwalifikowanej usługi zaufania do celów elektronicznego poświadczania atrybutów, jak określono w niniejszym rozporządzeniu. W tym kontekście państwa członkowskie powinny również uzgodnić wspólne elementy modelu biznesowego oraz strukturę opłat europejskich portfeli tożsamości cyfrowej, aby ułatwić korzystanie z tych portfeli,

([16]) Zalecenie Komisji (UE) 2021/946 z dnia 3 czerwca 2021 r. w sprawie wspólnego unijnego zestawu narzędzi na potrzeby skoordynowanego podejścia do europejskich ram tożsamości cyfrowej (Dz.U. L 210 z 14.6.2021, s. 51).

w szczególności przez MŚP, w kontekście transgranicznym. Zawartość zestawu narzędzi powinna ewoluować równolegle z postępami w dialogu i procesie przyjmowania europejskich ram tożsamości cyfrowej oraz powinna odzwierciedlać ich wyniki.

(71) Niniejsze rozporządzenie określa zharmonizowany poziom jakości, wiarygodności i bezpieczeństwa kwalifikowanych usług zaufania, niezależnie od miejsca prowadzenia operacji. W związku z tym kwalifikowany dostawca usług zaufania powinien mieć możliwość zlecania na zewnątrz swoich operacji związanych ze świadczeniem kwalifikowanej usługi zaufania w państwie trzecim, w przypadku gdy to państwo trzecie udzieli odpowiednich gwarancji zapewniających możliwość egzekwowania działań nadzorczych i audytów, tak jakby były one prowadzone w Unii. W przypadku gdy nie można w pełni zapewnić zgodności z niniejszym rozporządzeniem, organy nadzoru powinny mieć możliwość przyjęcia proporcjonalnych i uzasadnionych środków, w tym odebrania kwalifikowanego statusu świadczonej usługi zaufania.

(72) Aby zapewnić pewność prawa w odniesieniu do ważności zaawansowanych podpisów elektronicznych opartych na kwalifikowanych certyfikatach, niezbędne jest określenie sposobu oceny przeprowadzanej przez stronę ufającą dokonującą walidacji tego zaawansowanego podpisu elektronicznego opartego na kwalifikowanych certyfikatach.

(73) Dostawcy usług zaufania powinni stosować metody kryptograficzne odzwierciedlające aktualne najlepsze praktyki i wiarygodne przykłady wdrażania tych metod w celu zapewnienia bezpieczeństwa i wiarygodności ich usług zaufania.

(74) Niniejsze rozporządzenie ustanawia dla dostawców kwalifikowanych usług zaufania obowiązek weryfikacji tożsamości osoby fizycznej lub prawnej, której wydawany jest kwalifikowany certyfikat lub kwalifikowane elektroniczne poświadczenie atrybutów, w oparciu o różne zharmonizowane metody w całej Unii. W celu zapewnienia, aby kwalifikowane certyfikaty i kwalifikowane elektroniczne poświadczenia atrybutów były wydawane osobie, do której należą, oraz aby poświadczały prawidłowy i niepowtarzalny zestaw danych odpowiadających tożsamości tej osoby, dostawcy kwalifikowanych usług zaufania wydający kwalifikowane certyfikaty lub wydający kwalifikowane elektroniczne poświadczenia atrybutów powinni, w momencie wydawania tych certyfikatów i poświadczeń, potwierdzić z całkowitą pewnością tożsamość tej osoby. Ponadto oprócz obowiązkowej weryfikacji tożsamości danej osoby, o ile będzie to miało zastosowanie do celów wydawania kwalifikowanych certyfikatów oraz przy wydawaniu kwalifikowanych elektronicznych poświadczeń atrybutów, dostawcy kwalifikowanych usług zaufania powinni z całkowitą pewnością zapewniać prawidłowość i dokładność poświadczanych atrybutów osoby, której wydawane są kwalifikowany certyfikat lub kwalifikowane elektroniczne poświadczenie atrybutów. Te obowiązki dotyczące rezultatu i całkowitej pewności przy weryfikacji poświadczanych danych powinny być poparte odpowiednimi środkami, w tym zastosowaniem jednej konkretnej metody określonej w niniejszym rozporządzeniu lub, w stosownych przypadkach, ich połączenia. Powinno być możliwe łączenie tych metod w celu zapewnienia odpowiedniej podstawy do weryfikacji tożsamości osoby, której wydawane są kwalifikowany certyfikat lub kwalifikowane elektroniczne poświadczenie atrybutów. Powinno być możliwe, aby takie połączenie obejmowało poleganie na środkach identyfikacji elektronicznej, które spełniają wymogi dotyczące średniego poziomu bezpieczeństwa w połączeniu z innymi środkami weryfikacji tożsamości. Taka identyfikacja elektroniczna pozwoliłaby spełnić zharmonizowane wymogi określone w niniejszym rozporządzeniu w odniesieniu do wysokiego poziomu bezpieczeństwa, jako część dodatkowych zharmonizowanych procedur zdalnych, zapewniających dużą dozę pewności co do identyfikacji. Metody te powinny obejmować możliwość dokonania przez dostawcę kwalifikowanych usług zaufania wydającego kwalifikowane elektroniczne poświadczenie atrybutów weryfikacji atrybutów, które mają być poświadczone drogą elektroniczną na żądanie użytkownika oraz zgodnie z prawem Unii lub prawem krajowym, w tym względem źródeł autentycznych.

(75) Aby zachować aktualność niniejszego rozporządzenia względem globalnych zmian oraz przestrzegać najlepszych praktyk na rynku wewnętrznym, akty delegowane i wykonawcze przyjmowane przez Komisję powinny być regularnie poddawane przeglądowi i w razie potrzeby regularnie aktualizowane. Ocena, czy aktualizacje te są konieczne, powinna uwzględniać nowe technologie, praktyki, normy lub specyfikacje techniczne.

(76) Ponieważ cele niniejszego rozporządzenia, a mianowicie opracowanie ogólnounijnych europejskich ram tożsamości cyfrowej oraz ram usługi zaufania, nie mogą zostać osiągnięte w sposób wystarczający przez państwa członkowskie, natomiast ze względu na ich rozmiary i skutki możliwe jest ich lepsze osiągnięcie na poziomie Unii, może ona podjąć działania zgodnie z zasadą pomocniczości określoną w art. 5 Traktatu o Unii Europejskiej. Zgodnie z zasadą proporcjonalności określoną w tym artykule niniejsze rozporządzenie nie wykracza poza to, co jest konieczne do osiągnięcia tych celów.

(77) Zgodnie z art. 42 ust. 1 rozporządzenia (UE) 2018/1725 skonsultowano się z Europejskim Inspektorem Ochrony Danych.

(78) Należy zatem odpowiednio zmienić rozporządzenie (UE) nr 910/2014,

PRZYJMUJĄ NINIEJSZE ROZPORZĄDZENIE:

Artykuł 1

Zmiany w rozporządzeniu (UE) nr 910/2014

W rozporządzeniu (UE) nr 910/2014 wprowadza się następujące zmiany:

1) art. 1 otrzymuje brzmienie:

„*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.";

2) w art. 2 wprowadza się następujące zmiany:

a) ust. 1 otrzymuje brzmienie:

„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) ust. 3 otrzymuje brzmienie:

„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.

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

(*) 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).";

3) w art. 3 wprowadza się następujące zmiany:

a) pkt 1–5 otrzymują brzmienie:

„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;";

b) dodaje się punkt w brzmieniu:

„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;";

c) pkt 6 otrzymuje brzmienie:

„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;";

d) pkt 16 otrzymuje brzmienie:

„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;

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;";

e) pkt 18 otrzymuje brzmienie:

„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;";

f) pkt 21 otrzymuje brzmienie:

„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;";

g) dodaje się punkty w brzmieniu:

„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;

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;";

h) pkt 38 otrzymuje brzmienie:

„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;";

i) pkt 41 otrzymuje brzmienie:

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

j) dodaje się punkty w brzmieniu:

„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;

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.";

4) art. 5 otrzymuje brzmienie:

„*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.";

5) w rozdziale II dodaje się sekcję w brzmieniu:

„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;

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;

(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.

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.

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.

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 (*).

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

(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.

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 (**) 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.

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.

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.

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 (***)– 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 (****), 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.

(*) 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).

(**) 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).

(***) 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).

(****) 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).";

6) przed art. 6 dodaje się nagłówek w brzmieniu:

„SEKCJA 2

SYSTEMY IDENTYFIKACJI ELEKTRONICZNEJ";

7) w art. 7 lit. g) otrzymuje brzmienie:

„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;";

8) art. 8 ust. 3 akapit pierwszy otrzymuje brzmienie:

„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.";

9) art. 9 ust. 2 i 3 otrzymują brzmienie:

„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.";

10) tytuł art. 10 otrzymuje brzmienie:

„Naruszenie bezpieczeństwa systemów identyfikacji elektronicznej";

11) dodaje się artykuł w brzmieniu:

„*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.";

12) w art. 12 wprowadza się następujące zmiany:

a) tytuł otrzymuje brzmienie:

„Interoperacyjność";

b) w ust. 3 wprowadza się następujące zmiany:

(i) lit. c) otrzymuje brzmienie:

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

(ii) uchyla się lit. d);

c) w ust. 4 lit. d) otrzymuje brzmienie:

„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;";

d) ust. 5 i 6 otrzymują brzmienie:

„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.";

e) uchyla się ust. 7;

f) ust. 8 otrzymuje brzmienie:

„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.";

13) w rozdziale II dodaje się artykuły w brzmieniu:

„*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.

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 (*) 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.

(*) 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).";

14) w art. 13 ust. 1 otrzymuje brzmienie:

„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.";

15) art. 14, 15 i 16 otrzymują brzmienie:

„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.

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 (*) 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.

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.

(*) 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).";

16) w rozdziale III tytuł sekcji 2 otrzymuje brzmienie:

„Niekwalifikowani dostawcy usług zaufania";

17) uchyla się art. 17 i 18;

18) w rozdziale III sekcja 2 dodaje się artykuł w brzmieniu:

„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.";

19) w art. 20 wprowadza się następujące zmiany:

a) ust. 1 otrzymuje brzmienie:

„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.";

b) dodaje się ustępy w brzmieniu:

„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.";

c) ust. 2, 3 i 4 otrzymują brzmienie:

„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.

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.";

20) w art. 21 wprowadza się następujące zmiany:

a) ust. 1 i 2 otrzymują brzmienie:

„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.

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) ust. 4 otrzymuje brzmienie:

„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.";

21) w art. 24 wprowadza się następujące zmiany:

a) ust. 1 otrzymuje brzmienie:

„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);

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) w ust. 2 wprowadza się następujące zmiany:

(i) lit. a) otrzymuje brzmienie:

„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;";

(ii) lit. d) i e) otrzymują brzmienie:

„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;";

(iii) dodaje się litery w brzmieniu:

„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;";

(iv) lit. g), h) oraz i) otrzymują brzmienie:

„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;

(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);";

(v) uchyla się lit. j);

(vi) dodaje się akapit w brzmieniu:

„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.";

c) ust. 5 otrzymuje brzmienie:

„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.";

22) w rozdziale III sekcja 3 dodaje się artykuł w brzmieniu:

„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 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.

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

23) w art. 25 uchyla się ust. 3;

24) w art. 26 wprowadza się następujące zmiany:

a) pojedynczy ustęp staje się ust. 1;

b) dodaje się ustęp w brzmieniu:

„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.";

25) w art. 27 uchyla się ust. 4;

26) w art. 28 ust. 6 otrzymuje brzmienie:

„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.";

27) w art. 29 dodaje się ustęp w brzmieniu:

„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.";

28) dodaje się artykuł w brzmieniu:

„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;

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.";

29) w art. 30 dodaje się ustęp w brzmieniu:

„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.";

30) w art. 31 ust. 3 otrzymuje brzmienie:

„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.";

31) w art. 32 wprowadza się następujące zmiany:

a) w ust. 1 dodaje się akapit w brzmieniu:

„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) ust. 3 otrzymuje brzmienie:

„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.";

32) dodaje się artykuł w brzmieniu:

„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.";

33) w art. 33 ust. 2 otrzymuje brzmienie:

„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.";

34) w art. 34 wprowadza się następujące zmiany:

a) dodaje się ustęp w brzmieniu:

„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.";

b) ust. 2 otrzymuje brzmienie:

„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.";

35) w art. 35 uchyla się ust. 3;

36) w art. 36 wprowadza się następujące zmiany:

a) pojedynczy ustęp staje się ust. 1;

b) dodaje się ustęp w brzmieniu:

„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.";

37) w art. 37 uchyla się ust. 4;

38) w art. 38 ust. 6 otrzymuje brzmienie:

„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.";

39) dodaje się artykuł w brzmieniu:

„*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.";

40) w rozdziale III sekcja 5 dodaje się artykuł w brzmieniu:

„*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.";

41) w art. 41 uchyla się ust. 3;

42) w art. 42 wprowadza się następujące zmiany:

a) dodaje się ustęp w brzmieniu:

„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.";

b) ust. 2 otrzymuje brzmienie:

„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.";

43) w art. 44 wprowadza się następujące zmiany:

a) dodaje się ustęp w brzmieniu:

„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.";

b) ust. 2 otrzymuje brzmienie:

„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.";

c) dodaje się ustępy w brzmieniu:

„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.";

44) art. 45 otrzymuje brzmienie:

„*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.";

45) dodaje się artykuł w brzmieniu:

„*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 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.";

46) w rozdziale III dodaje się sekcje w brzmieniu:

„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.

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;

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.

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 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.

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.";

47) dodaje się rozdział w brzmieniu:

„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.

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.

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.

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;

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:

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:

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.

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.";

48) w art. 47 wprowadza się następujące zmiany:

a) ust. 2 i 3 otrzymują brzmienie:

„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) ust. 5 otrzymuje brzmienie:

„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.";

49) w rozdziale VI dodaje się artykuł w brzmieniu:

„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.";

50) art. 49 otrzymuje brzmienie:

„*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, 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.";

51) art. 51 otrzymuje brzmienie:

„*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.";

52) w załącznikach I–IV wprowadza się – odpowiednio – zmiany zgodnie z załącznikami I–IV do niniejszego rozporządzenia;

53) dodaje się nowe załączniki V, VI i VII, jak określono w załącznikach V, VI i VII do niniejszego rozporządzenia.

Artykuł 2

Wejście w życie

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

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

Sporządzono w Brukseli dnia 11 kwietnia 2024 r.

W imieniu Parlamentu Europejskiego	*W imieniu Rady*
Przewodnicząca	*Przewodnicząca*
R. METSOLA	H. LAHBIB

ZAŁĄCZNIK I

W załączniku I do rozporządzenia (UE) nr 910/2014 lit. (i) otrzymuje brzmienie:

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

ZAŁĄCZNIK II

W załączniku II do rozporządzenia (UE) nr 910/2014, uchyla się pkt 3 i 4.

ZAŁĄCZNIK III

W załączniku III do rozporządzenia (UE) nr 910/2014 lit. i) otrzymuje brzmienie:

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

ZAŁĄCZNIK IV

W załączniku IV do rozporządzenia (UE) nr 910/2014 wprowadza się następujące zmiany:

1) lit. c) otrzymuje brzmienie:

„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;";

2) lit. j) otrzymuje brzmienie:

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

ZAŁĄCZNIK V

„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.”.

ZAŁĄCZNIK VI

„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.”.

ZAŁĄCZNIK VII

„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.”.