Rada
Unii Europejskiej

Bruksela, 6 grudnia 2022 r.
(OR. en)

15706/22

Międzyinstytucjonalny numer referencyjny:
2021/0136(COD)

TELECOM 519
COMPET 1006
MI 919
DATAPROTECT 352
JAI 1634
CODEC 1941

WYNIK PRAC

Od:	Sekretariat Generalny Rady
Data:	6 grudnia 2022 r.
Do:	Delegacje
Nr poprz. dok.:	14959/22 + ADD 1 + ADD 2
Nr dok. Kom.:	9471/21
Dotyczy:	Wniosek dotyczący rozporządzenia Parlamentu Europejskiego i Rady zmieniającego rozporządzenie (UE) nr 910/2014 w odniesieniu do ustanowienia europejskich ram tożsamości cyfrowej – Podejście ogólne (6 grudnia 2022 r.)

Delegacje otrzymują w załączeniu podejście ogólne Rady w sprawie wyżej wymienionego wniosku w wersji zatwierdzonej przez Radę (ds. Transportu, Telekomunikacji i Energii) na jej 3917. posiedzeniu w dniu 6 grudnia 2022 r.

Podejście ogólne określa wstępne stanowisko Rady w sprawie tego wniosku i stanowi podstawę przygotowań do negocjacji z Parlamentem Europejskim.

ZAŁĄCZNIK

Wniosek

ROZPORZĄDZENIE PARLAMENTU EUROPEJSKIEGO I RADY

zmieniające rozporządzenie (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],

stanowiąc zgodnie ze zwykłą procedurą ustawodawczą,

a także mając na uwadze, co następuje:

(1) W komunikacie Komisji z dnia 19 lutego 2020 r. pt. „Kształtowanie cyfrowej przyszłości Europy”[2] zapowiedziano przegląd rozporządzenia Parlamentu Europejskiego i Rady (UE) nr 910/2014 w celu zwiększenia jego skuteczności, zwiększenia korzyści dla sektora prywatnego i promowania zaufanych tożsamości cyfrowych dla wszystkich Europejczyków.

[1] Dz.U. C […] z […], s. […].
[2] COM(2020) 67 final.

(2) W konkluzjach z 1–2 października 2020 r.[3] Rada Europejska zaapelowała do Komisji o przedstawienie wniosku w sprawie opracowania ogólnounijnych ram bezpiecznej publicznej identyfikacji elektronicznej, w tym interoperacyjnych podpisów cyfrowych, by zapewnić obywatelom kontrolę nad ich tożsamością i danymi w internecie, a także by umożliwić dostęp do publicznych, prywatnych i transgranicznych usług cyfrowych.

(3) W komunikacie Komisji z dnia 9 marca 2021 r. pt. „Cyfrowy kompas na 2030 r.: europejska droga w cyfrowej dekadzie”[4] wyznaczono cel ram Unii, zgodnie z którym do 2030 r. powinny one zapewnić wprowadzenie na szeroką skalę zaufanej, kontrolowanej przez użytkownika tożsamości, dzięki której każdy użytkownik będzie mógł kontrolować swoje kontakty i obecność online.

(4) Bardziej zharmonizowane podejście do identyfikacji cyfrowej powinno ograniczyć ryzyko i koszty wynikające z obecnej fragmentacji, która spowodowana jest stosowaniem rozbieżnych rozwiązań krajowych, oraz wzmocni jednolity rynek poprzez umożliwienie obywatelom, innym rezydentom określonym w prawie krajowym i przedsiębiorstwom identyfikacji online w dogodny i jednolity sposób w całej Unii. Europejski portfel tożsamości cyfrowej zapewni osobom fizycznym i prawnym w całej Unii zharmonizowany środek identyfikacji elektronicznej, który umożliwi im uwierzytelnianie i wymianę danych związanych z ich tożsamością. Każdy powinien mieć możliwość bezpiecznego dostępu do usług publicznych i prywatnych za pomocą ulepszonego ekosystemu usług zaufania oraz zweryfikowanych dowodów potwierdzających tożsamość i poświadczeń atrybutów takich jak dyplom ukończenia studiów wyższych prawnie uznawany i akceptowany w całej Unii. Ramy europejskiej tożsamości cyfrowej mają na celu przejście od polegania wyłącznie na krajowych rozwiązaniach w zakresie tożsamości cyfrowej do dostarczania elektronicznych poświadczeń atrybutów ważnych na szczeblu europejskim. Dostawcy elektronicznych poświadczeń atrybutów powinni odnieść korzyści dzięki jasnemu i jednolitemu zestawowi przepisów, a administracje publiczne powinny mieć możliwość polegania na dokumentach elektronicznych w określonym formacie.

---

[3] https://www.consilium.europa.eu/pl/press/press-releases/2020/10/02/european-council-conclusions-1-2-october-2020/

[4] COM(2021)118 final/2.

(4a) Kilka państw członkowskich wdrożyło i w dużej mierze stosuje środki identyfikacji elektronicznej, które obecnie są akceptowane przez dostawców usług w Unii. Ponadto dokonano inwestycji zarówno w rozwiązania krajowe, jak i transgraniczne oparte na obecnym rozporządzeniu eIDAS, w tym w infrastrukturę techniczną interoperacyjności węzłów eIDAS. Aby zagwarantować komplementarność i szybkie przyjęcie europejskich portfeli tożsamości cyfrowej przez obecnych użytkowników notyfikowanych środków identyfikacji elektronicznej oraz zminimalizować skutki dla 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 wdrożona infrastruktura eIDAS na szczeblu europejskim i krajowym.

(5) Aby wspierać konkurencyjność europejskich przedsiębiorstw, dostawcy usług online 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 europejskiego 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 UE.

(6) W ramach wdrażania niniejszego rozporządzenia do przetwarzania danych osobowych ma zastosowanie rozporządzenie (UE) 2016/679[5]. W związku z tym w niniejszym rozporządzeniu należy ustanowić określone zabezpieczenia uniemożliwiające dostawcom środków identyfikacji elektronicznej i elektronicznego poświadczenia atrybutów łączenie danych osobowych pochodzących z innych usług z danymi osobowymi dotyczącymi usług objętych zakresem stosowania niniejszego rozporządzenia. Dane osobowe związane z udostępnianiem europejskich portfeli tożsamości cyfrowej powinny być logicznie oddzielone od wszelkich innych danych będących w posiadaniu wydawcy. Niniejsze rozporządzenie nie uniemożliwia wydawcom europejskich portfeli tożsamości cyfrowej stosowania dodatkowych środków technicznych przyczyniających się do ochrony danych osobowych, takich jak fizyczne oddzielenie danych osobowych związanych z zapewnianiem portfeli od wszelkich innych danych będących w posiadaniu wydawcy.

---

[5] 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.

(7) Konieczne jest określenie zharmonizowanych warunków na potrzeby ustanowienia ram europejskich portfeli tożsamości cyfrowej zapewnianych przez państwa członkowskie, które to ramy powinny uprawniać wszystkich obywateli Unii i innych rezydentów określonych w prawie krajowym do bezpiecznej wymiany danych związanych z ich tożsamością w sposób przyjazny dla użytkownika i dogodny oraz pod wyłączną kontrolą użytkownika. Należy rozwijać technologie wykorzystywane do osiągnięcia tych celów, dążąc do zapewnienia najwyższego poziomu bezpieczeństwa, prywatności, wygody użytkowników i szerokiej używalności. Państwa członkowskie powinny zapewnić równy dostęp do identyfikacji cyfrowej wszystkim swoim obywatelom i rezydentom.

(8) W celu zapewnienia, aby strony ufające mogły polegać na korzystaniu z europejskich portfeli tożsamości cyfrowej, oraz w celu ochrony użytkownika przed bezprawnym wykorzystaniem danych wrażliwych, strony ufające powinny być rejestrowane w ramach procesu zgłaszania. Wymogi dotyczące zgłaszania mające zastosowanie do stron ufających powinny w większości przypadków opierać się na dostarczaniu ograniczonej ilości informacji wymaganych do uwierzytelniania strony ufającej w odniesieniu do europejskiego portfela tożsamości cyfrowej. Wymogi te powinny również umożliwiać stosowanie zautomatyzowanych lub prostych procedur samodzielnego raportowania, w tym poleganie na istniejących rejestrach i korzystanie z nich przez państwa członkowskie. Jednocześnie w odniesieniu do kategorii danych wrażliwych na szczeblu krajowym lub unijnym mogą istnieć szczególne systemy, które mogą nakładać na strony ufające bardziej rygorystyczne wymogi dotyczące rejestrowania i zezwoleń w celu zapobiegania bezprawnemu wykorzystywaniu danych dotyczących tożsamości w takich przypadkach. W innych przypadkach użycia strony ufające mogą być zwolnione z obowiązku zgłoszenia zamiaru polegania na europejskim portfelu cyfrowym, na przykład gdy prawo do weryfikacji specjalnych atrybutów nie wymaga uwierzytelnienia strony ufającej za pomocą środków elektronicznych ani na takie uwierzytelnianie nie pozwala. Zazwyczaj w tych scenariuszach, które obejmują kontakty osobiste, użytkownik jest w stanie zidentyfikować stronę ufającą dzięki kontekstowi, np. w kontaktach z pracownikiem biura wynajmu samochodów lub farmaceutą. Proces zgłaszania ma opierać się na unijnych lub krajowych przepisach sektorowych, ponieważ umożliwia to uwzględnienie różnych przypadków użycia, które mogą różnić się pod względem wymogów rejestracyjnych, trybu działania (online/offline) lub wymogu uwierzytelniania urządzeń zdolnych do połączenia z europejskim portfelem tożsamości cyfrowej. Na poziomie europejskiego portfela tożsamości cyfrowej nie należy nakazywać egzekwowania weryfikacji użycia przez strony ufające europejskiego portfela tożsamości cyfrowej.

(9) Wszystkie europejskie portfele tożsamości cyfrowej powinny umożliwiać użytkownikom elektroniczną identyfikację i uwierzytelnianie online i 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, portfele mogą również zaspokajać potrzeby instytucjonalne administracji publicznych, organizacji międzynarodowych oraz instytucji, organów i jednostek organizacyjnych Unii. Korzystanie z portfeli 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 opartych na „wysokim" poziomie bezpieczeństwa europejskich portfelach tożsamości cyfrowej należy wykorzystać potencjał, jaki oferują rozwiązania odporne na ingerencję, takie jak zabezpieczenia, by zapewnić zgodność z wymogami bezpieczeństwa określonymi w niniejszym rozporządzeniu. Europejskie portfele tożsamości cyfrowej powinny również umożliwiać użytkownikom tworzenie i używanie kwalifikowanych podpisów i pieczęci elektronicznych akceptowanych w całej UE. Aby zapewnić obywatelom i przedsiębiorstwom w całej UE korzyści w zakresie uproszczenia przepisów i zmniejszenia kosztów, w tym poprzez umożliwienie korzystania z uprawnień do reprezentowania i zgód elektronicznych, państwa członkowskie powinny wydawać europejskie portfele tożsamości cyfrowej oparte na wspólnych normach, aby zapewnić niezakłóconą interoperacyjność i wysoki poziom bezpieczeństwa. Wyłącznie właściwe organy państw członkowskich mogą zapewnić wysoki stopień pewności przy ustalaniu tożsamości danej osoby, gwarantując tym samym, że osoba podająca daną tożsamość jest faktycznie osobą, za którą się podaje. Europejskie portfele tożsamości cyfrowej muszą być zatem oparte na tożsamości prawnej obywateli, innych rezydentów lub podmiotów prawnych. Zaufanie do europejskich portfeli tożsamości cyfrowej ulegnie zwiększeniu ze względu na fakt, że podmioty je wydające są zobowiązane do wdrożenia odpowiednich środków technicznych i organizacyjnych w celu zapewnienia poziomu bezpieczeństwa współmiernego do stwarzanego ryzyka dla praw i wolności osób fizycznych zgodnie z rozporządzeniem (UE) 2016/679. Wydawanie, używanie w celu uwierzytelnienia i unieważnianie europejskich portfeli tożsamości cyfrowej powinno być nieodpłatne w przypadku osób fizycznych. Usługi oparte na użyciu portfela mogą pociągać za sobą koszty związane na przykład z wydawaniem elektronicznych poświadczeń atrybutów do portfela.

(9a) Korzystne jest ułatwienie upowszechnienia i wykorzystywania europejskich portfeli tożsamości cyfrowej poprzez płynne zintegrowanie ich z już wdrożonym na szczeblu krajowym, lokalnym lub regionalnym ekosystemem publicznych i prywatnych usług cyfrowych. Z myślą o osiągnięciu tego celu państwa członkowskie mogą przewidzieć środki prawne i organizacyjne, aby zwiększyć elastyczność dla wydawców europejskich portfeli tożsamości cyfrowej i umożliwić dodatkowe funkcje europejskich portfeli tożsamości cyfrowej wykraczające poza to, co określono w niniejszym rozporządzeniu, w tym poprzez zwiększoną interoperacyjność z istniejącymi krajowymi środkami identyfikacji elektronicznej. Nie powinno to w żadnym wypadku odbywać się ze szkodą dla zapewnienia podstawowych funkcji europejskich portfeli tożsamości cyfrowej określonych w niniejszym rozporządzeniu ani promowania istniejących rozwiązań krajowych jako alternatywy dla europejskich portfeli tożsamości cyfrowej. Ponieważ te dodatkowe funkcje wykraczają poza zakres niniejszego rozporządzenia, nie podlegają one określonym w niniejszym rozporządzeniu przepisom dotyczącym transgranicznego korzystania z europejskich portfeli tożsamości cyfrowej.

(10) Aby osiągnąć wysoki poziom ochrony, bezpieczeństwa i wiarygodności danych, w niniejszym rozporządzeniu należy ustanowić zharmonizowane ramy szczegółowo określające wspólne specyfikacje i wymogi mające zastosowanie do europejskich portfeli tożsamości cyfrowej. Zgodność europejskich portfeli tożsamości cyfrowej z tymi wymogami powinna być certyfikowana przez akredytowane jednostki oceniające zgodność wyznaczone przez państwa członkowskie. Certyfikacja powinna opierać się w szczególności na odpowiednich europejskich programach certyfikacji cyberbezpieczeństwa lub ich częściach, ustanowionych na podstawie rozporządzenia (UE) 2019/881[6], o ile obejmują one wymogi w zakresie cyberbezpieczeństwa mające zastosowanie do europejskich portfeli tożsamości cyfrowej. Opieranie się na europejskich programach certyfikacji cyberbezpieczeństwa powinno zapewnić zharmonizowany poziom zaufania do bezpieczeństwa europejskich portfeli tożsamości cyfrowej, niezależnie od tego, gdzie w Unii są one wydawane. Certyfikacja cyberbezpieczeństwa europejskich portfeli tożsamości cyfrowej powinna opierać się na roli krajowych organów ds. certyfikacji cyberbezpieczeństwa w nadzorowaniu i monitorowaniu zgodności certyfikatów wydawanych przez jednostki oceniające zgodność w ich jurysdykcji z odpowiednimi europejskimi programami cyberbezpieczeństwa. Podobnie certyfikacja powinna w stosownych przypadkach opierać się na normach i specyfikacjach technicznych określonych w rozporządzeniu (UE) 2019/881. Takie specyfikacje mogą być wykorzystywane jako dokumenty odzwierciedlające stan wiedzy, jak określono w odpowiednich programach certyfikacji cyberbezpieczeństwa na podstawie rozporządzenia (UE) 2019/881. W przypadku gdy żadne odpowiednie europejskie programy certyfikacji cyberbezpieczeństwa ustanowione na podstawie rozporządzenia (UE) 2019/881 nie obejmują certyfikacji odpowiednich usług lub procesów przyczyniających się do bezpieczeństwa portfela, należy ustanowić odpowiednie programy zgodnie z tytułem III rozporządzenia (UE) 2019/881. Należy ustanowić wspólny i zharmonizowany program certyfikacji europejskich portfeli tożsamości cyfrowej w celu oceny ich zgodności ze wspólnymi specyfikacjami i wymogami przewidzianymi w niniejszym rozporządzeniu, innymi niż te związane z cyberbezpieczeństwem i ochroną danych, w szczególności tymi dotyczącymi aspektów funkcjonalnych i operacyjnych. W odniesieniu do tej certyfikacji, aby zapewnić wysoki poziom zaufania i przejrzystości, należy ustanowić mechanizmy i procedury mające na celu wspieranie wzajemnego uczenia się i współpracy między państwami członkowskimi w zakresie monitorowania i kontroli organów ds. certyfikacji oraz wydawanych przez nie certyfikatów i sprawozdań z certyfikacji. Taki mechanizm wzajemnego uczenia się powinien pozostawać bez uszczerbku dla rozporządzenia (WE) 2016/679 i rozporządzenia (UE) 2019/881. Certyfikacja portfela na podstawie rozporządzenia (WE) 2016/679 jest jednym z dobrowolnych narzędzi, które można wykorzystać do wykazania zgodności z wymogami określonymi w rozporządzeniu (WE) 2016/679 w zakresie, w jakim mają one zastosowanie do europejskich portfeli tożsamości cyfrowej i ich udostępniania obywatelom Unii.

---

[6] 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.

(10a) Należy ułatwić onboarding obywateli i rezydentów do europejskiego portfela tożsamości cyfrowej poprzez poleganie na środkach identyfikacji elektronicznej wydawanych na „wysokim” poziomie bezpieczeństwa. Na środkach identyfikacji elektronicznej wydanych na „istotnym” poziomie bezpieczeństwa należy polegać wyłącznie w przypadkach, gdy zharmonizowane specyfikacje techniczne i operacyjne wykorzystujące środki identyfikacji elektronicznej wydane na „istotnym” poziomie bezpieczeństwa w połączeniu z innymi uzupełniającymi środkami weryfikacji tożsamości umożliwią spełnienie wymogów określonych w niniejszym rozporządzeniu w odniesieniu do „wysokiego” poziomu bezpieczeństwa. Takie dodatkowe środki powinny być niezawodne i łatwe do wykorzystania przez użytkowników i mogłyby opierać się na możliwości korzystania z procedur onboardingu na odległość, kwalifikowanych certyfikatów popartych kwalifikowanym podpisem, kwalifikowanym elektronicznym poświadczeniem atrybutów lub ich połączeniem. Aby zapewnić wystarczające upowszechnienie europejskich portfeli tożsamości cyfrowej, w aktach wykonawczych należy określić zharmonizowane specyfikacje techniczne i operacyjne dotyczące onboardingu użytkowników przy użyciu środków identyfikacji elektronicznej, w tym specyfikacje wydane na „istotnym” poziomie bezpieczeństwa.

(10b) Celem niniejszego rozporządzenia jest zapewnienie użytkownikowi w pełni mobilnego, bezpiecznego i łatwego w obsłudze europejskiego portfela tożsamości cyfrowej. Jako środek przejściowy do czasu dostępności certyfikowanych rozwiązań odpornych na ingerencję, takich jak zabezpieczenia w urządzeniach użytkowników, europejskie portfele tożsamości cyfrowej mogą opierać się na certyfikowanych zewnętrznych zabezpieczeniach w celu ochrony materiału kryptograficznego i innych danych wrażliwych lub na notyfikowanych rozwiązaniach krajowych na „wysokim” poziomie bezpieczeństwa w celu wykazania zgodności z odpowiednimi wymogami rozporządzenia w odniesieniu do poziomu bezpieczeństwa portfela. Stosowanie wyżej wymienionego środka przejściowego powinno być ograniczone do przypadków użycia wymagających „wysokiego” poziomu bezpieczeństwa, takich jak onboarding użytkownika do portfela i uwierzytelnienie na potrzeby usług wymagających „wysokiego” poziomu bezpieczeństwa. Przy uwierzytelnianiu na potrzeby usług wymagających „istotnego” poziomu bezpieczeństwa europejskie portfele tożsamości cyfrowej nie powinny wymagać stosowania wyżej wymienionego środka przejściowego. Niniejsze rozporządzenie powinno pozostawać bez uszczerbku dla krajowych warunków wydawania i stosowania certyfikowanego zewnętrznego zabezpieczenia, w przypadku gdy ten środek przejściowy opiera się na nim.

(11) Europejskie portfele tożsamości cyfrowej powinny zapewniać najwyższy poziom ochrony i bezpieczeństwa danych osobowych wykorzystywanych do uwierzytelniania niezależnie od tego, czy dane takie są przechowywane lokalnie, czy przy użyciu rozwiązań opartych na chmurze, z uwzględnieniem różnych poziomów ryzyka. Przetwarzanie danych biometrycznych jako czynnika uwierzytelniania w silnym uwierzytelnianiu użytkownika jest jedną z metod identyfikacji zapewniających wysoki poziom pewności, zwłaszcza w połączeniu z innymi elementami uwierzytelniania. Ponieważ dane biometryczne dotyczą unikalnych cech danej osoby, przetwarzanie tych danych jest dozwolone wyłącznie na podstawie wyjątków określonych w art. 9 ust. 2 rozporządzenia (UE) 2016/679 i wymaga odpowiednich zabezpieczeń, współmiernych do ryzyka, jakie takie przetwarzanie może stwarzać dla praw i wolności osób fizycznych.

(11a) Funkcjonowanie europejskich portfeli tożsamości cyfrowej powinno być przejrzyste i umożliwiać weryfikowalne przetwarzanie danych osobowych. W tym celu zachęca się państwa członkowskie do ujawniania kodu źródłowego komponentów oprogramowania europejskich portfeli tożsamości cyfrowej, które są związane z przetwarzaniem danych osobowych i danych osób prawnych. Ujawnienie takiego kodu źródłowego umożliwia społeczeństwu, w tym użytkownikom i programistom, zrozumienie jego funkcjonowania. Może to również zwiększyć zaufanie użytkowników do ekosystemu portfela i – poprzez umożliwienie każdemu zgłaszania słabych punktów i błędów w kodzie – przyczynić się do zwiększenia bezpieczeństwa portfeli. Skłania to dostawców do dostarczania i utrzymywania wysoce bezpiecznego produktu. Ponadto, w stosownych przypadkach, zachęca się również państwa członkowskie do udostępniania kodu źródłowego na podstawie licencji otwartego oprogramowania. Licencja otwartego oprogramowania umożliwia społeczeństwu, w tym użytkownikom i programistom, modyfikowanie i ponowne wykorzystywanie kodu źródłowego.

(12) Aby zapewnić otwartość europejskich ram tożsamości cyfrowej na innowacje i rozwój technologiczny oraz aby ramy te wytrzymywały próbę czasu, należy zachęcać państwa członkowskie do wspólnego tworzenia piaskownic do testowania innowacyjnych rozwiązań w kontrolowanym i bezpiecznym środowisku, w szczególności w celu poprawy funkcjonalności, ochrony danych osobowych, bezpieczeństwa i interoperacyjności tych rozwiązań oraz w celu uzyskiwania informacji na potrzeby przyszłych aktualizacji technicznych dokumentów referencyjnych i wymogów prawnych. Środowisko to powinno sprzyjać włączeniu europejskich małych i średnich przedsiębiorstw, przedsiębiorstw typu start-up oraz innowatorów i badaczy indywidualnych.

(13) Rozporządzenie (UE) 2019/1157[7] zwiększa bezpieczeństwo dowodów osobistych z ulepszonymi zabezpieczeniami do sierpnia 2021 r. Państwa członkowskie powinny rozważyć możliwość notyfikowania tych dowodów w ramach systemów identyfikacji elektronicznej, aby zwiększyć transgraniczną dostępność środków identyfikacji elektronicznej.

(14) 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 tożsamości do oferowania organom państw członkowskich systemów identyfikacji elektronicznej do notyfikacji jako krajowe systemy identyfikacji elektronicznej na podstawie rozporządzenia (UE) nr 910/2014.

(15) Usprawnienie obecnych procedur notyfikacji i wzajemnej oceny zapobiegnie niejednorodnemu podejściu do oceny różnych notyfikowanych systemów identyfikacji elektronicznej i ułatwi budowanie zaufania między państwami członkowskimi. Nowe, uproszczone mechanizmy powinny sprzyjać współpracy państw członkowskich w zakresie bezpieczeństwa i interoperacyjności notyfikowanych systemów identyfikacji elektronicznej.

(16) Państwa członkowskie powinny odnieść korzyści dzięki nowym, elastycznym narzędziom służącym do zapewniania zgodności z wymogami niniejszego rozporządzenia i odpowiednich aktów wykonawczych. Niniejsze rozporządzenie powinno umożliwiać państwom członkowskim korzystanie ze sprawozdań i ocen sporządzonych przez akredytowane jednostki oceniające zgodność, jak przewidywać będą programy certyfikacji, które mają zostać ustanowione na szczeblu Unii na podstawie rozporządzenia (UE) 2019/881, do celów poparcia twierdzeń dotyczących dostosowania programów lub ich części do wymogów rozporządzenia w zakresie interoperacyjności i bezpieczeństwa notyfikowanych systemów identyfikacji elektronicznej.

---

[7] 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).

(17a) Stosowanie unikalnych i trwałych identyfikatorów wydanych przez państwa członkowskie lub wygenerowanych przez europejski portfel tożsamości cyfrowej, wraz z wykorzystaniem danych identyfikujących osobę, ma zasadnicze znaczenie dla zapewnienia możliwości weryfikacji tożsamości użytkownika, w szczególności w sektorze publicznym i gdy jest to wymagane na mocy prawa krajowego lub unijnego. Niniejsze rozporządzenie powinno zapewnić, aby w ramach europejskiego portfela tożsamości cyfrowej możliwe było zapewnienie mechanizmu umożliwiającego dopasowywanie rekordów, w tym poprzez stosowanie kwalifikowanych elektronicznych poświadczeń atrybutów, oraz włączenie unikalnych i trwałych identyfikatorów do zbioru danych identyfikujących osobę. Unikalny i trwały identyfikator może składać się z pojedynczych albo wielu danych identyfikacyjnych, które mogą być specyficzne dla danego sektora, o ile służą jednoznacznej identyfikacji użytkownika w całej Unii. W europejskim portfelu tożsamości cyfrowej należy również przewidzieć mechanizm umożliwiający korzystanie z identyfikatorów specyficznych dla danej strony ufającej w przypadkach, gdy stosowanie unikalnego i trwałego identyfikatora jest wymagane na mocy prawa krajowego lub unijnego. We wszystkich przypadkach mechanizm zapewniony z myślą o ułatwieniu dopasowywania rekordów i stosowania unikalnych i trwałych identyfikatorów powinien zapewniać użytkownikowi ochronę przed niewłaściwym wykorzystaniem danych osobowych, zgodnie z niniejszym rozporządzeniem i mającym zastosowanie prawem Unii, w szczególności rozporządzeniem (UE) 2016/679, w tym przed ryzykiem profilowania i śledzenia związanym z korzystaniem z europejskiego portfela tożsamości cyfrowej.

(17aa) Konieczne jest uwzględnienie potrzeb użytkowników, a tym samym zwiększenie popytu na europejskie portfele tożsamości cyfrowej. Dostępne powinny być miarodajne przypadki użycia i usługi online polegające na europejskich portfelach tożsamości cyfrowej. Dla wygody użytkowników oraz aby zapewnić transgraniczną dostępność takich usług, ważne jest podjęcie działań w celu ułatwienia podobnego podejścia do projektowania, rozwijania i wdrażania usług online we wszystkich państwach członkowskich. Niewiążące wytyczne dotyczące sposobu projektowania, rozwijania i wdrażania usług online polegających na europejskich portfelach tożsamości cyfrowej mogą stać się użytecznym narzędziem umożliwiającym osiągnięcie tego celu. Wytyczne te należy przygotować z należytym uwzględnieniem unijnych ram interoperacyjności. Państwa członkowskie powinny odgrywać wiodącą rolę w ich przyjmowaniu.

(18) Zgodnie z dyrektywą (UE) 2019/882[8] osoby z niepełnosprawnościami powinny mieć możliwość korzystania z europejskich portfeli tożsamości cyfrowej, usług zaufania i produktów przeznaczonych dla użytkownika końcowego stosowanych do świadczenia tych usług na równi z innymi użytkownikami.

(19) Niniejsze rozporządzenie nie powinno obejmować aspektów związanych z zawieraniem i ważnością umów lub innych zobowiązań prawnych, w przypadku gdy istnieją wymogi dotyczące formy wprowadzone na mocy prawa krajowego lub unijnego. Dodatkowo nie powinno ono mieć wpływu na krajowe wymogi w zakresie formy dotyczące rejestrów publicznych, w szczególności rejestrów handlowych i rejestrów gruntów.

(20) Świadczenie usług zaufania i korzystanie z nich staje się coraz ważniejsze dla handlu międzynarodowego i współpracy międzynarodowej. Partnerzy międzynarodowi UE tworzą ramy zaufania oparte na rozporządzeniu (UE) nr 910/2014. Aby w związku z tym ułatwić uznawanie takich usług i ich dostawców, w przepisach wykonawczych można określić 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, jako uzupełnienie możliwości wzajemnego uznawania usług zaufania i dostawców tych usług mających siedzibę w Unii i w państwach trzecich zgodnie z art. 218 Traktatu. Określając w niniejszym rozporządzeniu warunki, na jakich ramy zaufania państw trzecich można uznać za równoważne ramom zaufania dotyczącym kwalifikowanych usług zaufania i kwalifikowanych dostawców tych usług, należy również zapewnić zgodność z odpowiednimi przepisami dyrektywy XXXX/XXXX, (dyrektywy NIS2) i rozporządzenia (UE) 2016/679, a także wykorzystanie zaufanych list jako istotnych elementów budowania zaufania.

---

[8] 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).

(21) Niniejsze rozporządzenie powinno opierać się na aktach Unii zapewniających kontestowalne i uczciwe rynki w sektorze cyfrowym. Jest ono oparte w szczególności na rozporządzeniu (UE) 2022/1925, w którym wprowadza się przepisy dotyczące dostawców podstawowych usług platformowych wyznaczonych jako strażnicy dostępu, a także m.in. zakazuje się strażnikom dostępu nakładania na użytkowników biznesowych obowiązku korzystania z usługi identyfikacyjnej świadczonej przez strażnika dostępu w kontekście usług oferowanych przez użytkowników biznesowych za pośrednictwem podstawowych usług platformowych tego strażnika dostępu, jak również obowiązku oferowania takiej usługi identyfikacyjnej lub współdziałania z taką usługą. W art. 6 ust. 7 rozporządzenia (UE) 2022/1925 zobowiązuje się strażników dostępu, aby zapewniali użytkownikom biznesowym i dostawcom usług pomocniczych dostęp do tego samego systemu operacyjnego, funkcji sprzętu lub oprogramowania, które są dostępne dla strażnika dostępu lub wykorzystywane przez niego do świadczenia dowolnych usług pomocniczych, oraz umożliwiali interoperacyjność z tym samym systemem operacyjnym oraz tymi samymi funkcjami sprzętu lub oprogramowania. Zgodnie z art. 2 pkt 19 aktu o rynkach cyfrowych usługi identyfikacyjne stanowią rodzaj usług pomocniczych. Użytkownicy biznesowi i dostawcy usług pomocniczych powinni zatem mieć możliwość dostępu do takich funkcji sprzętu lub oprogramowania, np. zabezpieczeń smartfonów, oraz współdziałać z nimi za pośrednictwem europejskich portfeli tożsamości cyfrowej lub notyfikowanych przez państwa członkowskie środków identyfikacji elektronicznej.

(22) Aby uprościć obowiązki 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) XXXX/XXXX (dyrektywą NIS 2), dostawcy usług zaufania są zobowiązani do wprowadzenia odpowiednich środków technicznych i organizacyjnych na podstawie dyrektywy (UE) XXXX/XXXX (dyrektywy NIS 2), takich jak środki służące przeciwdziałaniu awariom systemu, błędom ludzkim, szkodliwym działaniom lub zjawiskom naturalnym w celu zarządzania ryzykiem stwarzanym dla bezpieczeństwa sieci i systemów informatycznych, z których dostawcy ci korzystają przy świadczeniu swoich usług, a także w celu zgłaszania znaczących incydentów i zagrożeń dla cyberbezpieczeństwa zgodnie z dyrektywą (UE) XXXX/XXXX (dyrektywą NIS 2). Jeżeli chodzi o zgłaszanie incydentów, dostawcy usług zaufania powinni zgłaszać wszelkie incydenty mające znaczący wpływ na świadczenie ich usług, w tym incydenty spowodowane kradzieżą lub utratą urządzeń, uszkodzeniami kabla sieciowego lub incydenty występujące w kontekście identyfikacji osób. Wymogi w zakresie zarządzania ryzykiem w cyberprzestrzeni i obowiązki w zakresie zgłaszania incydentów określone w dyrektywie (UE) XXXX/XXXX [dyrektywie NIS 2] należy uznać za uzupełniające w stosunku do wymogów nałożonych niniejszym rozporządzeniem na dostawców usług zaufania. W stosownych przypadkach właściwe organy wyznaczone na podstawie dyrektywy (UE) XXXX/XXXX (dyrektywy NIS 2) powinny nadal stosować ustalone praktyki krajowe lub wytyczne dotyczące wdrażania wymogów w zakresie bezpieczeństwa i sprawozdawczości oraz nadzoru nad zgodnością z takimi wymogami na podstawie rozporządzenia (UE) nr 910/2014. Żadne wymogi wynikające z niniejszego rozporządzenia nie mają wpływu na obowiązek zawiadamiania o naruszeniach ochrony danych osobowych wynikający z rozporządzenia (UE) 2016/679.

(23) Należy zwrócić należytą uwagę na zapewnienie skutecznej współpracy między organami ds. bezpieczeństwa sieci i informacji a organami ds. eIDAS. W przypadkach, w których organ nadzoru na podstawie niniejszego rozporządzenia jest inny niż właściwe organy wyznaczone na podstawie dyrektywy (UE) XXXX/XXXX [dyrektywy NIS 2], organy te powinny ściśle i terminowo współpracować poprzez wymianę odpowiednich informacji, aby zapewnić skuteczny nadzór nad dostawcami usług zaufania i przestrzegania przez tych dostawców wymogów określonych w niniejszym rozporządzeniu i dyrektywie (UE) XXXX/XXXX [dyrektywie NIS 2]. Organy nadzoru określone w niniejszym rozporządzeniu powinny być w szczególności uprawnione do zwracania się do właściwego organu określonego w dyrektywie (UE) XXXXX/XXXX [dyrektywie NIS 2] 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 NIS 2 lub zażądania od tych dostawców, by zaradzili niezgodności.

(24) Istotne jest ustanowienie ram prawnych służących ułatwieniu transgranicznego uznawania między istniejącymi krajowymi systemami prawnymi, związanego z usługami rejestrowanego doręczenia elektronicznego. Ramy te mogłyby stworzyć także nowe możliwości rynkowe dla unijnych dostawców usług zaufania w odniesieniu do oferowania nowych ogólnoeuropejskich 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 wystarczyłby wysoki poziom 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 przekazywania rejestrowanych elektronicznie danych między co najmniej dwoma kwalifikowanymi dostawcami usług zaufania oraz promowania uczciwych praktyk na rynku wewnętrznym.

(25) W większości przypadków obywatele i inni rezydenci nie mogą – w sposób bezpieczny i z zapewnieniem wysokiego stopnia ochrony danych – prowadzić transgranicznej cyfrowej wymiany informacji związanych z tożsamością, takich jak: adresy, wiek i kwalifikacje zawodowe, prawa jazdy i inne zezwolenia oraz dane dotyczące płatności.

(26) Powinna istnieć możliwość wydawania i obsługi wiarygodnych atrybutów cyfrowych oraz przyczynienia się do zmniejszenia obciążenia administracyjnego dzięki umożliwieniu obywatelom i innym rezydentom korzystania z tych atrybutów w transakcjach prywatnych i publicznych. Obywatele i inni rezydenci 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 danych uwierzytelniających dotyczących zabezpieczenia społecznego lub z przyszłych cyfrowych dokumentów podróży w kontekście transgranicznym.

(27) Każdy podmiot, który gromadzi, tworzy i wydaje poświadczone atrybuty, takie jak: dyplomy, licencje, akty urodzenia, powinien móc stać się dostawcą elektronicznego poświadczenia atrybutów. Strony ufające powinny korzystać z elektronicznych poświadczeń atrybutów jako równoważnych poświadczeniom w formie papierowej. W związku z tym nie należy kwestionować skutku prawnego elektronicznego poświadczenia atrybutów z tego powodu, że poświadczenie to ma postać elektroniczną lub że nie spełnia wymogów kwalifikowanego elektronicznego poświadczenia atrybutów. W związku z tym należy ustanowić ogólne wymogi w celu zapewnienia, aby kwalifikowane elektroniczne poświadczenie atrybutów miało skutek prawny równoważny skutkowi prawnemu legalnie wystawionych 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 mającej podstawowe skutki prawne, a w szczególności do transgranicznego uznawania kwalifikowanego elektronicznego poświadczenia atrybutów w stosownych przypadkach.

(28) Do szerokiej dostępności i używalności europejskich portfeli tożsamości cyfrowej wymagana jest ich akceptacja przez prywatnych dostawców usług. Prywatne strony ufające świadczące usługi w obszarach transportu, energetyki, bankowości, usług finansowych, zabezpieczenia społecznego, zdrowia, wody pitnej, usług pocztowych, infrastruktury cyfrowej, edukacji lub telekomunikacji powinny akceptować korzystanie z europejskich portfeli tożsamości cyfrowej na potrzeby świadczenia usług, w przypadku gdy silne uwierzytelnienie użytkownika jest wymagane na mocy prawa krajowego lub unijnego lub na podstawie zobowiązania umownego. Aby ułatwić korzystanie z europejskiego portfela tożsamości cyfrowej i jego akceptację, należy uwzględnić powszechnie akceptowane normy i specyfikacje branżowe. W przypadku gdy bardzo duże platformy internetowe zdefiniowane w art. 25 ust. 1 rozporządzenia [odniesienie do rozporządzenia w sprawie aktu o usługach cyfrowych] wymagają uwierzytelniania użytkowników do celów dostępu do usług online, platformy te powinny być zobowiązane do akceptowania wykorzystywania europejskich portfeli tożsamości cyfrowej na podstawie dobrowolnego wniosku użytkownika. Użytkownicy nie powinni być zobowiązani do korzystania z portfela do celów dostępu do usług prywatnych, ale jeżeli sobie tego życzą, duże platformy internetowe powinny akceptować w tym celu europejski portfel tożsamości cyfrowej przy jednoczesnym poszanowaniu zasady minimalizacji danych. Biorąc pod uwagę znaczenie bardzo dużych platform internetowych ze względu na ich zasięg, w szczególności wyrażony liczbą odbiorców usługi i transakcji finansowych, jest to konieczne, aby zwiększyć ochronę użytkowników przed oszustwami i zapewnić wysoki poziom ochrony danych. Aby przyczynić się do zapewnienia szerokiej dostępności i używalności środków identyfikacji elektronicznej, w tym europejskich portfeli tożsamości cyfrowej objętych zakresem niniejszego rozporządzenia, należy opracować samoregulacyjne kodeksy postępowania na szczeblu Unii („kodeksy postępowania”). 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 korzystają z usług identyfikacji elektronicznej świadczonych przez strony trzecie. Kodeksy te należy opracować w terminie 12 miesięcy od przyjęcia niniejszego rozporządzenia. Po 24 miesiącach od wdrożenia tych przepisów Komisja powinna ocenić ich skuteczność pod względem dostępności i używalności dla użytkowników europejskich portfeli tożsamości cyfrowej.

(29) Selektywne ujawnianie jest pojęciem upoważniającym właściciela danych do ujawnienia jedynie niektórych części większego zbioru danych, aby podmiot otrzymujący mógł uzyskać wyłącznie informacje, które są wymagane, np. aby użytkownik mógł ujawnić stronie ufającej jedynie te dane, które są niezbędne do świadczenia usługi żądanej przez użytkownika. Europejski portfel tożsamości cyfrowej powinien pod względem technicznym umożliwiać selektywne ujawnianie atrybutów stronom ufającym. Takie selektywnie ujawnione atrybuty, również w przypadku gdy pierwotnie stanowiły one część wielu odrębnych elektronicznych poświadczeń, mogą być następnie łączone i przedstawiane stronom ufającym. Funkcja ta powinna stać się jedną z podstawowych cech projektowych, co zwiększy wygodę i ochronę danych osobowych, w tym jeżeli chodzi o minimalizację danych.

(30) Atrybuty dostarczane przez kwalifikowanych dostawców usług zaufania w ramach kwalifikowanego poświadczania atrybutów powinny być weryfikowane w zestawieniu ze źródłami autentycznymi bezpośrednio przez kwalifikowanego dostawcę usług zaufania albo przez wyznaczonych pośredników uznanych na poziomie krajowym zgodnie z prawem krajowym lub unijnym do celów bezpiecznej wymiany poświadczonych atrybutów między dostawcami usług w zakresie tożsamości lub poświadczania atrybutów a stronami ufającymi. Państwa członkowskie powinny ustanowić odpowiednie mechanizmy na szczeblu 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. Odpowiednie mechanizmy mogą obejmować korzystanie, zgodnie z prawem krajowym, z konkretnych pośredników lub rozwiązań technicznych umożliwiających dostęp do źródeł autentycznych. Zapewnienie dostępności mechanizmu, który umożliwi weryfikację atrybutów względem źródeł autentycznych, powinno ułatwić przestrzeganie przez kwalifikowanych dostawców usług zaufania, którzy dostarczają kwalifikowanych elektronicznych poświadczeń atrybutów, ich obowiązków określonych w niniejszym rozporządzeniu. Załącznik VI zawiera wykaz kategorii atrybutów, w odniesieniu do których państwa członkowskie powinny zapewnić podjęcie środków umożliwiających kwalifikowanym dostawcom elektronicznych poświadczeń atrybutów zweryfikowanie, drogą elektroniczną, na wniosek użytkownika, ich autentyczności względem odpowiedniego źródła autentycznego. Państwa członkowskie powinny uzgodnić specjalne atrybuty należące do tych kategorii.

(31) Bezpieczna identyfikacja elektroniczna i dostarczanie poświadczeń atrybutów powinny zapewniać sektorowi usług finansowych dodatkową elastyczność oraz rozwiązania umożliwiające identyfikację klientów i wymianę określonych atrybutów niezbędnych do spełnienia na przykład wymogów należytej staranności wobec klienta wynikających z rozporządzenia w sprawie przeciwdziałania praniu pieniędzy [odesłanie zostanie dodane po przyjęciu wniosku], 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 do rachunku i inicjowania transakcji w dziedzinie usług płatniczych.

(31a) Aby zapewnić spójność praktyk certyfikacji w całej UE, Komisja powinna wydać wytyczne dotyczące certyfikacji i ponownej certyfikacji kwalifikowanych urządzeń do składania podpisu elektronicznego i kwalifikowanych urządzeń do składania pieczęci elektronicznej, w tym ich ważności i ograniczeń w czasie. Niniejsze rozporządzenie nie uniemożliwia państwom członkowskim zezwolenia podmiotom publicznym lub prywatnym, które posiadają certyfikowane kwalifikowane urządzenia do składania podpisu elektronicznego, na czasowe przedłużenie ważności certyfikacji, w przypadku gdy ponownej certyfikacji tego samego urządzenia nie można było przeprowadzić w prawnie określonym terminie z przyczyn innych niż naruszenie lub incydent bezpieczeństwa oraz bez uszczerbku dla mającej zastosowanie praktyki dotyczącej certyfikacji.

(32) Usługi uwierzytelniania witryn internetowych dają użytkownikom wysoki poziom pewności, że za daną witryną internetową, bez względu na to, jaka platforma jest wykorzystywana do jej wyświetlenia, stoi prawdziwy i prawowity podmiot. Usługi te przyczyniają się do budowy zaufania do prowadzenia działalności gospodarczej online oraz do ograniczania liczby oszustw internetowych. Korzystanie przez witryny internetowe z usług uwierzytelniania witryn internetowych powinno być dobrowolne. Aby uwierzytelnianie witryny internetowej stało się środkiem zwiększającym zaufanie, zapewniającym użytkownikowi lepsze doświadczenie i wspierającym wzrost na rynku wewnętrznym, niniejsze rozporządzenie powinno określać minimalne obowiązki w zakresie bezpieczeństwa i odpowiedzialności dla dostawców usług uwierzytelniania witryn internetowych i dla tych usług. W tym celu dostawcy przeglądarek internetowych powinni zapewniać obsługę kwalifikowanych certyfikatów uwierzytelniania witryn internetowych na podstawie rozporządzenia (UE) nr 910/2014 i interoperacyjność z tymi certyfikatami. Powinny one uznawać kwalifikowane certyfikaty uwierzytelniania witryn internetowych i umożliwiać wyświetlanie certyfikowanych danych dotyczących tożsamości użytkownikowi końcowemu w środowisku przeglądarki w oparciu o specyfikacje określone zgodnie z niniejszym rozporządzeniem. Uznanie kwalifikowanego certyfikatu uwierzytelniania witryn internetowych za kwalifikowany certyfikat wydany przez kwalifikowanego dostawcę usług zaufania powinno zapewnić możliwość uwierzytelnienia i weryfikacji danych dotyczących tożsamości zawartych w certyfikacie zgodnie z niniejszym rozporządzeniem. Nie powinno to mieć wpływu na możliwość usuwania przez dostawców przeglądarek internetowych poważnych niezgodności związanych z naruszeniem bezpieczeństwa i utratą integralności poszczególnych certyfikatów, a tym samym przyczyniania się do bezpieczeństwa użytkowników końcowych w internecie. Aby lepiej chronić obywateli i szerzej propagować korzystanie z kwalifikowanych certyfikatów uwierzytelniania witryn internetowych, organy publiczne w państwach członkowskich powinny rozważyć włączenie tych certyfikatów do swoich witryn internetowych.

(33) Wiele państw członkowskich wprowadziło krajowe wymogi dotyczące usług zapewniających bezpieczną i wiarygodną archiwizację cyfrową, aby umożliwić długoterminową konserwację danych elektronicznych i 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 pozostałych usług zaufania określonych w niniejszym rozporządzeniu. Ramy te 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 dokumentów sporządzonych w formacie elektronicznym oraz dokumentów papierowych, które zostały zeskanowane i zdigitalizowane. W razie potrzeby przepisy te powinny umożliwiać przenoszenie przechowywanych danych elektronicznych na różnych nośnikach lub formatach w celu przedłużenia ich trwałości i czytelności poza technologiczny okres ważności, przy jednoczesnym minimalizowaniu strat i modyfikacji w możliwie największym zakresie. W przypadku gdy dane elektroniczne przekazywane do usługi archiwizacji cyfrowej 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 konserwacji takich danych, w miarę możliwości w oparciu o wykorzystanie innych kwalifikowanych elektronicznych usług zaufania ustanowionych niniejszym rozporządzeniem. Do tworzenia dowodów konserwacji przy użyciu podpisów elektronicznych, pieczęci elektronicznych lub elektronicznych znaczników czasu należy korzystać z kwalifikowanych elektronicznych usług zaufania. W zakresie, w jakim usługi archiwizacji elektronicznej nie są zharmonizowane niniejszym rozporządzeniem, państwa członkowskie mogą utrzymać lub wprowadzić przepisy krajowe, zgodne z prawem Unii, odnoszące się do tych usług, takie jak przepisy szczegółowe dopuszczające pewne odstępstwa w odniesieniu do usług zintegrowanych w ramach danej organizacji i wykorzystywanych wyłącznie do „archiwów wewnętrznych” tej organizacji. Niniejsze rozporządzenie nie powinno wprowadzać rozróżnienia między dokumentami sporządzonymi w formacie elektronicznym a dokumentami fizycznymi, które zostały zdigitalizowane.

(33a) Krajowe archiwa i instytucje pamięci, jako organizacje, które w interesie publicznym zajmują się ochroną dziedzictwa mającego postać dokumentów, są zazwyczaj upoważnione do prowadzenia działalności na mocy prawa krajowego i niekoniecznie świadczą usługi zaufania w rozumieniu niniejszego rozporządzenia. W zakresie, w jakim instytucje te nie świadczą takich usług, niniejsze rozporządzenie pozostaje bez uszczerbku dla ich funkcjonowania.

(34) Rejestry elektroniczne to sekwencje elektronicznych rekordów danych zapewniające integralność tych danych i dokładność ich chronologicznego uporządkowania. Celem rejestrów elektronicznych jest ustanowienie chronologicznej sekwencji rekordów danych, aby zapobiec kopiowaniu aktywów cyfrowych i ich sprzedaży kilku odbiorcom. Rejestry elektroniczne mogą być na przykład wykorzystywane do prowadzenia cyfrowych rekordów dotyczących: własności w handlu światowym, finansowania łańcucha dostaw, cyfryzacji praw własności intelektualnej lub towarów takich jak energia elektryczna. W połączeniu z innymi technologiami mogą one przyczynić się do opracowania rozwiązań na rzecz bardziej wydajnych usług publicznych w większym stopniu przyczyniających się do transformacji, takich jak głosowanie elektroniczne, transgraniczna współpraca organów celnych, transgraniczna współpraca instytucji akademickich lub rejestrowanie własności nieruchomości w zdecentralizowanych rejestrach gruntów. Kwalifikowane rejestry elektroniczne tworzą domniemanie prawne dotyczące niepowtarzalnego i dokładnego sekwencyjnego uporządkowania chronologicznego i integralności rekordów danych w rejestrze. Specjalne atrybuty rejestrów elektronicznych, tj. sekwencyjne uporządkowanie chronologiczne rekordów danych, odróżniają rejestry elektroniczne od innych usług zaufania, takich jak elektroniczne znaczniki czasu i usługi rejestrowanego doręczenia elektronicznego. W szczególności ani stosowanie znaczników czasu dokumentów cyfrowych, ani ich przekazywanie za pośrednictwem usług rejestrowanego doręczenia elektronicznego nie może – bez dalszych środków technicznych lub organizacyjnych – 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 (scentralizowanego lub rozproszonego).

(35) Aby zapobiec fragmentacji rynku wewnętrznego, należy ustanowić ogólnoeuropejskie ramy prawne umożliwiające transgraniczne uznawanie usług zaufania do celów rejestrowania danych w kwalifikowanych rejestrach elektronicznych. Dostawcy usług zaufania do celów rejestrów elektronicznych powinni być upoważnieni do ustalenia sekwencyjnego rejestrowania danych w rejestrze. Niniejsze rozporządzenie nie narusza żadnych zobowiązań prawnych, które użytkownicy rejestrów elektronicznych mogą być zobowiązani spełnić na mocy prawa unijnego i prawa krajowego. I tak na przykład przypadki użycia związane z przetwarzaniem danych osobowych powinny być zgodne z rozporządzeniem (UE) 2016/679. Przypadki użycia obejmujące kryptoaktywa powinny być zgodne ze wszystkimi mającymi zastosowanie przepisami finansowymi, w tym np. z dyrektywą w sprawie rynków instrumentów finansowych[9], dyrektywą w sprawie usług płatniczych[10], dyrektywą w sprawie pieniądza elektronicznego[11], a także z ewentualnymi przyszłymi przepisami dotyczącymi rynków kryptoaktywów oraz z przepisami dotyczącymi przeciwdziałania praniu pieniędzy, które mogłyby zostać włączone do rozporządzenia w sprawie transferu środków pieniężnych[12], i mogłyby wymagać od dostawców usług w zakresie kryptoaktywów weryfikacji tożsamości użytkowników rejestrów elektronicznych w celu zapewnienia zgodności z międzynarodowymi standardami przeciwdziałania praniu pieniędzy.

---

9 Dyrektywa Parlamentu Europejskiego i Rady 2014/65/UE z dnia 15 maja 2014 r. w sprawie rynków instrumentów finansowych oraz zmieniająca dyrektywę 2002/92/WE, (Dz.U. L 173 z 12.6.2014, s. 349–496).

10 Dyrektywa Parlamentu Europejskiego i Rady (UE) 2015/2366 z dnia 25 listopada 2015 r. w sprawie usług płatniczych w ramach rynku wewnętrznego, zmieniająca dyrektywy 2002/65/WE, 2009/110/WE, 2013/36/UE i rozporządzenie (UE) nr 1093/2010 oraz uchylająca dyrektywę 2007/64/WE, Dz.U. L 337 z 23.12.2015, s. 35–127.

11 Dyrektywa Parlamentu Europejskiego i Rady 2009/110/WE z dnia 16 września 2009 r. w sprawie podejmowania i prowadzenia działalności przez instytucje pieniądza elektronicznego oraz nadzoru ostrożnościowego nad ich działalnością, zmieniająca dyrektywy 2005/60/WE i 2006/48/WE oraz uchylająca dyrektywę 2000/46/WE (Dz.U. L 267 z 10.10.2009, s. 7–17).

12 Zob. wniosek Komisji z dnia 20 lipca 2021 r. dotyczący przekształcenia rozporządzenia Parlamentu Europejskiego i Rady (UE) 2015/847 z dnia 20 maja 2015 r. w sprawie informacji towarzyszących transferom środków pieniężnych, COM(2021) 422 final.

(36) Aby uniknąć fragmentacji i barier wynikających z rozbieżnych norm i ograniczeń technicznych oraz aby zapewnić skoordynowany proces mający na celu wyeliminowanie zagrożeń dla wdrożenia przyszłych europejskich ram tożsamości cyfrowej, potrzebne są ramy bliskiej i zorganizowanej współpracy między Komisją, państwami członkowskimi i sektorem prywatnym. Aby osiągnąć ten cel, państwa członkowskie powinny współpracować w obrębie ram określonych w zaleceniu Komisji (UE) XXX/XXXX [zestaw narzędzi na potrzeby skoordynowanego podejścia do europejskich ram tożsamości cyfrowej][13] nad sformułowaniem zestawu narzędzi na potrzeby europejskich ram tożsamości cyfrowej. Zestaw narzędzi powinien zawierać kompleksową architekturę techniczną i ramy odniesienia, zestaw wspólnych norm i technicznych dokumentów referencyjnych oraz zestaw wytycznych i opisów najlepszych praktyk obejmujące co najmniej wszystkie aspekty funkcji i interoperacyjności europejskich portfeli tożsamości cyfrowej, w tym podpisów elektronicznych, oraz kwalifikowanej usługi zaufania służącej poświadczaniu atrybutów, które to rozwiązania określono w niniejszym rozporządzeniu. W tym kontekście państwa członkowskie powinny również osiągnąć porozumienie w sprawie wspólnych elementów modelu biznesowego i struktury opłat europejskich portfeli tożsamości cyfrowej, aby ułatwić korzystanie z tych portfeli, w szczególności przez małe i średnie przedsiębiorstwa 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.

(36a) Państwa członkowskie powinny ustanowić przepisy dotyczące kar za naruszenia, takie jak bezpośrednie lub pośrednie praktyki prowadzące do pomylenia niekwalifikowanych usług zaufania z kwalifikowanymi usługami zaufania lub do nadużywania unijnego znaku zaufania przez niekwalifikowanych dostawców usług zaufania. Znak zaufania UE nie powinien być używany na warunkach, które bezpośrednio lub pośrednio prowadzą do przekonania, że jakiekolwiek niekwalifikowane usługi zaufania oferowane przez tego dostawcę są usługami kwalifikowanymi.

---

13 [po przyjęciu wstawić odesłanie]

(36b) Niniejsze rozporządzenie powinno zapewnić 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 poza Unię, jeżeli dostawca ten udzieli gwarancji, zapewniając możliwość egzekwowania działań nadzorczych i audytów, tak jakby te operacje były prowadzone w Unii. Jeżeli nie można w pełni zagwarantować zgodności z rozporządzeniem, organy nadzoru powinny mieć możliwość przyjęcia proporcjonalnych i uzasadnionych środków, w tym odebrania kwalifikowanego statusu świadczonej usługi zaufania.

(36c) Aby zagwarantować pewność prawa w odniesieniu do ważności zaawansowanych podpisów elektronicznych opartych na kwalifikowanych certyfikatach, niezbędne jest wyszczególnienie elementów zaawansowanych podpisów elektronicznych opartych na kwalifikowanych certyfikatach, które powinny być ocenione przez stronę ufającą dokonującą walidacji tych podpisów.

(36d) Dostawcy usług zaufania powinni stosować algorytmy kryptograficzne odzwierciedlające aktualne najlepsze praktyki i godne zaufania wdrażanie tych algorytmów w celu zapewnienia bezpieczeństwa i wiarygodności ich usług zaufania.

(36e) Niniejsze rozporządzenie powinno nakładać na dostawców kwalifikowanych usług zaufania obowiązek weryfikacji tożsamości osoby fizycznej lub prawnej, której wydawany jest kwalifikowany certyfikat, w oparciu o różne zharmonizowane metody w całej UE. Metoda taka może obejmować poleganie na środkach identyfikacji elektronicznej, które spełniają wymogi „średniego” poziomu bezpieczeństwa w połączeniu z dodatkowymi zharmonizowanymi zdalnymi procedurami zapewniającymi identyfikację osoby przy wysokim poziomie pewności.

(36f) Za użytkowników biznesowych zgodnie z art. 2 pkt 21 rozporządzenia (UE) 2022/1925 należy uznać wydawców europejskich portfeli tożsamości cyfrowej i wydawców notyfikowanych środków identyfikacji elektronicznej działających w celach handlowych lub zawodowych i korzystających z podstawowych usług platformowych oferowanych przez strażników dostępu do celów oferowania użytkownikom końcowym towarów i usług lub w trakcie ich dostarczania. W związku z tym na strażnikach dostępu powinien spoczywać wymóg zapewnienia nieodpłatnie skutecznej interoperacyjności z tym samym systemem operacyjnym oraz funkcjami sprzętu lub oprogramowania, a także dostępu do tego systemu operacyjnego i tych funkcji na potrzeby interoperacyjności, które to system i funkcje są dostępne dla nich lub używane przez nich do świadczenia własnych uzupełniających i wspierających usług lub dostarczania własnego uzupełniającego lub wspierającego sprzętu. Powinno to umożliwić wydawcom europejskich portfeli tożsamości cyfrowej i wydawcom notyfikowanych środków identyfikacji elektronicznej łączenie się za pośrednictwem interfejsów lub podobnych rozwiązań z odpowiednimi funkcjami tak skutecznie, jak ma to miejsce w przypadku własnych usług lub sprzętu strażnika dostępu.

(36g) Aby zachować zgodność niniejszego rozporządzenia z obecnymi zmianami i dotrzymać kroku praktykom na rynku wewnętrznym, akty delegowane i wykonawcze przyjmowane przez Komisję powinny być poddawane przeglądowi i w razie potrzeby regularnie aktualizowane. Ocena, czy aktualizacje te są konieczne, powinna uwzględniać nowe technologie, praktyki, normy lub specyfikacje techniczne pojawiające się na rynku wewnętrznym.

(37) Na podstawie art. 42 ust. 1 rozporządzenia Parlamentu Europejskiego i Rady (UE) 2018/1525[14] zasięgnięto opinii Europejskiego Inspektora Ochrony Danych.

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

---

14 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).

PRZYJMUJĄ NINIEJSZE ROZPORZĄDZENIE:

Artykuł 1

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

1) art. 1 otrzymuje brzmienie:

„Celem niniejszego rozporządzenia jest zapewnienie należytego funkcjonowania rynku wewnętrznego oraz odpowiedniego poziomu bezpieczeństwa środków identyfikacji elektronicznej i usług zaufania. W tym celu niniejsze rozporządzenie:

aa) określa warunki, na jakich państwa członkowskie zapewniają i uznają środki identyfikacji elektronicznej osób fizycznych i prawnych, objęte notyfikowanym systemem identyfikacji elektronicznej innego państwa członkowskiego;

ab) określa warunki, na jakich państwa członkowskie zapewniają i uznają europejskie portfele tożsamości cyfrowej;

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

c) ustanawia ramy prawne dla podpisów elektronicznych, pieczęci elektronicznych, elektronicznych znaczników czasu, dokumentów elektronicznych, usług rejestrowanego doręczenia elektronicznego, usług certyfikacji uwierzytelniania witryn internetowych, elektronicznej walidacji podpisów elektronicznych, pieczęci elektronicznych i ich certyfikatów, elektronicznej walidacji certyfikatów uwierzytelniania witryn internetowych, elektronicznej konserwacji elektronicznych podpisów, pieczęci elektronicznych i ich certyfikatów, archiwizacji elektronicznej, elektronicznego poświadczenia atrybutów, zarządzania urządzeniami do składania kwalifikowanych podpisów i pieczęci elektronicznych na odległość 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, które zostały notyfikowane przez państwo członkowskie, do europejskich portfeli tożsamości cyfrowej zapewnianych przez państwa członkowskie oraz do dostawców usług zaufania mających siedzibę w Unii.”;

b) ust. 3 otrzymuje brzmienie:

„3. Niniejsze rozporządzenie nie ma wpływu na prawo krajowe ani unijne związane z zawieraniem i ważnością umów lub innych zobowiązań prawnych lub proceduralnych, dotyczące ich formy, ani na wymogi sektorowe dotyczące ich formy.”;

3) w art. 3 wprowadza się następujące zmiany:

(X) pkt 1 otrzymuje brzmienie:

„1) »identyfikacja elektroniczna« oznacza proces używania danych w postaci elektronicznej identyfikujących osobę, unikalnie reprezentujących albo osobę fizyczną lub prawną, albo osobę fizyczną reprezentującą osobę fizyczną lub prawną;”;

a) pkt 2 otrzymuje brzmienie:

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

aa) pkt 3 otrzymuje brzmienie:

„3) »dane identyfikujące osobę« oznaczają zestaw danych wydawanych zgodnie z prawem unijnym lub prawem krajowym umożliwiających ustalenie tożsamości osoby fizycznej lub prawnej, lub osoby fizycznej reprezentującej osobę fizyczną lub prawną;”;

b) pkt 4 otrzymuje brzmienie:

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

ba) pkt 5 otrzymuje brzmienie:

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

bb) dodaje się pkt 5a w brzmieniu:

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

c) pkt 14 otrzymuje brzmienie:

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

d) pkt 16 otrzymuje brzmienie:

„16) »usługa zaufania« oznacza usługę elektroniczną zazwyczaj świadczoną za wynagrodzeniem i obejmującą:

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

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

b) składanie podpisów elektronicznych lub pieczęci elektronicznych;

c) walidację podpisów elektronicznych lub pieczęci elektronicznych;

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

e) zarządzanie urządzeniami do składania kwalifikowanego podpisu elektronicznego na odległość lub urządzeniami do składania kwalifikowanej pieczęci elektronicznej na odległość;

f) wydawanie elektronicznych poświadczeń atrybutów;

fa) walidację elektronicznego poświadczenia atrybutów;

g) tworzenie elektronicznych znaczników czasu;

ga) walidację elektronicznych znaczników czasu;

gb) świadczenie usług rejestrowanego doręczenia elektronicznego;

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

h) archiwizację elektroniczną danych elektronicznych; lub

i) rejestrowanie danych elektronicznych w rejestrze elektronicznym.”;

da) pkt 18 otrzymuje brzmienie:

„18) »jednostka oceniająca zgodność« oznacza jednostkę określoną 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 do dokonywania walidacji europejskich portfeli tożsamości cyfrowej lub środków identyfikacji elektronicznej;”;

e) pkt 21 otrzymuje brzmienie:

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

f) dodaje się pkt 23a i 23b w brzmieniu:

„23a) »kwalifikowane urządzenie do składania podpisu elektronicznego na odległość« oznacza kwalifikowane urządzenie do składania podpisu elektronicznego zarządzane przez kwalifikowanego dostawcę 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 zarządzane przez kwalifikowanego dostawcę usług zaufania zgodnie z art. 39a w imieniu podmiotu składającego pieczęć;”;

g) pkt 29 otrzymuje brzmienie:

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

h) pkt 41 otrzymuje brzmienie:

„41) »walidacja« oznacza proces weryfikacji i potwierdzania, że dane w postaci elektronicznej są ważne zgodnie z wymogami niniejszego rozporządzenia;”;

i) dodaje się pkt 42–55b w brzmieniu:

„42) »europejski portfel tożsamości cyfrowej« jest środkiem identyfikacji elektronicznej, który umożliwia użytkownikowi przechowywanie i pobieranie danych dotyczących tożsamości, w tym danych identyfikujących osobę, elektronicznych poświadczeń atrybutów powiązanych z ich tożsamością, dostarczanie ich na żądanie stronom ufającym oraz wykorzystywanie ich do uwierzytelniania online i, w stosownych przypadkach, offline na potrzeby usługi zgodnie z art. 6a, i umożliwia podpisywanie za pomocą kwalifikowanych podpisów elektronicznych i pieczętowanie za pomocą kwalifikowanych pieczęci elektronicznych;

43) »atrybut« oznacza cechę charakterystyczną, właściwość, prawo lub zgodę osoby fizycznej lub osoby 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 i spełnia wymogi określone w załączniku V;

45a) »elektroniczne poświadczenie atrybutów wydane przez podmiot sektora publicznego odpowiedzialny za autentyczne źródło lub w jego imieniu« oznacza elektroniczne poświadczenia atrybutów wydawane przez podmiot sektora publicznego odpowiedzialny za autentyczne źródło lub przez podmiot sektora publicznego wyznaczony przez państwo członkowskie do wydawania takich poświadczeń atrybutów w imieniu podmiotów sektora publicznego odpowiedzialnych za źródła autentyczne zgodnie z art. 45da i spełniających wymogi określone w załączniku VII;

46) »źródło autentyczne« oznacza repozytorium lub system, prowadzone na odpowiedzialność podmiotu sektora publicznego lub podmiotu prywatnego, które zawierają i dostarczają atrybuty dotyczące osoby fizycznej lub prawnej i które uważa się za jedno z podstawowych źródeł tych informacji lub uznaje za autentyczne zgodnie z prawem unijnym lub prawem krajowym, w tym praktykami administracyjnymi;

47) »archiwizacja elektroniczna« oznacza usługę zapewniającą odbiór, przechowywanie, pobieranie i usuwanie danych elektronicznych w celu zagwarantowania ich trwałości i czytelności, a także konserwacji ich integralności, poufności i dowodu pochodzenia przez cały okres konserwacji;

48) »kwalifikowana usługa archiwizacji elektronicznej« oznacza usługę archiwizacji elektronicznej, która spełnia wymogi określone w art. 45ga;

49) »unijny znak zaufania dla portfela tożsamości cyfrowej« oznacza weryfikowalne wskazanie w prosty, rozpoznawalny i jasny sposób, że europejski portfel tożsamości cyfrowej zapewniono zgodnie z niniejszym rozporządzeniem;

50) »silne uwierzytelnianie użytkownika« oznacza uwierzytelnianie w oparciu o zastosowanie co najmniej dwóch składników uwierzytelniania należących do różnych kategorii: wiedza (coś, co wie wyłącznie użytkownik), posiadanie (coś, co posiada wyłącznie użytkownik) albo cechy klienta (coś, czym jest użytkownik), niezależnych w tym sensie, że naruszenie jednego z nich nie osłabia wiarygodności pozostałych, które to uwierzytelnianie jest zaprojektowane w sposób zapewniający ochronę poufności danych uwierzytelniających;

53) »rejestr elektroniczny« oznacza sekwencje elektronicznych rekordów danych zapewniającą integralność tych danych i dokładność ich chronologicznego uporządkowania;

53a) »kwalifikowany rejestr elektroniczny« oznacza rejestr elektroniczny, który spełnia wymogi określone w art. 45i;

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

55) »dopasowywanie rekordów« oznacza proces, w ramach którego dane identyfikacyjne osoby, środki identyfikacji osoby, kwalifikowane elektroniczne poświadczenie atrybutów lub poświadczenia atrybutów wydane przez podmiot sektora publicznego odpowiedzialny za autentyczne źródło lub w jego imieniu są dopasowane do istniejącego konta należącego do tej samej osoby lub są z nim związane;

55a) »unikalny i trwały identyfikator« oznacza identyfikator, który może składać się z albo pojedynczych albo wielu krajowych lub sektorowych danych identyfikacyjnych, jest powiązany z pojedynczym użytkownikiem w ramach danego systemu i jest trwały w czasie;

55b) »rekord danych« oznacza dane elektroniczne zarejestrowane wraz z powiązanymi metadanymi (lub atrybutami) wspierającymi przetwarzanie danych;

55c) »korzystanie z europejskich portfeli tożsamości cyfrowej offline« oznacza interakcję między użytkownikiem a stroną ufającą w fizycznej lokalizacji, przy czym portfel nie musi do celów tej interakcji mieć dostępu do systemów zdalnych za pośrednictwem sieci komunikacji elektronicznej.”.

„*Artykuł 5*

Pseudonimy w transakcji elektronicznej

Bez uszczerbku dla skutku prawnego, jaki prawo krajowe przyznaje pseudonimom, nie zakazuje się używania pseudonimów w transakcjach elektronicznych.”;

5) w rozdziale II przed art. 6a dodaje się następujący nagłówek:

„SEKCJA I

Europejskie portfele tożsamości cyfrowej”;

7) dodaje się art. 6a, 6b, 6c i 6d w brzmieniu:

„*Artykuł 6a*

Europejskie portfele tożsamości cyfrowej

1. W celu zapewnienia wszystkim osobom fizycznym i prawnym w Unii bezpiecznego, zaufanego i sprawnego transgranicznego dostępu do usług publicznych i prywatnych każde państwo członkowskie zapewnia, aby europejski portfel tożsamości cyfrowej był zapewniany w terminie 24 miesięcy od wejścia w życie aktów wykonawczych, o których mowa w ust. 11 i art. 6c ust. 4.

2. Europejskie portfele tożsamości cyfrowej są zapewniane:

   a) przez państwo członkowskie;

   b) na mocy upoważnienia od państwa członkowskiego lub

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

3. Europejskie portfele tożsamości cyfrowej są środkami identyfikacji elektronicznej, które umożliwiają użytkownikowi w sposób dla niego przejrzysty i identyfikowalny:

   a) bezpieczne żądanie, wybieranie, łączenie, przechowywanie, usuwanie i przedstawianie elektronicznego poświadczenia atrybutów i danych identyfikujących osobę stronom ufającym, w tym uwierzytelnianie online i, w stosownych przypadkach, offline, w celu korzystania z usług publicznych i prywatnych, przy jednoczesnym zapewnieniu możliwości selektywnego ujawniania danych;

   b) podpisywanie za pomocą kwalifikowanych podpisów elektronicznych i pieczętowanie za pomocą kwalifikowanych pieczęci elektronicznych.

4. Europejskie portfele tożsamości cyfrowej w szczególności:

a) zapewniają wspólny zbiór interfejsów:

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

2) dla stron ufających do celów wnioskowania o dane identyfikujące osobę i elektroniczne poświadczenia atrybutów;

3) do celów przedstawiania stronom ufającym danych identyfikujących osobę lub elektronicznego poświadczenia atrybutów online i, w stosownych przypadkach, również offline;

4) dla użytkownika, aby umożliwić interakcję z europejskim portfelem tożsamości cyfrowej i wyświetlić „unijny znak zaufania dla portfela tożsamości cyfrowej”;

b) nie dostarczają dostawcom usług zaufania elektronicznych poświadczeń atrybutów żadnych informacji na temat wykorzystywania tych atrybutów po ich wydaniu;

ba) zapewniają możliwość walidacji tożsamości stron ufających poprzez wdrożenie mechanizmów uwierzytelniania zgodnie z art. 6b;

c) spełniają wymogi określone w art. 8 w odniesieniu do „wysokiego” poziomu bezpieczeństwa stosowane, odpowiednio, do zarządzania danymi identyfikującymi osobę i ich wykorzystywania za pośrednictwem portfela, w tym do elektronicznej identyfikacji i elektronicznego uwierzytelniania;

e) zapewniają, aby dane identyfikujące osobę, o których mowa w art. 12 ust. 4 lit. d), unikalnie i trwale reprezentowały osobę fizyczną, osobę prawną lub osobę fizyczną reprezentującą osobę fizyczną lub prawną, które są powiązane z portfelem.

4a. Państwa członkowskie ustanawiają procedury umożliwiające użytkownikowi zgłaszanie ewentualnej utraty lub niewłaściwego wykorzystania jego portfela oraz wnioskowanie o jego unieważnienie.

5. Państwa członkowskie zapewniają mechanizmy walidacji europejskich portfeli tożsamości cyfrowej, aby:

a) zapewnić możliwość weryfikacji ich autentyczności i ważności;

d) umożliwić użytkownikowi uwierzytelnienie stron ufających zgodnie z art. 6b.

6. Europejskie portfele tożsamości cyfrowej wydaje się w ramach notyfikowanego systemu identyfikacji elektronicznej o „wysokim” poziomie bezpieczeństwa.

6a. Wydawanie, używanie w celu uwierzytelnienia i unieważnianie europejskich portfeli tożsamości cyfrowej jest nieodpłatne w przypadku osób fizycznych.

6b. Bez uszczerbku dla art. 6db państwa członkowskie mogą przewidzieć, zgodnie z prawem krajowym, dodatkowe funkcje europejskich portfeli tożsamości cyfrowej, w tym interoperacyjność z istniejącymi krajowymi środkami identyfikacji elektronicznej.

7. Użytkownicy powinni mieć pełną kontrolę nad wykorzystywaniem europejskiego portfela tożsamości cyfrowej i znajdujących się w nim danych. Wydawca europejskiego portfela tożsamości cyfrowej nie gromadzi informacji na temat korzystania z portfela, które nie są niezbędne do świadczenia usług związanych z portfelem, ani nie łączy danych identyfikujących osobę ani żadnych innych danych osobowych przechowywanych lub związanych z korzystaniem z europejskiego portfela tożsamości cyfrowej z danymi osobowymi pochodzącymi z innych usług oferowanych przez tego wydawcę lub z usług osób trzecich, które nie są niezbędne do świadczenia usług związanych z portfelem, chyba że użytkownik wyraźnie o to wystąpi. Dane osobowe związane z udostępnianiem europejskich portfeli tożsamości cyfrowej powinny być logicznie oddzielone od wszelkich innych danych będących w posiadaniu wydawcy europejskich portfeli tożsamości cyfrowej. Jeśli europejski portfel tożsamości cyfrowej jest udostępniany przez podmioty prywatne zgodnie z ust. 2 lit. b) i c), przepisy art. 45f ust. 4 stosuje się odpowiednio.

7a. Państwa członkowskie bez zbędnej zwłoki przekazują Komisji informacje o:

a) organie odpowiedzialnym za sporządzenie i prowadzenie wykazu notyfikowanych stron ufających, które polegają na europejskich portfelach tożsamości cyfrowej zgodnie z art. 6b ust. 2;

b) organach odpowiedzialnych za zapewnianie europejskich portfeli tożsamości cyfrowej zgodnie z art. 6a ust. 1;

c) organach odpowiedzialnych za zapewnienie powiązania danych identyfikujących osobę z portfelem zgodnie z art. 6a ust. 4 lit. e).

Wśród tych przekazywanych informacji powinny się również znaleźć informacje na temat mechanizmu umożliwiającego walidację danych identyfikujących osobę, o których mowa w art. 12 ust. 4, oraz tożsamości stron ufających.

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

8. Art. 11 stosuje się odpowiednio do europejskiego portfela tożsamości cyfrowej.

9. Art. 24 ust. 2 lit. b), e), g) i h) stosuje się odpowiednio do wydawcy europejskich portfeli tożsamości cyfrowej.

10. Europejski portfel tożsamości cyfrowej udostępnia się osobom z niepełnosprawnościami zgodnie z wymogami dostępności określonymi w dyrektywie (UE) 2019/882.

11. W terminie 6 miesięcy od wejścia w życie niniejszego rozporządzenia Komisja ustanawia specyfikacje techniczne i operacyjne oraz normy referencyjne dotyczące wymogów, o których mowa w ust. 3, 4, 5 i 7a, w drodze aktu wykonawczego dotyczącego wdrożenia europejskiego portfela tożsamości cyfrowej. Wspomniany akt wykonawczy przyjmuje się zgodnie z procedurą sprawdzającą, o której mowa w art. 48 ust. 2.

11a. Komisja ustanawia specyfikacje techniczne i operacyjne oraz normy referencyjne w celu ułatwienia onboardingu do europejskiego portfela tożsamości cyfrowej użytkowników korzystających ze środków identyfikacji elektronicznej zgodnych z „wysokim" poziomem albo środków identyfikacji elektronicznej zgodnych ze „średnim" poziomem, w połączeniu z dodatkowymi procedurami onboardingu na odległość, które łącznie spełniają wymogi dotyczące „wysokiego" poziomu bezpieczeństwa. Wspomniany akt wykonawczy przyjmuje się zgodnie z procedurą sprawdzającą, o której mowa w art. 48 ust. 2.

Artykuł 6b

Strony ufające europejskich portfeli tożsamości cyfrowej

1. W przypadku gdy strony ufające, które świadczą usługi prywatne lub publiczne, zamierzają polegać na europejskich portfelach tożsamości cyfrowej dostarczonych zgodnie z niniejszym rozporządzeniem, zgłaszają to temu państwu członkowskiemu, w którym mają siedzibę.

1a. Procedura zgłaszania musi być racjonalna pod względem kosztów i proporcjonalna do ryzyka oraz zapewniać, by strony ufające dostarczały co najmniej informacje niezbędne do uwierzytelnienia europejskich portfeli tożsamości cyfrowej. Informacje te powinny obejmować co najmniej państwo członkowskie, w którym mają siedzibę, nazwę strony ufającej oraz, w stosownych przypadkach, jej numer rejestrowy zgodnie z oficjalnym rejestrem.

1b. Wymóg zgłoszenia pozostaje bez uszczerbku dla innych wymogów dotyczących zgłaszania i rejestracji zgodnie z prawem unijnym lub prawem krajowym, takich jak wymogi mające zastosowanie do szczególnych kategorii danych osobowych, z którymi mogą wiązać się dodatkowe wymogi dotyczące zezwoleń.

1c. Państwa członkowskie mogą zwolnić strony ufające z wymogu zgłoszenia, jeżeli prawo unijne lub prawo krajowe nie przewiduje szczególnych wymogów dotyczących zgłaszania lub rejestracji w celu uzyskania dostępu do informacji przekazywanych za pośrednictwem europejskiego portfela tożsamości cyfrowej. Zwolnione strony ufające nie muszą uwierzytelniać europejskiego portfela tożsamości cyfrowej.

1d. Strony ufające, które zgłosiły się zgodnie z niniejszym artykułem, niezwłocznie informują dane państwo członkowskie o wszelkich późniejszych zmianach w pierwotnie przekazanych informacjach.

2. Strony ufające zapewniają wdrożenie mechanizmów uwierzytelniania, o których mowa w art. 6a ust. 4 lit. ba).

3. Strony ufające są odpowiedzialne za przeprowadzenie procedury uwierzytelniania danych identyfikujących osobę oraz walidacji elektronicznego poświadczenia atrybutów pochodzących z europejskich portfeli tożsamości cyfrowej uzyskanych poprzez wspólny interfejs zgodnie z art. 6a ust. 4 lit. a) pkt 2.

4. W terminie 6 miesięcy od wejścia w życie niniejszego rozporządzenia Komisja ustanawia specyfikacje techniczne i operacyjne dotyczące wymogów, o których mowa w ust. 1, 1a i 1bd w drodze aktu wykonawczego dotyczącego wdrożenia europejskich portfeli tożsamości cyfrowej, o którym to akcie mowa w art. 6a ust. 11. Wspomniany akt wykonawczy przyjmuje się zgodnie z procedurą sprawdzającą, o której mowa w art. 48 ust. 2.

Artykuł 6c

Certyfikacja europejskich portfeli tożsamości cyfrowej

1. Zgodność europejskich portfeli tożsamości cyfrowej z wymogami określonymi w art. 6a ust. 3, 4 i 5, z wymogiem dotyczącym logicznego oddzielenia określonym w art. 6a ust. 7 oraz, w stosownych przypadkach, z wymogami określonymi w art. 6a ust. 11a jest certyfikowana przez wyznaczone przez państwa członkowskie jednostki oceniające zgodność akredytowane zgodnie z art. 60 aktu o cyberbezpieczeństwie oraz z systemami, specyfikacjami, normami i procedurami, o których mowa w ust. 4 lit. a), aa) i aaa). Certyfikacja nie może przekraczać pięciu lat i podlega warunkowi przeprowadzania, co dwa lata, oceny podatności na zagrożenia. W przypadku gdy zostaną stwierdzone podatności na zagrożenia i nie zostaną one naprawione w terminie trzech miesięcy, certyfikacja zostaje odwołana.

2. Jeżeli chodzi o zgodność z wymogami ochrony danych na podstawie art. 6a ust. 7, certyfikacja na podstawie ust. 1 może zostać uzupełniona o certyfikację zgodnie z art. 42 rozporządzenia (UE) 2016/679.

3. Zgodność europejskich portfeli tożsamości cyfrowej lub ich części z odpowiednimi wymogami dotyczącymi cyberbezpieczeństwa określonymi w art. 6a ust. 3, 4, 5, 7 oraz, w stosownych przypadkach, ust. 11a, jest certyfikowana przez jednostki oceniające zgodność, o których mowa w ust. 1, w ramach odpowiednich programów certyfikacji cyberbezpieczeństwa na podstawie rozporządzenia (UE) 2019/881, wymienione zgodnie z ust. 4 lit. a) i ust. 4 lit. aa).

3a. Certyfikowane europejskie portfele tożsamości cyfrowej nie podlegają wymogom, o którym mowa w art. 7 i 9.

4. W terminie 6 miesięcy od wejścia w życie niniejszego rozporządzenia Komisja w drodze aktów wykonawczych sporządza:

a) wykaz programów certyfikacji cyberbezpieczeństwa zgodnie z rozporządzeniem (UE) 2019/881, wymaganych do certyfikacji europejskich portfeli tożsamości cyfrowej, o których mowa w ust. 3;

aa) specyfikacje, procedury i normy referencyjne dotyczące ich stosowania w ramach odpowiednich programów certyfikacji cyberbezpieczeństwa wymienionych zgodnie z lit. a);

aaa) wykaz specyfikacji, procedur i norm referencyjnych ustanawiających wspólne wymogi certyfikacyjne nieobjęte odpowiednimi programami certyfikacji cyberbezpieczeństwa na podstawie rozporządzenia (UE) 2019/881 do celów certyfikacji, o której mowa w ust. 1, w celu wykazania, że europejski portfel tożsamości cyfrowej spełnia wymogi, o których mowa w ust. 1;

b) specyfikacje techniczne, proceduralne, organizacyjne i operacyjne dotyczące wyznaczania jednostek oceniających zgodność, o których mowa w ust. 1, oraz – w odniesieniu do wymogów dotyczących certyfikacji ustanowionych zgodnie z lit. aaa) – dotyczące monitorowania i przeglądu programów certyfikacji i powiązanych metod oceny stosowanych przez te jednostki oraz wydawanych przez nie certyfikatów i sprawozdań z certyfikacji.

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

6. Akty wykonawcze, o których mowa w ust. 4, przyjmuje się zgodnie z procedurą sprawdzającą, o której mowa w art. 48 ust. 2.

Artykuł 6d

Publikacja wykazu certyfikowanych europejskich portfeli tożsamości cyfrowej

1. Państwa członkowskie bez zbędnej zwłoki informują Komisję o europejskich portfelach tożsamości cyfrowej, które zostały zapewnione zgodnie z art. 6a i certyfikowane przez organy, o których mowa w art. 6c ust. 1. Bez zbędnej zwłoki informują również Komisję o odwołaniu certyfikacji.

2. Na podstawie otrzymanych informacji Komisja sporządza, publikuje i aktualizuje wykaz certyfikowanych europejskich portfeli tożsamości cyfrowej sporządzony w formacie nadającym się do odczytu maszynowego.

3. W terminie 6 miesięcy od wejścia w życie niniejszego rozporządzenia Komisja określa formaty i procedury mające zastosowanie do celów ust. 1 i 2 w drodze aktu wykonawczego dotyczącego wdrożenia europejskich portfeli tożsamości cyfrowej, o których mowa w art. 6a ust. 11. Wspomniany akt wykonawczy przyjmuje się zgodnie z procedurą sprawdzającą, o której mowa w art. 48 ust. 2.

Artykuł 6da

Naruszenie bezpieczeństwa europejskich portfeli tożsamości cyfrowej

1. W przypadku gdy nastąpi naruszenie lub częściowa kompromitacja europejskich portfeli tożsamości cyfrowej zapewnionych na podstawie art. 6a lub mechanizmów walidacji, o których mowa w art. 6a ust. 5 lit. a), d) lub e), mające wpływ na wiarygodność tych portfeli i mechanizmów lub na wiarygodność innych europejskich portfeli tożsamości cyfrowej, wydawca portfeli, których to dotyczy, bez zbędnej zwłoki zawiesza wydawanie i używanie europejskiego portfela tożsamości cyfrowej. Państwo członkowskie, w którym zapewniono portfele, których to dotyczy, bez zbędnej zwłoki informuje o tym państwa członkowskie i Komisję. Wydawca portfeli, których to dotyczy, lub dane państwo członkowskie odpowiednio informują strony ufające i użytkowników.

2. W przypadku usunięcia naruszenia lub kompromitacji, o których mowa w ust. 1, wydawca danego portfela przywraca wydawanie i używanie europejskiego portfela tożsamości cyfrowej. Państwo członkowskie, w którym zapewniono portfele, których to dotyczy, bez zbędnej zwłoki informuje o tym państwa członkowskie i Komisję. Wydawca portfeli, których to dotyczy, lub dane państwo członkowskie bez zbędnej zwłoki odpowiednio informują strony ufające i użytkowników.

3. Jeżeli naruszenie lub kompromitacja, o których mowa w ust. 1, nie zostaną usunięte w ciągu trzech miesięcy od zawieszenia, dane państwo członkowskie wycofuje dany europejski portfel tożsamości cyfrowej oraz odpowiednio powiadamia pozostałe państwa członkowskie i Komisję. W przypadku gdy jest to uzasadnione wagą naruszenia, dany europejski portfel tożsamości cyfrowej wycofuje się bez zbędnej zwłoki.

4. Komisja bez zbędnej zwłoki publikuje w *Dzienniku Urzędowym Unii Europejskiej* odpowiednie zmiany w wykazie, o którym mowa w art. 6d.

5. W terminie 6 miesięcy od wejścia w życie niniejszego rozporządzenia Komisja doprecyzuje środki, o których mowa w ust. 1, 2 i 3, w drodze aktu wykonawczego dotyczącego wdrożenia europejskich portfeli tożsamości cyfrowej, o którym to akcie mowa w art. 6a ust. 11. Wspomniany akt wykonawczy przyjmuje się zgodnie z procedurą sprawdzającą, o której mowa w art. 48 ust. 2.

Artykuł 6db

Transgraniczne poleganie na europejskich portfelach tożsamości cyfrowej

1. Jeżeli państwa członkowskie wymagają identyfikacji elektronicznej przy użyciu środka identyfikacji elektronicznej oraz uwierzytelnienia w celu dostępu do usługi online świadczonej przez podmiot sektora publicznego, akceptują również europejskie portfele tożsamości cyfrowej zapewnione zgodnie z niniejszym rozporządzeniem.

2. W przypadku gdy prywatne strony ufające świadczące usługi, z wyjątkiem mikroprzedsiębiorstw i małych przedsiębiorstw zdefiniowane w zaleceniu Komisji 2003/361/WE, są na mocy prawa krajowego lub unijnego zobowiązane do stosowania silnego uwierzytelniania użytkownika do celów identyfikacji online lub gdy silne uwierzytelnienie użytkownika jest wymagane na mocy zobowiązania umownego, w tym w obszarach transportu, energii, bankowości, usług finansowych, zabezpieczenia społecznego, zdrowia, wody pitnej, usług pocztowych, infrastruktury cyfrowej, edukacji lub telekomunikacji, prywatne strony ufające nie później niż 12 miesięcy od daty zapewnienia europejskich portfeli tożsamości cyfrowej zgodnie z art. 6a ust. 1 i wyłącznie na dobrowolny wniosek użytkownika, akceptują również używanie europejskich portfeli tożsamości cyfrowej zapewnionych zgodnie z niniejszym rozporządzeniem w odniesieniu do minimalnych danych niezbędnych do celów konkretnej usługi online, w odniesieniu do której żądane jest uwierzytelnienie użytkownika.

3. W przypadku gdy bardzo duże platformy internetowe zdefiniowane w art. 25 ust. 1 rozporządzenia [odniesienie do rozporządzenia w sprawie aktu o usługach cyfrowych] wymagają uwierzytelniania użytkowników do celów dostępu do usług online, akceptują one również używanie europejskich portfeli tożsamości cyfrowej zapewnionych zgodnie z niniejszym rozporządzeniem do celów uwierzytelnienia użytkownika, wyłącznie na podstawie dobrowolnego wniosku użytkownika i w odniesieniu do minimalnych atrybutów konkretnej usługi online, w odniesieniu do której żądane jest uwierzytelnienie.

4. We współpracy z państwami członkowskimi Komisja wspiera i ułatwia opracowywanie kodeksów postępowania, aby przyczynić się do szerokiej dostępności i użyteczności europejskich portfeli tożsamości cyfrowej objętych zakresem niniejszego rozporządzenia. Te kodeksy postępowania ułatwiają akceptację środków identyfikacji elektronicznej, w tym europejskich portfeli tożsamości cyfrowej objętych zakresem niniejszego rozporządzenia, w szczególności przez dostawców usług korzystających z usług identyfikacji elektronicznej świadczonych przez strony trzecie do celów uwierzytelniania użytkownika. Komisja ułatwi opracowanie takich kodeksów postępowania w ścisłej współpracy ze wszystkimi odpowiednimi zainteresowanymi stronami i zachęci dostawców usług do ukończenia prac nad kodeksami postępowania w terminie 12 miesięcy od daty przyjęcia niniejszego rozporządzenia, a także do ich skutecznego wdrożenia w terminie 18 miesięcy od daty przyjęcia niniejszego rozporządzenia.

5. W terminie 24 miesięcy od uruchomienia europejskich portfeli tożsamości cyfrowej Komisja ocenia, czy na podstawie dowodów ukazujących popyt na europejskie portfele tożsamości cyfrowej oraz ich dostępność i używalność należy zobowiązać dodatkowych prywatnych dostawców usług online do akceptowania wykorzystywania europejskich portfeli tożsamości cyfrowej wyłącznie na podstawie dobrowolnego wniosku użytkownika. Kryteria oceny obejmują zakres bazy użytkowników, transgraniczną obecność dostawców usług, rozwój technologiczny, zmiany sposobów użytkowania oraz popyt ze strony konsumentów.

8) przed art. 7 dodaje się następujący nagłówek:

„SEKCJA II

SYSTEMY IDENTYFIKACJI ELEKTRONICZNEJ”;

9) w art. 7 formuła wprowadzająca otrzymuje brzmienie:

„Zgodnie z art. 9 ust. 1 państwa członkowskie, które jeszcze tego nie uczyniły, notyfikują w terminie 24 miesięcy od wejścia w życie aktów wykonawczych, o których mowa w art. 6a ust. 11 i art. 6c ust. 4, co najmniej jeden system identyfikacji elektronicznej obejmujący co najmniej jeden środek identyfikacji o wysokim poziomie bezpieczeństwa. System identyfikacji elektronicznej kwalifikuje się do notyfikowania zgodnie z art. 9 ust. 1, jeżeli spełnione zostaną wszystkie następujące warunki:”;

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

„2. Komisja publikuje w *Dzienniku Urzędowym Unii Europejskiej* wykaz systemów identyfikacji elektronicznej, które zostały notyfikowane zgodnie z ust. 1 niniejszego artykułu, oraz podstawowe informacje na ich temat.

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

12) dodaje się art. 11a w brzmieniu:

„*Artykuł 11a*

Dopasowywanie rekordów

1. W przypadku gdy notyfikowane środki identyfikacji elektronicznej lub europejskie portfele tożsamości cyfrowej są używane do celów uwierzytelniania, państwa członkowskie, działając jako strony ufające, zapewniają dopasowywanie rekordów.

2. Do celów zapewniania europejskich portfeli tożsamości cyfrowej państwa członkowskie włączają do minimalnego zbioru danych identyfikujących osobę, o którym mowa w art. 12 ust. 4 lit. d), co najmniej jeden unikalny i trwały identyfikator zgodny z prawem Unii i prawem krajowym w celu identyfikacji użytkownika na jego wniosek w przypadkach, gdy identyfikacja użytkownika jest wymagana przepisami prawa.

2a. Państwa członkowskie przewidują środki techniczne i organizacyjne w celu zapewnienia wysokiego poziomu ochrony danych osobowych wykorzystywanych do dopasowywania rekordów i w celu zapobiegania profilowaniu użytkowników.

2aa. Państwa członkowskie mogą postanowić, zgodnie z prawem krajowym, że użytkownik europejskiego portfela tożsamości cyfrowej może zażądać, aby unikalny i trwały identyfikator włączony do minimalnego zbioru danych identyfikujących osobę i powiązany z portfelem zgodnie z art. 6a ust. 4 lit. e) został zastąpiony innym unikalnym i trwałym identyfikatorem wydanym przez państwo członkowskie.

3. W terminie 6 miesięcy od wejścia w życie niniejszego rozporządzenia Komisja doprecyzuje środki, o których mowa w ust. 1, w drodze aktu wykonawczego Ten akt wykonawczy przyjmuje się zgodnie z procedurą sprawdzającą, o której mowa w art. 48 ust. 2.

3a. W terminie 6 miesięcy od wejścia w życie niniejszego rozporządzenia Komisja określi szczegółowo środki, o których mowa w ust. 2 i 2aa, w drodze aktu wykonawczego. Ten akt wykonawczy przyjmuje się zgodnie z procedurą sprawdzającą, o której mowa w art. 48 ust. 2.”;

13) w art. 12 wprowadza się następujące zmiany:

Współpraca i interoperacyjność

a) w ust. 3 uchyla się lit. d);

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

„d) odniesienie do minimalnego zbioru danych identyfikujących osobę niezbędnych do unikalnego i trwałego reprezentowania osoby fizycznej, osoby prawnej lub osoby fizycznej reprezentującej osoby fizyczne lub prawne;”;

ba) w ust. 5 dodaje się lit. c) w brzmieniu:

„c) podobne podejście do usług online akceptujących używanie europejskich portfeli tożsamości cyfrowej zapewnianych zgodnie z niniejszym rozporządzeniem;”;

c) w ust. 6 lit. a) otrzymuje brzmienie:

„a) wymianę informacji, doświadczeń i dobrych praktyk w zakresie systemów identyfikacji elektronicznej, a w szczególności wymogów technicznych związanych z interoperacyjnością, dopasowywaniem rekordów i poziomami bezpieczeństwa;”;

ca) w ust. 6 dodaje się lit. e) w brzmieniu:

„e) wymianę informacji, doświadczeń i dobrych praktyk oraz wydawanie wytycznych dotyczących sposobu projektowania, rozwijania i wdrażania usług online polegających na europejskich portfelach cyfrowych.”;

14) dodaje się art. 12a i 12b w brzmieniu:

„*Artykuł 12a*

Certyfikacja systemów identyfikacji elektronicznej

1. Zgodność notyfikowanych systemów identyfikacji elektronicznej z wymogami określonymi w niniejszym rozporządzeniu podlega certyfikacji w celu wykazania, że systemy takie lub ich części spełniają wymogi określone w art. 8 ust. 2 dotyczące poziomów bezpieczeństwa systemów identyfikacji elektronicznej, w ramach odpowiedniego programu certyfikacji cyberbezpieczeństwa na podstawie rozporządzenia (UE) 2019/881 lub części programu certyfikacji, o ile certyfikat cyberbezpieczeństwa lub jego części obejmują wymogi określone w art. 8 ust. 2 dotyczące poziomów bezpieczeństwa systemów identyfikacji elektronicznej. Certyfikacja nie może przekraczać pięciu lat i podlega warunkowi przeprowadzania, co dwa lata, oceny podatności na zagrożenia. W przypadku gdy zostaną stwierdzone podatności na zagrożenia i nie zostaną one naprawione w terminie trzech miesięcy, certyfikacja zostaje odwołana.

   Certyfikacji dokonują akredytowane publiczne lub prywatne jednostki oceniające zgodność wyznaczone przez państwa członkowskie zgodnie z rozporządzeniem (WE) nr 765/2008.

2. Wzajemna ocena systemów identyfikacji elektronicznej, o której mowa w art. 12 ust. 6 lit. c), nie ma zastosowania do systemów identyfikacji elektronicznej certyfikowanych zgodnie z ust. 1 ani do części takich systemów.

2a. Niezależnie od ust. 2 niniejszego artykułu państwa członkowskie mogą zwrócić się do notyfikującego państwa członkowskiego o dodatkowe informacje na temat systemów identyfikacji elektronicznej lub ich części, certyfikowanych zgodnie z ust. 2 niniejszego artykułu.

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

Artykuł 12b

Dostęp do funkcji sprzętu i oprogramowania

Wydawcy europejskich portfeli tożsamości cyfrowej i wydawcy notyfikowanych środków identyfikacji elektronicznej działający w celach handlowych lub zawodowych i korzystający z podstawowych usług platformowych zdefiniowanych w art. 2 pkt 2 rozporządzenia (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 identyfikacji elektronicznej są użytkownikami biznesowymi zgodnie z art. 2 pkt 21 rozporządzenia (UE) 2022/1925.”;

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

„1. Niezależnie od ust. 2 niniejszego artykułu, dostawcy usług zaufania są odpowiedzialni za szkody wyrządzone w sposób zamierzony lub z powodu zaniedbania osobie fizycznej lub prawnej w związku z niewypełnieniem obowiązków określonych w niniejszym rozporządzeniu.

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

Domniemywa się zamiar lub zaniedbanie kwalifikowanego dostawcy usług zaufania, chyba że kwalifikowany dostawca usług zaufania udowodni, że szkoda, o której mowa w akapicie pierwszym, nie powstała z powodu zamierzonego działania lub zaniedbania tego kwalifikowanego dostawcy usług zaufania.

18) art. 14 otrzymuje brzmienie:

„*Artykuł 14*

Aspekty międzynarodowe

1. Usługi zaufania świadczone przez dostawców usług zaufania mających siedzibę w państwie trzecim lub przez organizację międzynarodową są uznawane 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 na mocy decyzji wykonawczej lub umowy zawartej między Unią a danym państwem trzecim lub organizacją międzynarodową zgodnie z art. 218 Traktatu.

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

   Umowy, o których mowa w ust. 1, zapewniają, by 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 państwie trzecim lub przez organizacje międzynarodowe, z którymi zawarta została umowa.

3. Decyzje wykonawcze, o których mowa w ust. 1, przyjmuje się zgodnie z procedurą sprawdzającą, o której mowa w art. 48 ust. 2.

19) art. 15 otrzymuje brzmienie:

„*Artykuł 15*

Dostępność dla osób z niepełnosprawnościami

Świadczenie usług zaufania i produkty przeznaczone dla użytkownika końcowego stosowane do świadczenia tych usług są dostępne dla osób z niepełnosprawnościami zgodnie z wymogami dostępności określonymi w dyrektywie (UE) 2019/882 w sprawie wymogów dostępności produktów i usług.”;

20) w art. 17 wprowadza się następujące zmiany:

a) w ust. 4 wprowadza się następujące zmiany:

1) ust. 4 lit. c) otrzymuje brzmienie:

„c) informowanie odpowiednich właściwych organów krajowych zainteresowanego państwa członkowskiego wyznaczonych zgodnie z dyrektywą (UE) XXXX/XXXX [dyrektywą NIS 2] o wszelkich istotnych naruszeniach bezpieczeństwa lub utracie integralności, o których otrzyma informacje w ramach wykonywania swoich obowiązków. W przypadku gdy naruszenie bezpieczeństwa lub utrata integralności dotyczy innych państw członkowskich, organ nadzoru powiadamia pojedynczy punkt kontaktowy zainteresowanego państwa członkowskiego wyznaczony zgodnie z dyrektywą (UE) XXXX/XXXX [dyrektywą NIS 2] oraz organy nadzoru wyznaczone zgodnie z art. 17 niniejszego rozporządzenia w tych innych zainteresowanych państwach członkowskich. Zawiadomiony organ nadzoru podaje zaistniałe fakty do wiadomości publicznej lub nakłada taki obowiązek na dostawcę usług zaufania, w przypadku gdy uzna, że ujawnienie naruszenia bezpieczeństwa lub utraty integralności leży w interesie publicznym;”;

2) lit. f) otrzymuje brzmienie:

„f) współpracę z właściwymi organami nadzorczymi ustanowionymi na mocy rozporządzenia (UE) 2016/679, w szczególności przez informowanie ich, bez zbędnej zwłoki, w przypadku gdy wydaje się, że naruszone zostały przepisy dotyczące ochrony danych osobowych, a także o naruszeniach bezpieczeństwa, które wydają się stanowić, naruszenie ochrony danych osobowych;”;

b) ust. 6 otrzymuje brzmienie:

„6. Do dnia 31 marca każdego roku każdy organ nadzoru przekazuje Komisji sprawozdanie z jego głównych działań w poprzednim roku kalendarzowym.”;

c) ust. 8 otrzymuje brzmienie:

„8. W terminie 12 miesięcy od wejścia w życie niniejszego rozporządzenia Komisja przyjmuje wytyczne dotyczące wykonywania przez organy nadzoru zadań, o których mowa w ust. 4, oraz określa, w drodze aktów wykonawczych przyjętych zgodnie z procedurą sprawdzającą, o której mowa w art. 48 ust. 2, formaty i procedury dotyczące sprawozdania, o którym mowa w ust. 6.”;

21) w art. 18 wprowadza się następujące zmiany:

a) tytuł art. 18 otrzymuje brzmienie:

„Wzajemna pomoc i współpraca”;

b) ust. 1 otrzymuje brzmienie:

„1. Organy nadzoru prowadzą współpracę, w ramach której wymieniają się dobrymi praktykami oraz informacjami na temat świadczenia usług zaufania.”;

c) dodaje się ust. 4 i 5 w brzmieniu:

„4. Organy nadzoru i właściwe organy krajowe na podstawie dyrektywy Parlamentu Europejskiego i Rady (UE) XXXX/XXXX [dyrektywy NIS 2] prowadzą współpracę i udzielają sobie wzajemnie pomocy w celu zapewnienia, aby dostawcy usług zaufania spełniali wymogi określone w niniejszym rozporządzeniu i w dyrektywie (UE) XXXX/XXXX [dyrektywie NIS 2]. Organy nadzoru zwracają się do właściwych organów krajowych na podstawie dyrektywy (UE) XXXX/XXXX [dyrektywy NIS 2] o przeprowadzenie działań nadzorczych w celu zweryfikowania spełniania przez dostawców usług zaufania wymogów określonych w dyrektywie (UE) XXXX/XXXX [dyrektywie NIS 2], o nałożenie wymogu, aby dostawcy usług zaufania eliminowali wszelkie przypadki niespełnienia tych wymogów, o terminowe przekazywanie wyników wszelkich działań nadzorczych związanych z dostawcami usług zaufania oraz o informowanie organów nadzoru o istotnych incydentach zgłaszanych zgodnie z dyrektywą (UE) XXXX/XXXX [dyrektywą NIS 2].

5. W terminie 12 miesięcy od wejścia w życie niniejszego rozporządzenia Komisja w drodze aktów wykonawczych ustanawia niezbędne warunki proceduralne ułatwiania współpracy między organami nadzoru, o których mowa w ust. 1. Te akty wykonawcze przyjmuje się zgodnie z procedurą sprawdzającą, o której mowa w art. 48 ust. 2.”;

21a) dodaje się art. 19a w brzmieniu:

„Wymogi dla niekwalifikowanych dostawców usług zaufania

1. Niekwalifikowany dostawca usług zaufania świadczący niekwalifikowane usługi zaufania:

a) stosuje odpowiednie polityki i wprowadza stosowne środki w celu zarządzania ryzykiem prawnym, biznesowym, operacyjnym oraz innym bezpośrednim lub pośrednim rodzajem ryzyka dla świadczenia niekwalifikowanej usługi zaufania. Niezależnie od przepisów art. 18 dyrektywy (UE) XXXX/XXXX [dyrektywy NIS 2] środki te obejmują co najmniej następujące elementy:

(i) środki związane z procedurami rejestracji i onboardingu do usługi;

(ii) środki związane z kontrolami proceduralnymi lub administracyjnymi;

(iii) środki związane z zarządzaniem usługami i ich wdrażaniem;

b) bez zbędnej zwłoki, a w każdym razie nie później niż w terminie 24 godzin od otrzymania informacji o wszelkich naruszeniach lub zakłóceniach w świadczeniu usługi lub we wdrażaniu środków, o których mowa w lit. a) ppkt (i), (ii) i (iii), mających znaczący wpływ na świadczoną usługę zaufania lub na przetwarzane w jej ramach dane osobowe, powiadamiają organ nadzoru, możliwe do zidentyfikowania osoby fizyczne, których to dotyczy, oraz opinię publiczną, jeżeli leży to w interesie publicznym, oraz, w stosownych przypadkach, inne odpowiednie właściwe organy.

2. W terminie 12 miesięcy od wejścia w życie niniejszego rozporządzenia Komisja w drodze aktów wykonawczych określa charakterystykę techniczną środków, o których mowa w ust. 1 lit. a). Te akty wykonawcze przyjmuje się zgodnie z procedurą sprawdzającą, o której mowa w art. 48 ust. 2.”;

22) w art. 20 wprowadza się następujące zmiany:

a) ust. 1 otrzymuje brzmienie:

„1. Kwalifikowani dostawcy usług zaufania podlegają audytowi, na ich własny koszt co najmniej raz na 24 miesiące, przeprowadzanemu przez jednostkę oceniającą zgodność. W ramach audytu potwierdza się, czy kwalifikowani dostawcy usług zaufania oraz świadczone przez nich kwalifikowane usługi zaufania spełniają wymogi określone w niniejszym rozporządzeniu oraz w art. 18 dyrektywy (UE) XXXX/XXXX [dyrektywy NIS 2]. Kwalifikowani dostawcy usług zaufania przedkładają powstały w ten sposób raport z oceny zgodności organowi nadzoru w terminie trzech dni roboczych od jego otrzymania.”;

aa) dodaje się ustęp w brzmieniu:

„1a. Państwa członkowskie mogą postanowić, że kwalifikowani dostawcy usług zaufania informują z wyprzedzeniem organ nadzoru o planowanych audytach i umożliwiają organowi nadzoru, na jego wniosek, udział w charakterze obserwatora.”;

b) w ust. 2 ostatnie zdanie otrzymuje brzmienie:

„W przypadku gdy wydaje się, że zostały naruszone przepisy dotyczące ochrony danych, organ nadzoru informuje, bez zbędnej zwłoki, organy nadzorcze właściwe na podstawie rozporządzenia (UE) 2016/679.”;

c) ust. 3 i 4 otrzymują brzmienie:

„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, przypadków niespełnienia wymogów.

Jeżeli dostawca ten nie wyeliminuje przypadków niespełnienia wymogów, w stosownych przypadkach w terminie ustalonym przez organ nadzoru, organ nadzoru, biorąc pod uwagę w szczególności zakres, czas trwania i skutki tego niespełnienia wymogów, może odebrać status kwalifikowany temu dostawcy lub świadczonej przez niego usłudze, której to dotyczy.

3a. Jeżeli organ nadzoru został poinformowany przez właściwe organy krajowe na podstawie dyrektywy XXXX/XXXX [NIS2], że kwalifikowany dostawca usług zaufania nie spełnia któregokolwiek z wymogów określonych w art. 18 dyrektywy (UE) XXXX/XXXX [NIS2], organ nadzoru, biorąc pod uwagę w szczególności zakres, czas trwania i skutki tego niespełnienia wymogów, może odebrać status kwalifikowany temu dostawcy lub świadczonej przez niego usłudze, której to dotyczy.

3b. Jeżeli organ nadzoru został poinformowany przez organy nadzorcze na podstawie rozporządzenia (EU) 2016/679, że kwalifikowany dostawca usług zaufania nie spełnia któregokolwiek z wymogów określonych w rozporządzeniu (UE) 2016/679, organ nadzoru, biorąc pod uwagę w szczególności zakres, czas trwania i skutki tego niespełnienia wymogów, może odebrać 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, o którym mowa w art. 22 ust. 3, do celów zaktualizowania zaufanych list, o których mowa w art. 22 ust. 1, oraz właściwy organ krajowy, o którym mowa w dyrektywie XXXX [NIS2].

4. W terminie 12 miesięcy od wejścia w życie niniejszego rozporządzenia Komisja w drodze aktów wykonawczych ustanawia specyfikacje techniczne oraz numery referencyjne norm w odniesieniu do:

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

b) wymogów audytów, zgodnie z którymi jednostki oceniające zgodność przeprowadzają oceny zgodności 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.”;

23) w art. 21 wprowadza się następujące zmiany:

„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 i w art. 18 dyrektywy (UE) XXXX/XXXX [NIS2].”;

a) ust. 2 otrzymuje brzmienie:

„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 i świadczonych przez nich kwalifikowanych usług zaufania.

W celu zweryfikowania zgodności dostawcy usług zaufania z wymogami określonymi w art. 18 dyrektywy (UE) XXXX [NIS 2] organ nadzoru zwraca się do właściwych organów, o których mowa w dyrektywie (UE) XXXX [NIS 2], o przeprowadzenie działań nadzorczych w tym zakresie oraz o udzielenie informacji na temat wyniku tych działań bez zbędnej zwłoki i nie później niż w terminie dwóch miesięcy od otrzymania tego wniosku przez właściwe organy, o których mowa w dyrektywie XXXX [NIS2]. Jeżeli weryfikacja nie została zakończona w terminie dwóch miesięcy od zgłoszenia, organy właściwe, o których mowa w dyrektywie XXXX [NIS2], informują organ nadzoru o przyczynach opóźnienia oraz podają termin, w którym weryfikacja zostanie 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 dostawcy 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.

Jeżeli weryfikacja nie została zakończona w terminie trzech miesięcy od zgłoszenia, organ nadzoru informuje dostawcę usług zaufania o przyczynach opóźnienia oraz podaje termin, w którym weryfikacja zostanie zakończona.”;

b) ust. 4 otrzymuje brzmienie:

„4. W terminie 12 miesięcy od wejścia w życie niniejszego rozporządzenia Komisja w drodze aktów wykonawczych określa formaty i procedury zgłaszania i weryfikacji na potrzeby ust. 1 i 2. Te akty wykonawcze przyjmuje się zgodnie z procedurą sprawdzającą, o której mowa w art. 48 ust. 2.”;

25) 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 i, w stosownym przypadku, wszelkie specjalne atrybuty osoby fizycznej lub prawnej, której zostanie wydany kwalifikowany certyfikat lub kwalifikowane elektroniczne poświadczenie atrybutów.

Informacje, o których mowa w akapicie pierwszym, są weryfikowane przez kwalifikowanego dostawcę usług zaufania albo bezpośrednio, albo polegając na stronie trzeciej, w którykolwiek z następujących sposobów:

a) przy użyciu 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 kwalifikowanych elektronicznych poświadczeń atrybutów lub 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) przez fizyczną obecność osoby fizycznej lub upoważnionego przedstawiciela osoby prawnej, za pomocą odpowiednich procedur oraz zgodnie z prawem krajowym.”;

b) dodaje się ust. 1a w brzmieniu:

„1a. W terminie 12 miesięcy od wejścia w życie niniejszego rozporządzenia Komisja w drodze aktów wykonawczych określa minimalne specyfikacje techniczne, normy i procedury w odniesieniu do weryfikacji tożsamości i atrybutów zgodnie z ust. 1 lit. c). Te akty wykonawcze przyjmuje się zgodnie z procedurą sprawdzającą, o której mowa w art. 48 ust. 2.”;

c) w ust. 2 wprowadza się następujące zmiany:

0) w lit. a) wprowadza się następujące zmiany:

„a) informuje organ nadzoru z co najmniej miesięcznym wyprzedzeniem o wprowadzeniu jakiejkolwiek zmiany w świadczeniu przez niego kwalifikowanych usług zaufania lub z co najmniej trzymiesięcznym wyprzedzeniem – o zamiarze zaprzestania tej działalności. Organ nadzoru może zażądać dodatkowych informacji lub wyników oceny zgodności przed udzieleniem zezwolenia na wdrożenie planowanych zmian w kwalifikowanych usługach zaufania. Jeżeli weryfikacja nie została zakończona w terminie trzech miesięcy od zgłoszenia, organ nadzoru informuje dostawcę usług zaufania o przyczynach opóźnienia oraz podaje termin, w którym weryfikacja zostanie zakończona;”;

1) lit. d) i e) otrzymują brzmienie:

„d) przed wejściem w stosunek umowny informuje w jasny, szczegółowy i łatwo dostępny sposób w przestrzeni publicznej oraz indywidualnie wszystkie osoby pragnące 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 bezpieczeństwo techniczne i wiarygodność procesów przez nie obsługiwanych, w tym przy użyciu odpowiednich algorytmów kryptograficznych, długości kluczy i funkcji skrótu w systemach, produktach i procesach przez nie obsługiwanych;”;

2) dodaje się nowe lit. fa) i fb) w brzmieniu:

„fa) stosuje odpowiednie polityki i wprowadza stosowne środki w celu zarządzania ryzykiem prawnym, biznesowym, operacyjnym oraz każdym innym bezpośrednim lub pośrednim rodzajem ryzyka dla świadczenia kwalifikowanej usługi zaufania. Niezależnie od przepisów art. 18 dyrektywy (UE) XXXX/XXXX [dyrektywy NIS 2] środki te obejmują co najmniej następujące elementy:

(i) środki związane z procedurami rejestracji i onboardingu do usługi;

(ii) środki związane z kontrolami proceduralnymi lub administracyjnymi;

(iii) środki związane z zarządzaniem usługami i ich wdrażaniem;

fb) bez zbędnej zwłoki, a w każdym razie nie później niż w terminie 24 godzin od wystąpienia incydentu, zawiadamia 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 lub zakłóceniach w świadczeniu usługi lub we wdrażaniu środków, o których mowa w lit. fa) ppkt (i), (ii) i (iii), mających znaczący wpływ na świadczoną usługę zaufania lub na przetwarzane w jej ramach dane osobowe;";

3) lit. g) i h) otrzymują brzmienie:

„g) podejmuje 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, wszelkie odpowiednie informacje dotyczące danych wydanych i otrzymanych przez kwalifikowanego dostawcę usług zaufania, do celów przedstawienia dowodów w postępowaniach sądowych i do celów zapewnienia ciągłości usług. Informacje mogą być przechowywane w formie elektronicznej;";

4) uchyla się lit. j);

d) dodaje się ust. 4a w brzmieniu:

„4a. Ust. 3 i 4 stosuje się odpowiednio do unieważniania elektronicznych poświadczeń atrybutów.";

e) ust. 5 otrzymuje brzmienie:

„5. W terminie 12 miesięcy od wejścia w życie niniejszego rozporządzenia Komisja w drodze aktów wykonawczych ustanawia specyfikacje techniczne, procedury oraz numery referencyjne norm w odniesieniu do wymogów, o których mowa w ust. 2. W przypadku spełnienia wymogów tych specyfikacji technicznych, procedur i norm, 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.”;

f) dodaje się ust. 6 w brzmieniu:

„6. Komisja jest uprawniona do przyjęcia aktów wykonawczych określających charakterystykę techniczną środków, o których mowa w ust. 2 lit. fa).”;

25a) w art. 26 wprowadza się następujące zmiany:

„2. W terminie 12 miesięcy od wejścia w życie niniejszego rozporządzenia Komisja w drodze aktów wykonawczych ustanawia specyfikacje techniczne oraz numery referencyjne norm w odniesieniu do zaawansowanych podpisów elektronicznych. W przypadku gdy zaawansowany podpis elektroniczny spełnia wymogi tych specyfikacji i norm, 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.”;

25b) w art. 27 wprowadza się następujące zmiany:

uchyla się ust. 4.

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

„6. W terminie 12 miesięcy od wejścia w życie niniejszego rozporządzenia Komisja w drodze aktów wykonawczych ustanawia specyfikacje techniczne oraz numery referencyjne norm w odniesieniu do kwalifikowanych certyfikatów podpisów elektronicznych. W przypadku gdy kwalifikowany certyfikat podpisu elektronicznego spełnia wymogi tych specyfikacji i norm, 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 nowy ust. 1a w brzmieniu:

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

28) dodaje się art. 29a w brzmieniu:

„*Artykuł 29a*

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

1. Zarządzaniem kwalifikowanymi urządzeniami do składania podpisu elektronicznego na odległość jako usługą kwalifikowaną może zajmować się 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 może kopiować 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 przekracza minimum niezbędnego do zapewnienia ciągłości usługi;

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

2. W terminie 12 miesięcy od wejścia w życie niniejszego rozporządzenia Komisja w drodze aktów wykonawczych ustanawia specyfikacje techniczne oraz numery referencyjne norm do celów ust. 1.”;

29) w art. 30 dodaje się ust. 3a w brzmieniu:

„3a. Ważność certyfikacji, o której mowa w ust. 1, wynosi pięć lat, pod warunkiem że regularnie, co dwa lata, przeprowadza się ocenę podatności na zagrożenia. W przypadku gdy zostaną stwierdzone podatności na zagrożenia i nie zostaną one naprawione, certyfikacja zostaje odwołana.”;

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

„3. W terminie 12 miesięcy od wejścia w życie niniejszego rozporządzenia Komisja w drodze aktów wykonawczych określa formaty i procedury mające zastosowanie na potrzeby ust. 1. 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:

„Jeżeli walidacja kwalifikowanych podpisów elektronicznych spełnia wymogi specyfikacji i norm, o których mowa w ust. 3, domniemywa się zgodność z wymogami określonymi w akapicie pierwszym.”;

b) ust. 3 otrzymuje brzmienie:

„3. W terminie 12 miesięcy od wejścia w życie niniejszego rozporządzenia Komisja w drodze aktów wykonawczych zapewnia specyfikacje i numery referencyjne norm w odniesieniu do walidacji kwalifikowanych podpisów elektronicznych. Te akty wykonawcze przyjmuje się zgodnie z procedurą sprawdzającą, o której mowa w art. 48 ust. 2.”;

31a) dodaje się art. 32a w brzmieniu:

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

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

f) integralność podpisanych danych nie została naruszona;

g) wymogi przewidziane w art. 26 zostały spełnione w momencie składania podpisu. W przypadku gdy walidacja zaawansowanych podpisów elektronicznych spełnia wymogi specyfikacji i norm, o których mowa w ust. 3, domniemywa się zgodność z wymogami określonymi w akapicie pierwszym.

2. System wykorzystany do walidacji zaawansowanego podpisu elektronicznego opartego na kwalifikowanym certyfikacie zapewnia stronie ufającej prawidłowy wynik procesu walidacji i umożliwia stronie ufającej wykrycie wszelkich problemów związanych z bezpieczeństwem.

3. W terminie 12 miesięcy od wejścia w życie niniejszego rozporządzenia Komisja w drodze aktów wykonawczych zapewnia specyfikacje i numery referencyjne norm w odniesieniu do walidacji zaawansowanych podpisów elektronicznych opartych na kwalifikowanych certyfikatach. Te akty wykonawcze przyjmuje się zgodnie z procedurą sprawdzającą, o której mowa w art. 48 ust. 2.”;

31b) w art. 33 wprowadza się następujące zmiany:

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

„2. W terminie 12 miesięcy od wejścia w życie niniejszego rozporządzenia Komisja w drodze aktów wykonawczych ustanawia specyfikacje techniczne oraz numery referencyjne norm w odniesieniu do kwalifikowanych usług walidacji, o których mowa w ust. 1. W przypadku gdy usługa walidacji kwalifikowanych podpisów elektronicznych spełnia wymogi tych specyfikacji i norm, domniemywa się zgodność z wymogami określonymi w ust. 1. Te akty wykonawcze przyjmuje się zgodnie z procedurą sprawdzającą, o której mowa w art. 48 ust. 2.”;

32) art. 34 otrzymuje brzmienie:

„*Artykuł 34*

Kwalifikowana usługa konserwacji kwalifikowanych podpisów elektronicznych

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

2. W przypadku gdy ustalenia w zakresie kwalifikowanej usługi konserwacji kwalifikowanych podpisów elektronicznych spełniają wymogi tych specyfikacji i norm, domniemywa się zgodność z wymogami określonymi w ust. 1.

3. W terminie 12 miesięcy od wejścia w życie niniejszego rozporządzenia Komisja w drodze aktów wykonawczych ustanawia specyfikacje techniczne i numery referencyjne norm w odniesieniu do kwalifikowanej usługi konserwacji kwalifikowanych podpisów elektronicznych. Te akty wykonawcze przyjmuje się zgodnie z procedurą sprawdzającą, o której mowa w art. 48 ust. 2.”;

32a) w art. 36 dodaje się nowy ust. 2 w brzmieniu:

„2. W terminie 12 miesięcy od wejścia w życie niniejszego rozporządzenia Komisja w drodze aktów wykonawczych ustanawia specyfikacje techniczne i numery referencyjne norm w odniesieniu do zaawansowanych pieczęci elektronicznych.

W przypadku gdy zaawansowana pieczęć elektroniczna spełnia wymogi tych specyfikacji i norm, domniemywa się zgodność z wymogami dotyczącymi zaawansowanej pieczęci elektronicznej. Te akty wykonawcze przyjmuje się zgodnie z procedurą sprawdzającą, o której mowa w art. 48 ust. 2.”;

33) w art. 37 wprowadza się następujące zmiany:

uchyla się ust. 4;

34) w art. 38 wprowadza się następujące zmiany:

a) ust. 1 otrzymuje brzmienie:

„1. Kwalifikowane certyfikaty pieczęci elektronicznych muszą spełniać wymogi określone w załączniku III. W przypadku gdy kwalifikowany certyfikat pieczęci elektronicznej spełnia wymogi specyfikacji i norm, o których mowa w ust. 6, domniemywa się zgodność z wymogami określonymi w załączniku III.”;

b) ust. 6 otrzymuje brzmienie:

„6. W terminie 12 miesięcy od wejścia w życie niniejszego rozporządzenia Komisja w drodze aktów wykonawczych ustanawia specyfikacje techniczne i numery referencyjne norm w odniesieniu do kwalifikowanych certyfikatów pieczęci elektronicznych. Te akty wykonawcze przyjmuje się zgodnie z procedurą sprawdzającą, o której mowa w art. 48 ust. 2.”;

35) dodaje się art. 39a w brzmieniu:

„*Artykuł 39a*

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

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

35a) dodaje się art. 40a w brzmieniu:

„*Artykuł 40a*

Wymogi dotyczące walidacji zaawansowanych pieczęci elektronicznych opartych na kwalifikowanych certyfikatach

(1) Art. 32a stosuje się odpowiednio do walidacji zaawansowanych pieczęci elektronicznych opartych na kwalifikowanych certyfikatach.”;

36) w art. 42 wprowadza się następujące zmiany:

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

„1a. W przypadku gdy powiązanie daty i czasu z danymi i precyzyjne źródło czasu spełniają wymogi specyfikacji i norm, o których mowa w ust. 2, domniemywa się zgodność z wymogami określonymi w ust. 1.”;

b) ust. 2 otrzymuje brzmienie:

„2. W terminie 12 miesięcy od wejścia w życie niniejszego rozporządzenia Komisja w drodze aktów wykonawczych ustanawia specyfikacje techniczne i numery referencyjne norm w odniesieniu do 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.”;

36a) w art. 43 dodaje się nowy ust. 3 w brzmieniu:

„2a. Kwalifikowane usługi rejestrowanego doręczenia w jednym państwie członkowskim są uznawane za kwalifikowane usługi rejestrowanego doręczenia w każdym innym państwie członkowskim.”;

37) w art. 44 wprowadza się następujące zmiany:

a) dodaje się ust. 1a w brzmieniu:

„1a. W przypadku gdy proces wysyłania i otrzymywania danych spełnia wymogi specyfikacji i norm, o których mowa w ust. 2, domniemywa się zgodność z wymogami określonymi w ust. 1.”;

b) ust. 2 otrzymuje brzmienie:

„2. W terminie 12 miesięcy od wejścia w życie niniejszego rozporządzenia Komisja w drodze aktów wykonawczych ustanawia specyfikacje techniczne i numery referencyjne norm w odniesieniu do procesów wysyłania i otrzymywania danych. Te akty wykonawcze przyjmuje się zgodnie z procedurą sprawdzającą, o której mowa w art. 48 ust. 2.”;

c) dodaje się ust. 3 i 4 w brzmieniu:

„3. 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. Zgodność ta musi zostać potwierdzona przez jednostkę oceniającą zgodność.

4. Komisja może, w drodze aktu wykonawczego, ustanowić specyfikacje techniczne i numery referencyjne norm w celu ułatwienia przekazywania danych między co najmniej dwoma kwalifikowanymi dostawcami usług zaufania. Specyfikacje techniczne i treść norm muszą charakteryzować się opłacalnością i proporcjonalnością. Ten akt wykonawczy przyjmuje się zgodnie z procedurą sprawdzającą, o której mowa w art. 48 ust. 2.”;

38) 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 wymogami określonymi w załączniku IV przeprowadza się zgodnie ze specyfikacjami i normami, o których mowa w ust. 4.

2. Kwalifikowane certyfikaty uwierzytelniania witryn internetowych, o których mowa w ust. 1, muszą być rozpoznawane przez przeglądarki internetowe. Przeglądarki internetowe zapewniają w tym celu, aby dane dotyczące tożsamości dostarczane przy użyciu którejkolwiek z metod były wyświetlane w sposób przyjazny dla użytkownika. Przeglądarki internetowe zapewniają obsługę kwalifikowanych certyfikatów uwierzytelniania witryn internetowych, o których mowa w ust. 1, oraz interoperacyjność z tymi certyfikatami, z wyjątkiem przedsiębiorstw, które uznaje się za mikroprzedsiębiorstwa i małe przedsiębiorstwa zgodnie z zaleceniem Komisji 2003/361/WE w ciągu pierwszych pięciu lat ich działalności jako dostawców usług przeglądania stron internetowych.

4. W terminie 12 miesięcy od wejścia w życie niniejszego rozporządzenia Komisja w drodze aktów wykonawczych zapewnia specyfikacje oraz numery referencyjne norm w odniesieniu do kwalifikowanych certyfikatów uwierzytelniania witryn internetowych, o których mowa w ust. 1 i 2. Te akty wykonawcze przyjmuje się zgodnie z procedurą sprawdzającą, o której mowa w art. 48 ust. 2.”;

39) po art. 45 dodaje się następujące sekcje 9, 10 i 11:

„SEKCJA 9

ELEKTRONICZNE POŚWIADCZENIE ATRYBUTÓW

Artykuł 45a

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 i 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 formie papierowej.

3. Kwalifikowane elektroniczne poświadczenie atrybutów wydane w jednym państwie członkowskim jest uznawane za kwalifikowane elektroniczne poświadczenie atrybutów w każdym innym państwie członkowskim.

4. Poświadczenie atrybutów wydane przez podmiot sektora publicznego odpowiedzialny za źródło autentyczne lub w jego imieniu jest uznawane za poświadczenie atrybutów wydane przez podmiot sektora publicznego odpowiedzialny za źródło autentyczne lub w jego imieniu we wszystkich państwach członkowskich.

Artykuł 45b

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 ani 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 45c

Wymogi dotyczące kwalifikowanego elektronicznego poświadczenia atrybutów

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

1a. Ocenę zgodności z wymogami określonymi w załączniku V przeprowadza się zgodnie ze specyfikacjami i normami, o których mowa w ust. 4.

2. Kwalifikowane elektroniczne poświadczenia atrybutów nie podlegają żadnym obowiązkowym wymogom wykraczającym poza wymogi określone w załączniku V.

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

4. W terminie 6 miesięcy od wejścia w życie niniejszego rozporządzenia Komisja ustanawia specyfikacje techniczne i numery referencyjne norm w odniesieniu do kwalifikowanych elektronicznych poświadczeń atrybutów w drodze aktu wykonawczego dotyczącego wdrożenia europejskich portfeli tożsamości cyfrowej, o których mowa w art. 6a ust. 11.

Artykuł 45d

Weryfikacja atrybutów na podstawie źródeł autentycznych

1. Państwa członkowskie zapewniają w terminie 24 miesięcy od wejścia w życie aktów wykonawczych, o których mowa w art. 6a ust. 11 i art. 6c ust. 4, aby przynajmniej w odniesieniu do atrybutów wymienionych w załączniku VI, w przypadku gdy atrybuty te polegają na źródłach autentycznych w sektorze publicznym, podjęto działania umożliwiające kwalifikowanym dostawcom elektronicznych poświadczeń atrybutów weryfikację tych atrybutów drogą elektroniczną, na żądanie użytkownika i zgodnie z prawem krajowym lub unijnym.

2. W terminie 6 miesięcy od wejścia w życie niniejszego rozporządzenia, uwzględniając mające zastosowanie normy międzynarodowe, Komisja określa – w drodze aktu wykonawczego dotyczącego wdrożenia europejskich portfeli tożsamości cyfrowej, o których mowa w art. 6a ust. 11 – minimalne specyfikacje techniczne, normy i procedury dotyczące katalogu atrybutów i systemów poświadczania atrybutów i procedur weryfikacji kwalifikowanych elektronicznych poświadczeń atrybutów.

Artykuł 45da

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 spełnia następujące wymogi:

a) wymogi określone w załączniku VII;

b) kwalifikowany certyfikat potwierdzający kwalifikowany podpis elektroniczny lub kwalifikowaną pieczęć elektroniczną podmiotu sektora publicznego, o którym mowa w art. 3 pkt 45a, zidentyfikowanego jako wydawca, o którym mowa w załączniku VII lit. b), zawiera określony zestaw poświadczonych atrybutów w postaci nadającej się do automatycznego przetwarzania:

(i) wskazanie, że podmiot wydający został ustanowiony zgodnie z prawem krajowym lub unijnym 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 krajowego lub unijnego, o którym mowa w ppkt (i).

2. Państwo członkowskie, w którym mają siedzibę podmioty sektora publicznego, o których mowa w art. 3 pkt 45a, zapewnia, aby podmioty sektora publicznego, które wydają elektroniczne poświadczenia atrybutów, spełniały równoważny poziom wiarygodności co kwalifikowani dostawcy usług zaufania zgodnie z art. 24.

2a. Państwa członkowskie notyfikują Komisji podmioty sektora publicznego, o których mowa w art. 3 pkt 45a. 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 udostępnia publicznie wykaz podmiotów sektora publicznego, o których mowa w ust. 3 pkt 45a, w elektronicznie podpisanej lub opatrzonej pieczęcią elektroniczną postaci nadającej się do automatycznego przetwarzania, używając w tym celu zabezpieczonego kanału komunikacji.

3. Jeżeli elektroniczne poświadczenie atrybutów wydane przez podmiot sektora publicznego odpowiedzialny za źródło autentyczne lub w jego imieniu zostało unieważnione po początkowym wydaniu, traci ono ważność od momentu jego unieważnienia. Po unieważnieniu nie można przywrócić poprzedniego statusu unieważnionego poświadczenia elektronicznego.

4. 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 niniejszego artykułu, jeżeli spełnia ono normy, o których mowa w ust. 5.

5. W terminie 6 miesięcy od wejścia w życie niniejszego rozporządzenia Komisja ustanawia – w drodze aktu wykonawczego dotyczącego wdrożenia europejskich portfeli tożsamości cyfrowej, o których mowa w art. 6a ust. 11 – specyfikacje techniczne i numery referencyjne norm w odniesieniu do elektronicznego poświadczenia atrybutów wydanego przez podmiot sektora publicznego odpowiedzialny za źródło autentyczne lub w jego imieniu.

5a. W terminie 6 miesięcy od wejścia w życie niniejszego rozporządzenia Komisja określa formaty, procedury, specyfikacje i normy do celów ust. 2a w drodze aktu wykonawczego dotyczącego wdrożenia europejskich portfeli tożsamości cyfrowej, o których mowa w art. 6a ust. 11.

6. Podmioty sektora publicznego, o których mowa w art. 3 pkt 45a, wydające elektroniczne poświadczenie atrybutów zapewniają interfejs z europejskimi portfelami tożsamości cyfrowej zapewnianymi zgodnie z art. 6a.

Artykuł 45e

Wydawanie elektronicznych poświadczeń atrybutów do europejskich portfeli tożsamości cyfrowej

Dostawcy kwalifikowanych elektronicznych poświadczeń atrybutów zapewniają interfejs z europejskimi portfelami tożsamości cyfrowej zapewnianymi zgodnie z art. 6a.

Artykuł 45f

Dodatkowe przepisy w odniesieniu do świadczenia usług elektronicznego poświadczania atrybutów

1. Dostawcy kwalifikowanych i niekwalifikowanych usług elektronicznego poświadczania atrybutów nie łączą 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.

4. Dostawcy usług kwalifikowanego elektronicznego poświadczania atrybutów wdrażają rozdział funkcjonalny w celu świadczenia takich usług.

SEKCJA 10

USŁUGI ARCHIWIZACJI ELEKTRONICZNEJ

Artykuł 45g

Skutek prawny usługi archiwizacji elektronicznej

1. Danym elektronicznym przechowywanym przy użyciu usługi archiwizacji 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 przechowywane przy użyciu kwalifikowanej usługi archiwizacji elektronicznej korzystają z domniemania ich integralności i pochodzenia przez cały okres przechowywania przez kwalifikowanego dostawcę usług zaufania.

3. Kwalifikowane usługi archiwizacji elektronicznej w jednym państwie członkowskim są uznawane za kwalifikowane usługi archiwizacji elektronicznej w każdym innym państwie członkowskim.

Artykuł 45ga

Wymogi dotyczące kwalifikowanych usług archiwizacji elektronicznej

1. Kwalifikowane usługi archiwizacji elektronicznej spełniają następujące wymogi:

   a) są świadczone przez kwalifikowanych dostawców usług zaufania;

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

c) zapewniają konserwację danych 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 pobrane z kwalifikowanego archiwum elektronicznego korzystają z domniemania integralności danych od początku okresu konserwacji do momentu pobrania. Raport ten jest przekazywany w sposób niezawodny i efektywny oraz opatrzony jest kwalifikowanym podpisem elektronicznym lub kwalifikowaną pieczęcią elektroniczną dostawcy kwalifikowanej usługi archiwizacji elektronicznej.

2. W terminie 12 miesięcy od wejścia w życie niniejszego rozporządzenia Komisja w drodze aktów wykonawczych ustanawia specyfikacje techniczne i numery referencyjne norm w odniesieniu do kwalifikowanych usług archiwizacji elektronicznej. W przypadku gdy kwalifikowana usługa archiwizacji elektronicznej spełnia wymogi tych specyfikacji i norm, 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 45h

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

3. Kwalifikowany rejestr elektroniczny w jednym państwie członkowskim jest uznawany za kwalifikowany rejestr elektroniczny w każdym innym państwie członkowskim.

Artykuł 45i

Wymogi dotyczące kwalifikowanych rejestrów elektronicznych

1. Kwalifikowane rejestry elektroniczne spełniają następujące wymogi:

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

   b) ustalają pochodzenie rekordów danych w rejestrze;

   c) zapewniają niepowtarzalne sekwencyjne uporządkowanie chronologiczne rekordów 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 spełnia wymogi specyfikacji i norm, o których mowa w ust. 3, domniemywa się zgodność z wymogami określonymi w ust. 1.

3. Komisja w drodze aktów wykonawczych ustanawia specyfikacje techniczne i numery referencyjne norm w odniesieniu do tworzenia i obsługi kwalifikowanych rejestrów elektronicznych. Te akty wykonawcze przyjmuje się zgodnie z procedurą sprawdzającą, o której mowa w art. 48 ust. 2.”;

40) dodaje się art. 48a w brzmieniu:

„*Artykuł 48a*

Wymogi dotyczące sprawozdawczości

1. Państwa członkowskie zapewniają gromadzenie danych statystycznych dotyczących funkcjonowania europejskich portfeli tożsamości cyfrowej od momentu, gdy portfele te są zapewniane na ich terytorium.

2. Dane statystyczne gromadzone 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) zestawienie zawierające dane dotyczące incydentów uniemożliwiających używanie europejskiego portfela tożsamości cyfrowej.

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.”;

41) art. 49 otrzymuje brzmienie:

„*Artykuł 49*

Przegląd

1. Komisja dokona przeglądu stosowania niniejszego rozporządzenia i przekaże sprawozdanie Parlamentowi Europejskiemu i Radzie w terminie 36 miesięcy od jego wejścia w życie. Komisja oceni w szczególności zakres stosowania art. 6 i art. 6db oraz czy należy zmienić zakres stosowania niniejszego rozporządzenia lub jego poszczególnych przepisów, biorąc pod uwagę doświadczenia zdobyte przy stosowaniu niniejszego rozporządzenia, a także popyt ze strony klientów, rozwój technologiczny, sytuację rynkową i prawną. W stosownych przypadkach do sprawozdania dołącza się wniosek dotyczący zmiany niniejszego rozporządzenia.

2. Sprawozdanie z oceny obejmuje ocenę dostępności i używalności europejskich portfeli tożsamości cyfrowej, objętych zakresem niniejszego rozporządzenia, oraz ocenę, czy wszyscy prywatni dostawcy usług online polegający na usługach identyfikacji elektronicznej świadczonych przez strony trzecie do celów uwierzytelniania użytkowników zostaną zobowiązani do akceptowania używania europejskiego portfela tożsamości cyfrowej.

3. Ponadto, co cztery lata po sporządzeniu sprawozdania, o którym mowa w akapicie pierwszym, Komisja przekazuje Parlamentowi Europejskiemu i Radzie sprawozdanie dotyczące postępów w osiąganiu celów niniejszego rozporządzenia.”;

42) 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 mocy niniejszego rozporządzenia przez okres nieprzekraczający 36 miesięcy po wejściu w życie niniejszego rozporządzenia.

2. Kwalifikowane certyfikaty wydane osobom fizycznym na mocy dyrektywy 1999/93/WE w dalszym ciągu uznaje się za kwalifikowane certyfikaty podpisów elektronicznych na mocy niniejszego rozporządzenia do przez okres nieprzekraczający 24 miesięcy po wejściu w życie niniejszego rozporządzenia.

2a. Zarządzanie urządzeniami do składania kwalifikowanych podpisów i pieczęci elektronicznych na odległość przez kwalifikowanych dostawców usług zaufania, innych niż kwalifikowani dostawcy usług zaufania świadczący kwalifikowane usługi zaufania na potrzeby zarządzania urządzeniami do składania kwalifikowanych podpisów i pieczęci elektronicznych na odległość zgodnie z art. 29a i 39a, uznaje się w dalszym ciągu, bez konieczności uzyskania statusu kwalifikowanego do celów świadczenia tych usług zarządzania przez okres nieprzekraczający 24 miesięcy po wejściu w życie niniejszego rozporządzenia.

2b. Kwalifikowani dostawcy usług zaufania, którym na mocy niniejszego rozporządzenia przyznano status kwalifikowany przed dniem [data wejścia w życie rozporządzenia zmieniającego], stosując metody weryfikacji tożsamości do celów wydawania kwalifikowanych certyfikatów zgodnie z art. 24 ust. 1, przedkładają organowi nadzoru raport z oceny zgodności potwierdzający zgodność z art. 24 ust. 1 najszybciej jak to możliwe, ale nie później niż 30 miesięcy po wejściu w życie rozporządzenia zmieniającego. Do czasu przedłożenia takiego raportu z oceny zgodności i zakończenia jego oceny przez organ nadzoru kwalifikowany dostawca usług zaufania może nadal polegać na stosowaniu metod weryfikacji tożsamości określonych w art. 24 ust. 1 rozporządzenia (UE) nr 910/2014.”;

43) w załączniku I wprowadza się zmiany zgodnie z załącznikiem I do niniejszego rozporządzenia;

44) załącznik II zastępuje się tekstem znajdującym się w załączniku II do niniejszego rozporządzenia;

45) w załączniku III wprowadza się zmiany zgodnie z załącznikiem III do niniejszego rozporządzenia;

46) w załączniku IV wprowadza się zmiany zgodnie z załącznikiem IV do niniejszego rozporządzenia;

47) dodaje się nowy załącznik V w brzmieniu określonym w załączniku V do niniejszego rozporządzenia;

48) do niniejszego rozporządzenia dodaje się nowy załącznik VI.

Artykuł 52

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 […] r.

W imieniu Parlamentu Europejskiego W imieniu Rady

Przewodniczący / Przewodnicząca Przewodniczący / Przewodnicząca

ZAŁĄCZNIK I

W załączniku I lit. i) otrzymuje brzmienie:

„i) informacje na temat statusu ważności kwalifikowanego certyfikatu lub miejsce usług, z którego można skorzystać w celu złożenia zapytania o status ważności kwalifikowanego certyfikatu;”.

ZAŁĄCZNIK II

WYMOGI DLA KWALIFIKOWANYCH URZĄDZEŃ DO SKŁADANIA PODPISU ELEKTRONICZNEGO

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

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

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

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

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

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

ZAŁĄCZNIK III

W załączniku III lit. i) otrzymuje brzmienie:

„i) informacje na temat statusu ważności kwalifikowanego certyfikatu lub miejsce usług, z którego można skorzystać w celu złożenia zapytania o status ważności kwalifikowanego certyfikatu;”.

ZAŁĄCZNIK IV

W załączniku IV lit. j) otrzymuje brzmienie:

„j) informacje na temat statusu ważności kwalifikowanego certyfikatu lub miejsce usług statusu ważności certyfikatu, z których można skorzystać w celu złożenia zapytania o status ważności kwalifikowanego certyfikatu.”.

ZAŁĄCZNIK V

WYMOGI DOTYCZĄCE KWALIFIKOWANEGO ELEKTRONICZNEGO POŚWIADCZENIA ATRYBUTÓW

Kwalifikowane elektroniczne poświadczenie atrybutów zawiera:

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

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

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

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

(g) zestaw danych jednoznacznie reprezentujących podmiot, do którego poświadczone atrybuty się odnoszą: jeżeli używany jest pseudonim, fakt ten jest jasno wskazany;

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

(i) dane dotyczące początku i końca okresu ważności poświadczenia;

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

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

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

(m) informacje na temat statusu ważności kwalifikowanego poświadczenia lub miejsce usług, z którego można skorzystać w celu złożenia zapytania o status ważności kwalifikowanego poświadczenia.

ZAŁĄCZNIK VI

MINIMALNY WYKAZ ATRYBUTÓW

Zgodnie z art. 45d państwa członkowskie zapewniają, aby podjęto działania umożliwiające kwalifikowanym dostawcom elektronicznych poświadczeń 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 krajowym lub unijnym oraz jeżeli 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. urzędowe zezwolenia i licencje;
10. dane finansowe i dane dotyczące przedsiębiorstwa.

ZAŁĄCZNIK VII

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

Elektroniczne poświadczenie atrybutów wydane przez podmiot publiczny odpowiedzialny za źródło autentyczne lub w jego imieniu zawiera:

a) wskazanie, co najmniej w postaci nadającej się do automatycznego przetwarzania, że poświadczenie zostało wydane jako elektroniczne poświadczenie atrybutów wydane 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 jego nazwę i, w stosownych przypadkach, jego numer rejestrowy zgodnie z oficjalnym rejestrem;
c) zestaw danych jednoznacznie reprezentujących podmiot, do którego poświadczone atrybuty się odnoszą; jeżeli używany jest pseudonim, fakt ten jest jasno wskazany;
d) poświadczony atrybut lub poświadczone atrybuty, w tym – w stosownych przypadkach – informacje niezbędne do określenia zakresu tych atrybutów;
e) dane dotyczące początku i końca okresu ważności poświadczenia;
f) kod identyfikacyjny poświadczenia, który musi być niepowtarzalny dla wydającego podmiotu publicznego, i 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, z którego można skorzystać w celu złożenia zapytania o status ważności poświadczenia.