Text

ROZPORZĄDZENIE PARLAMENTU EUROPEJSKIEGO I RADY (UE) NR 910/2014

z dnia 23 lipca 2014 r.

w sprawie identyfikacji elektronicznej i usług zaufania w odniesieniu do transakcji elektronicznych na rynku wewnętrznym oraz uchylające dyrektywę 1999/93/WE

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 ([2]),

a także mając na uwadze, co następuje:

(1) Budowanie zaufania do środowiska *online* jest kluczowe dla rozwoju gospodarczego i społecznego. Brak zaufania, spowodowany w szczególności odczuwanym brakiem pewności prawa, sprawia, że konsumenci, przedsiębiorstwa i organy publiczne wahają się, czy przeprowadzać transakcje elektroniczne i wdrażać nowe usługi.

(2) Celem niniejszego rozporządzenia jest zwiększenie zaufania do transakcji elektronicznych na rynku wewnętrznym poprzez zapewnienie wspólnej podstawy bezpiecznej interakcji elektronicznej między obywatelami, przedsiębiorstwami i organami publicznymi, co pozwoli podnieść efektywność publicznych i prywatnych usług *online*, e-biznesu i e-handlu w Unii.

(3) Dyrektywa Parlamentu Europejskiego i Rady 1999/93/WE ([3]) dotyczyła podpisów elektronicznych, nie zapewniając szczegółowych ram transgranicznych i międzysektorowych, które pozwoliłyby na bezpieczne, wiarygodne i łatwe w użyciu transakcje elektroniczne. Niniejsze rozporządzenie umacnia i poszerza dorobek tej dyrektywy.

(4) W komunikacie Komisji z dnia 26 sierpnia 2010 r. zatytułowanym „Europejska agenda cyfrowa” stwierdzono, że rozdrobnienie rynku cyfrowego, brak interoperacyjności i rosnąca cyberprzestępczość stanowią główne przeszkody w pozytywnym cyklu rozwoju gospodarki cyfrowej. W sprawozdaniu na temat obywatelstwa UE z 2010 r. zatytułowanym „Usuwanie przeszkód w zakresie praw obywatelskich UE” Komisja ponownie podkreśliła konieczność rozwiązania głównych problemów, które uniemożliwiają obywatelom Unii czerpanie korzyści z jednolitego rynku cyfrowego i transgranicznych usług cyfrowych.

(5) W konkluzjach z dnia 4 lutego 2011 r. i z dnia 23 października 2011 r. Rada Europejska zwróciła się do Komisji o utworzenie jednolitego

rynku cyfrowego do 2015 r. w celu osiągnięcia szybkiego postępu w kluczowych obszarach gospodarki cyfrowej oraz propagowania w pełni zintegrowanego jednolitego rynku cyfrowego poprzez ułatwianie transgranicznego korzystania z usług *online*, ze szczególnym uwzględnieniem ułatwiania bezpiecznej elektronicznej identyfikacji i uwierzytelniania.

(6) W konkluzjach z dnia 27 maja 2011 r. Rada zwróciła się do Komisji o wsparcie rozwoju jednolitego rynku cyfrowego poprzez tworzenie odpowiednich warunków sprzyjających wzajemnemu transgranicznemu uznawaniu głównych aktywatorów, takich jak elektroniczna identyfikacja, dokumenty elektroniczne, podpisy elektroniczne i usługi doręczeń elektronicznych, oraz odpowiednich warunków sprzyjających interoperacyjności usług administracji elektronicznej w całej Unii Europejskiej.

(7) Parlament Europejski w rezolucji z dnia 21 września 2010 r. dotyczącej ostatecznego utworzenia wewnętrznego rynku handlu elektronicznego ([4]) podkreślił znaczenie bezpieczeństwa usług elektronicznych, zwłaszcza podpisów elektronicznych, i potrzebę stworzenia infrastruktury klucza publicznego na poziomie ogólnoeuropejskim, a także wezwał Komisję do stworzenia bramki europejskich urzędów walidacyjnych w celu zapewnienia transgranicznej interoperacyjności podpisów elektronicznych i podniesienia bezpieczeństwa transakcji przeprowadzanych przy użyciu internetu.

(8) Dyrektywa 2006/123/WE Parlamentu Europejskiego i Rady ([5]) nakłada na państwa członkowskie obowiązek utworzenia pojedynczych punktów kontaktowych dla zapewnienia, aby wszelkie procedury i formalności dotyczące podejmowania i prowadzenia działalności usługowej były łatwe do wypełnienia na odległość oraz drogą elektroniczną, poprzez odpowiedni pojedynczy punkt kontaktowy i w odpowiednich właściwych organach. Wiele usług *online* dostępnych za pośrednictwem pojedynczych punktów kontaktowych wymaga elektronicznej identyfikacji, uwierzytelnienia i podpisu.

(9) W większości przypadków obywatele nie mogą korzystać ze swojej identyfikacji elektronicznej w celu uwierzytelnienia się w innym państwie członkowskim, ponieważ krajowe systemy identyfikacji elektronicznej w ich kraju nie są uznawane w innych państwach członkowskich. Ta bariera elektroniczna nie pozwala dostawcom usług w pełni korzystać z rynku wewnętrznego. Wzajemnie uznawane środki identyfikacji elektronicznej ułatwią transgraniczne świadczenie licznych usług na rynku wewnętrznym i umożliwią przedsiębiorstwom prowadzenie działalności za granicą bez konieczności zmagania się z przeszkodami w kontaktach z organami publicznymi.

(10) Dyrektywa Parlamentu Europejskiego i Rady 2011/24/UE ([6]) ustanawia sieć organów krajowych odpowiedzialnych za e-zdrowie. Aby zwiększyć bezpieczeństwo i ciągłość transgranicznej opieki zdrowotnej, sieć musi opracować wytyczne w sprawie transgranicznego dostępu do danych i usług związanych z e-zdrowiem, również poprzez wspieranie „wspólnych środków identyfikacji i uwierzytelniania, aby ułatwić przenoszalność danych w transgranicznej opiece zdrowotnej”. Zapewnienie wzajemnego uznawania elektronicznej identyfikacji i uwierzytelniania jest niezbędne, aby urzeczywistnić transgraniczną opiekę zdrowotną dla obywateli Europy. Gdy obywatele wyjeżdżają w celu podjęcia leczenia, ich dane medyczne muszą być dostępne w kraju, w którym prowadzone jest leczenie. Wymaga to stworzenia solidnych, bezpiecznych i wiarygodnych ram identyfikacji elektronicznej.

(11) Niniejsze rozporządzenie powinno być stosowane w pełnej zgodności z zasadami dotyczącymi ochrony danych osobowych przewidzianymi w dyrektywie 95/46/WE Parlamentu Europejskiego i Rady ([7]). W tym względzie, jeżeli chodzi o zasadę wzajemnego uznawania ustanowioną w niniejszym rozporządzeniu, uwierzytelnianie dla usługi *online* powinno dotyczyć przetwarzania tylko tych danych identyfikacyjnych, które są adekwatne, właściwe i nie wykraczają poza cele przyznania dostępu do tej usługi *online*. Ponadto dostawcy usług zaufania i organy nadzoru powinny przestrzegać wymogów na mocy dyrektywy 95/46/WE dotyczących poufności i bezpieczeństwa przetwarzania.

(12) Jednym z celów niniejszego rozporządzenia jest zniesienie, przynajmniej w przypadku usług publicznych, istniejących barier w transgranicznym stosowaniu środków identyfikacji elektronicznej stosowanych w państwach członkowskich w celu uwierzytelniania. Celem niniejszego rozporządzenia nie jest ingerowanie w systemy zarządzania tożsamością elektroniczną i w powiązane z nimi infrastruktury ustanowione w państwach członkowskich. Jego celem jest zapewnienie bezpiecznej elektronicznej identyfikacji i uwierzytelniania na potrzeby dostępu do transgranicznych usług *online* oferowanych przez państwa członkowskie.

(13) Państwa członkowskie powinny zachować swobodę w stosowaniu lub wprowadzaniu środków dostępu do usług *online* do celów identyfikacji elektronicznej. Powinny również mieć możliwość podjęcia decyzji, czy w dostarczanie tych środków należy zaangażować sektor prywatny. Państwa członkowskie nie powinny być zobowiązane do notyfikowania Komisji swoich systemów identyfikacji elektronicznej. Do państw członkowskich należy wybór tego, czy notyfikować Komisji wszystkie, niektóre lub żaden z systemów identyfikacji elektronicznej używanych na szczeblu krajowym dla uzyskiwania dostępu przynajmniej do publicznych usług *online* lub szczególnych usług.

(14) W niniejszym rozporządzeniu należy ustanowić pewne warunki dotyczące tego, które środki identyfikacji elektronicznej muszą być uznawane i w jaki sposób należy notyfikować systemy identyfikacji elektronicznej. Warunki te powinny pomóc państwom członkowskim w zbudowaniu niezbędnego wzajemnego zaufania do stosowanych przez nie systemów identyfikacji elektronicznej oraz we wzajemnym uznawaniu środków identyfikacji elektronicznej objętych notyfikowanymi systemami. Zasada wzajemnego uznawania powinna mieć zastosowanie, jeżeli system identyfikacji elektronicznej notyfikującego państwa członkowskiego spełnił warunki notyfikacji i notyfikacja ta została opublikowana w *Dzienniku Urzędowym Unii Europejskiej*. Jednak zasada wzajemnego uznawania powinna odnosić się wyłącznie do uwierzytelniania dla usługi *online*. Dostęp do tych usług *online* i ich ostateczne wykonanie na rzecz wnioskodawcy powinny być ściśle powiązane z prawem do korzystania z takich usług na warunkach określonych w przepisach krajowych.

(15) Obowiązek uznawania środka identyfikacji elektronicznej powinien odnosić się wyłącznie do tych środków, których poziom bezpieczeństwa tożsamości jest równy poziomowi wymaganemu w odniesieniu do danej usługi *online* lub wyższy od tego poziomu. Ponadto obowiązek ten powinien mieć zastosowanie wyłącznie wtedy, gdy dany podmiot sektora publicznego używa „średniego” lub „wysokiego” poziomu bezpieczeństwa w odniesieniu do dostępu do tej usługi *online*. Państwa członkowskie powinny mieć nadal swobodę, zgodnie z prawem unijnym, w zakresie uznawania środków identyfikacji elektronicznej charakteryzujących się niższymi poziomami bezpieczeństwa.

(16) Poziomy bezpieczeństwa powinny oznaczać stopień, w jakim można mieć zaufanie do środka identyfikacji elektronicznej przy ustalaniu tożsamości danej osoby, dając tym samym pewność, że osoba podająca daną tożsamość jest faktycznie osobą, której przypisano tę tożsamość. Poziom bezpieczeństwa zależy od stopnia zaufania, jaki ten środek identyfikacji elektronicznej zapewnia co do podawanej lub

zgłaszanej tożsamości danej osoby, przy uwzględnieniu procesów (na przykład potwierdzanie i weryfikacja tożsamości oraz uwierzytelnianie), działań zarządczych (na przykład jednostka wydająca środek identyfikacji elektronicznej i procedura wydawania takiego środka) oraz stosowanych zabezpieczeń technicznych. W wyniku wielkoskalowych projektów pilotażowych finansowanych na szczeblu unijnym, standaryzacji i działań międzynarodowych istnieją różne techniczne definicje i opisy poziomów bezpieczeństwa. W szczególności wielkoskalowy projekt pilotażowy STORK i ISO 29115 odnoszą się między innymi do poziomów 2, 3 i 4, które powinny być szczególnie brane pod uwagę przy ustalaniu minimalnych technicznych wymogów, standardów i procedur dotyczących niskiego, średniego i wysokiego poziomu bezpieczeństwa w rozumieniu niniejszego rozporządzenia, przy zapewnieniu spójnego stosowania niniejszego rozporządzenia, w szczególności w odniesieniu do wysokiego poziomu bezpieczeństwa związanego z potwierdzeniem tożsamości do celów wydania kwalifikowanych certyfikatów. Ustanowione wymogi powinny być neutralne pod względem technologicznym. Spełnienie niezbędnych wymogów bezpieczeństwa powinno być możliwe za pomocą różnych technologii.

(17) Państwa członkowskie powinny zachęcać sektor prywatny do dobrowolnego korzystania ze środków identyfikacji elektronicznej w ramach notyfikowanego systemu do celów identyfikacji, gdy jest ona potrzebna do celów usług *online* lub transakcji elektronicznych. Możliwość korzystania z takich środków identyfikacji elektronicznej sprawiłaby, że sektor prywatny mógłby polegać na elektronicznej identyfikacji i uwierzytelnianiu stosowanych już powszechnie w wielu państwach członkowskich przynajmniej w odniesieniu do usług publicznych, a przedsiębiorstwom i obywatelom ułatwiłaby transgraniczny dostęp do ich usług *online*. Aby ułatwić transgraniczne korzystanie z takich środków identyfikacji elektronicznej przez sektor prywatny, możliwość uwierzytelniania zapewniona przez jakiekolwiek państwo członkowskie powinna być dostępna dla stron ufających z sektora prywatnego mających siedzibę poza terytorium tego państwa członkowskiego na tych samych warunkach co warunki stosowane do stron ufających z sektora prywatnego mających siedzibę na terytorium tego państwa członkowskiego. W rezultacie, jeżeli chodzi o strony ufające z sektora prywatnego, notyfikujące państwo członkowskie może określić warunki dostępu do środków uwierzytelniania. W takich warunkach dostępu można podawać, czy środki uwierzytelniania powiązane z notyfikowanym systemem są obecnie dostępne dla stron ufających z sektora prywatnego.

(18) Niniejsze rozporządzenie powinno przewidywać, że notyfikujące państwo członkowskie, strona wydająca środek identyfikacji elektronicznej oraz strona przeprowadzająca procedury uwierzytelniania przyjmują odpowiedzialność za niewypełnienie odpowiednich obowiązków na mocy niniejszego rozporządzenia. Niniejsze rozporządzenie powinno być jednak stosowane zgodnie z krajowymi przepisami dotyczącymi odpowiedzialności. Nie narusza ono zatem tych przepisów krajowych, na przykład dotyczących definicji odszkodowania lub odpowiednich obowiązujących przepisów proceduralnych, w tym przepisów krajowych dotyczących ciężaru dowodu.

(19) Bezpieczeństwo systemów identyfikacji elektronicznej ma kluczowe znaczenie dla wiarygodnego transgranicznego wzajemnego uznawania środków identyfikacji elektronicznej. W tym kontekście państwa członkowskie powinny współpracować w odniesieniu do bezpieczeństwa i interoperacyjności systemów identyfikacji elektronicznej na szczeblu unijnym. W każdym przypadku, gdy systemy identyfikacji elektronicznej nakładają wymóg korzystania przez strony ufające na szczeblu krajowym z konkretnego sprzętu lub oprogramowania, transgraniczna interoperacyjność oznacza wymóg nienakładania przez te państwa członkowskie takich wymogów i powiązanych kosztów na strony ufające mające siedzibę poza ich terytorium. W takim przypadku należy w zakresie ram interoperacyjności omówić i opracować odpowiednie rozwiązania. Niemniej jednak nieuniknione są wymogi techniczne wynikające ze specyfikacji właściwych krajowym środkom identyfikacji elektronicznej i mogące wpływać na posiadaczy takich środków elektronicznych (np. kart elektronicznych).

(20) Współpraca między państwami członkowskimi powinna ułatwiać techniczną interoperacyjność notyfikowanych systemów identyfikacji elektronicznej w celu uzyskania wysokiego poziomu zaufania i bezpieczeństwa, stosownie do poziomu ryzyka. We współpracy tej pomóc powinna wymiana informacji i najlepszych praktyk między państwami członkowskimi mająca na celu wzajemne uznawanie ich systemów.

(21) W niniejszym rozporządzeniu należy również ustanowić ogólne ramy prawne dotyczące korzystania z usług zaufania. Nie należy jednak wprowadzać ogólnego obowiązku korzystania z nich ani instalowania punktu dostępu dla wszystkich istniejących usług zaufania. W szczególności niniejsze rozporządzenie nie powinno obejmować świadczenia usług wykorzystywanych wyłącznie w obrębie systemów zamkniętych przez określoną grupę uczestników i niemających skutków dla stron trzecich. Wymogom niniejszego rozporządzenia nie powinny na przykład podlegać systemy utworzone w przedsiębiorstwach lub administracjach publicznych w celu zarządzania procedurami wewnętrznymi przy użyciu usług zaufania. Wymogi określone w rozporządzeniu powinny spełniać jedynie usługi zaufania świadczone na rzecz społeczeństwa, mające skutki dla stron trzecich. Niniejsze rozporządzenie nie powinno również obejmować aspektów związanych z zawieraniem i ważnością umów lub innych obowiązków 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.

(22) Aby wspierać ogólne transgraniczne korzystanie z usług zaufania, należy zapewnić możliwość używania tych usług jako dowodu w postępowaniach sądowych we wszystkich państwach członkowskich. W prawie krajowym należy określić skutki prawne usług zaufania, o ile w niniejszym rozporządzeniu nie postanowiono inaczej.

(23) W zakresie, w jakim niniejsze rozporządzenie tworzy obowiązek uznania usługi zaufania, taka usługa zaufania może nie zostać uznana wyłącznie wtedy, gdy adresat tego obowiązku nie może jej odczytać lub zweryfikować z powodów technicznych będących poza bezpośrednią kontrolą tego adresata. Jednak obowiązek ten nie powinien sam w sobie nakładać na organ publiczny wymogu uzyskania sprzętu i oprogramowania niezbędnych do zapewnienia technicznej możliwości odczytania wszystkich istniejących usług zaufania.

(24) Państwa członkowskie mogą utrzymać lub wprowadzić przepisy krajowe, zgodne z prawem unijnym, odnoszące się do usług zaufania, o ile usługi te nie są w pełni zharmonizowane w drodze niniejszego rozporządzenia. Jednak usługi zaufania spełniające wymogi niniejszego rozporządzenia powinny podlegać swobodnemu obrotowi na rynku wewnętrznym.

(25) Państwa członkowskie powinny zachować swobodę określania innych rodzajów usług zaufania oprócz tych, które figurują w zamkniętym wykazie usług zaufania przewidzianym w niniejszym rozporządzeniu, do celów uznania ich na szczeblu krajowym jako kwalifikowanych usług zaufania.

(26) Ze względu na tempo zmian technologicznych w niniejszym rozporządzeniu należy przyjąć podejście otwarte na innowacje.

(27) Niniejsze rozporządzenie powinno być neutralne pod względem technologicznym. Określone w nim skutki prawne powinny być osiągalne za pomocą dowolnego środka technicznego, o ile spełnione zostaną wymogi niniejszego rozporządzenia.

(28) Aby zwiększyć w szczególności zaufanie małych i średnich przedsiębiorstw (MŚP) oraz konsumentów do rynku wewnętrznego i propagować korzystanie z usług i produktów zaufania, należy wprowadzić pojęcia kwalifikowanych usług zaufania i kwalifikowanego dostawcy usług zaufania w celu wskazania wymogów i obowiązków mających zapewnić wysoki poziom bezpieczeństwa wszelkich świadczonych kwalifikowanych usług zaufania lub stosowanych produktów.

(29) Zgodnie z obowiązkami wynikającymi z Konwencji Narodów Zjednoczonych o prawach osób niepełnosprawnych, zatwierdzonej decyzją Rady 2010/48/WE ([8]), w szczególności art. 9 tej konwencji, osoby niepełnosprawne powinny mieć możliwość korzystania z usług zaufania i produktów przeznaczonych dla użytkownika końcowego stosowanych do świadczenia tych usług na równych zasadach z innymi konsumentami. Dlatego, gdy jest to wykonalne, świadczone usługi zaufania i produkty przeznaczone dla użytkownika końcowego stosowane do świadczenia tych usług powinny być dostępne dla osób niepełnosprawnych. Ocena wykonalności powinna obejmować między innymi względy techniczne i gospodarcze.

(30) Państwa członkowskie powinny wyznaczyć organ nadzoru lub organy nadzoru do celów prowadzenia działań nadzorczych na mocy niniejszego rozporządzenia. Państwa członkowskie powinny także mieć możliwość podjęcia decyzji, za obopólnym porozumieniem z innym państwem członkowskim, w sprawie wyznaczenia organu nadzoru na terytorium tego innego państwa członkowskiego.

(31) Organy nadzoru powinny współpracować z organami ochrony danych na przykład przez informowanie ich o wynikach audytów kwalifikowanych dostawców usług zaufania, w przypadku gdy wydaje się, że zostały naruszone przepisy dotyczące ochrony danych osobowych. Przekazywanie informacji powinno obejmować w szczególności incydenty związane z bezpieczeństwem oraz przypadki naruszenia ochrony danych osobowych.

(32) Na wszystkich dostawcach usług zaufania powinien spoczywać obowiązek stosowania dobrych praktyk w zakresie bezpieczeństwa dostosowanych do zagrożeń związanych z ich działalnością, tak aby zwiększyć zaufanie użytkowników do jednolitego rynku.

(33) Przepisy dotyczące używania pseudonimów w certyfikatach nie powinny uniemożliwiać państwom członkowskim wymogu identyfikacji osób zgodnie z prawem unijnym lub prawem krajowym.

(34) W celu zapewnienia porównywalnego poziomu bezpieczeństwa kwalifikowanych usług zaufania wszystkie państwa członkowskie powinny stosować wspólne podstawowe wymogi dotyczące nadzoru. Aby ułatwić spełnianie tych wymogów w jednolity sposób w całej Unii, państwa członkowskie powinny przyjąć porównywalne procedury i powinny wymieniać się informacjami na temat swoich działań nadzorczych oraz najlepszymi praktykami stosowanymi w tej dziedzinie.

(35) Wszyscy dostawcy usług zaufania powinni podlegać wymogom niniejszego rozporządzenia, w szczególności wymogom dotyczącym bezpieczeństwa i odpowiedzialności, aby zapewnić należytą staranność, przejrzystość i rozliczalność ich operacji i usług. Biorąc jednak pod uwagę rodzaj usług świadczonych przez dostawców usług zaufania, należy, w odniesieniu do tych wymogów, dokonać rozróżnienia między kwalifikowanymi i niekwalifikowanymi dostawcami usług zaufania.

(36) Ustanowienie systemu nadzoru dla wszystkich dostawców usług zaufania powinno zapewnić jednakowe zasady dotyczące bezpieczeństwa i rozliczalności ich operacji i usług, przyczyniając się w ten sposób do ochrony użytkowników i do funkcjonowania rynku wewnętrznego. Niekwalifikowani dostawcy usług zaufania powinni podlegać łagodnym i reaktywnym działaniom nadzorczym *ex post*, uzasadnionym przez charakter ich usług i operacji. Organ nadzoru nie powinien zatem mieć ogólnego obowiązku nadzorowania niekwalifikowanych dostawców usług. Organ nadzoru powinien podejmować działania wyłącznie wtedy, gdy został poinformowany (na przykład przez samego niekwalifikowanego dostawcę usług zaufania, przez inny organ nadzoru, w drodze zgłoszenia od użytkownika lub partnera handlowego lub na podstawie własnego dochodzenia), że niekwalifikowany dostawca usług zaufania nie spełnia wymogów niniejszego rozporządzenia.

(37) Niniejsze rozporządzenie powinno przewidywać odpowiedzialność wszystkich dostawców usług zaufania. W szczególności ustanawia system odpowiedzialności, w ramach którego wszyscy dostawcy usług zaufania powinni być odpowiedzialni za szkody wyrządzone osobie fizycznej lub osobie prawnej w związku z niewypełnieniem obowiązków na mocy niniejszego rozporządzenia. Aby ułatwić ocenę ryzyka finansowego, które dostawcy usług zaufania mogą być zmuszeni ponosić lub które powinni pokryć za pomocą polis ubezpieczeniowych, niniejsze rozporządzenie umożliwia dostawcom usług zaufania ustalanie, pod pewnymi warunkami, ograniczeń w zakresie korzystania ze świadczonych przez nich usług i zwalnia ich z odpowiedzialności za szkody wynikające z korzystania z usług wykraczających poza takie ograniczenia. Klienci powinni być z góry należycie informowani o tych ograniczeniach. Te ograniczenia powinny być uznawalne przez stronę trzecią, na przykład poprzez zawieranie informacji o nich w warunkach świadczonej usługi lub za pomocą innych uznawalnych środków. Do celów nadania tym zasadom mocy obowiązującej niniejsze rozporządzenie powinno być stosowane zgodnie z krajowymi przepisami dotyczącymi odpowiedzialności. Niniejsze rozporządzenie nie wpływa zatem na przepisy krajowe dotyczące, na przykład, definicji szkód, zamiaru, zaniedbania lub odpowiednich obowiązujących zasad proceduralnych.

(38) Zgłaszanie przypadków naruszenia bezpieczeństwa i przeprowadzanie ocen ryzyka w zakresie bezpieczeństwa ma zasadnicze znaczenie pod względem zapewnienia odpowiednich informacji zainteresowanym stronom w razie naruszenia bezpieczeństwa lub utraty integralności.

(39) Aby Komisja i państwa członkowskie mogły ocenić skuteczność mechanizmu zgłaszania naruszeń wprowadzonego niniejszym rozporządzeniem, należy zwrócić się do organów nadzoru o dostarczenie Komisji i Agencji Unii Europejskiej ds. Bezpieczeństwa Sieci i Informacji (ENISA) zbiorczych informacji.

(40) Aby Komisja i państwa członkowskie mogły ocenić skuteczność usprawnionego mechanizmu nadzoru wprowadzonego niniejszym rozporządzeniem, należy zwrócić się do organów nadzoru o składanie sprawozdań ze swojej działalności. Sprawozdania te w zasadniczy sposób ułatwiłyby wymianę dobrych praktyk między organami nadzoru i umożliwiłyby sprawdzenie jednolitości i skuteczności wdrażania podstawowych wymogów dotyczących nadzoru we wszystkich państwach członkowskich.

(41) Aby zapewnić stabilność i trwałość kwalifikowanych usług zaufania oraz zwiększyć zaufanie użytkowników do ciągłości kwalifikowanych usług zaufania, organy nadzoru powinny weryfikować istnienie i prawidłowe stosowanie przepisów dotyczących planów zakończenia działalności, w przypadkach gdy kwalifikowani dostawcy usług zaufania zaprzestają swojej działalności.

(42) Aby ułatwić nadzór nad kwalifikowanymi dostawcami usług zaufania, na przykład w sytuacji, gdy dostawca świadczy swoje usługi na

terytorium innego państwa członkowskiego i nie podlega tam nadzorowi lub gdy komputery dostawcy znajdują się na terytorium innego państwa członkowskiego niż państwo, w którym ma siedzibę, należy utworzyć system wzajemnej pomocy między organami nadzoru w państwach członkowskich.

(43) Aby zapewnić przestrzeganie przez kwalifikowanych dostawców usług zaufania wymogów określonych w niniejszym rozporządzeniu i zgodność świadczonych przez nich usług z tymi wymogami, jednostka oceniająca zgodność powinna przeprowadzać ocenę zgodności, a będące jej wynikiem raporty z oceny zgodności powinny być przekazywane przez kwalifikowanych dostawców usług zaufania organowi nadzoru. W każdym przypadku, gdy organ nadzoru nakłada na kwalifikowanego dostawcę usług zaufania wymóg przekazywania raportów z oceny zgodności *ad hoc*, organ nadzoru powinien przestrzegać w szczególności zasad dobrego zarządzania, w tym obowiązku uzasadniania swoich decyzji, a także zasady proporcjonalności. Organ nadzoru powinien zatem należycie uzasadnić swą decyzję ustanawiającą wymóg przeprowadzenia oceny zgodności *ad hoc*.

(44) Niniejsze rozporządzenie służy zapewnieniu spójnych ram z myślą o zagwarantowaniu wysokiego poziomu bezpieczeństwa i pewności prawa w odniesieniu do usług zaufania. W tym względzie, zajmując się oceną zgodności produktów i usług, Komisja powinna w stosownych przypadkach dążyć do synergii z istniejącymi odpowiednimi europejskimi i międzynarodowymi systemami, takimi jak rozporządzenie Parlamentu Europejskiego i Rady (WE) nr 765/2008 ([9]) ustanawiające wymogi w zakresie akredytacji jednostek oceniających zgodność i nadzoru rynku produktów.

(45) Aby umożliwić efektywne zainicjowanie procedury, która powinna doprowadzić do umieszczenia kwalifikowanych dostawców usług zaufania i świadczonych przez nich kwalifikowanych usług zaufania na zaufanych listach, należy dążyć do nawiązania wstępnych interakcji między potencjalnymi kwalifikowanymi dostawcami usług zaufania a właściwym organem nadzoru w celu ułatwienia należytej staranności niezbędnej do świadczenia kwalifikowanych usług zaufania.

(46) Zaufane listy są podstawowym elementem procesu budowania zaufania wśród operatorów rynku, ponieważ wskazują kwalifikowany status dostawcy usługi podczas nadzoru.

(47) Zaufanie do usług *online* i ich wygoda mają podstawowe znaczenie dla użytkowników, by mogli w pełni korzystać z zalet usług elektronicznych i świadomie na tych usługach polegali. W tym celu należy stworzyć unijny znak zaufania, aby oznaczać kwalifikowane usługi zaufania świadczone przez kwalifikowanych dostawców usług zaufania. Taki unijny znak zaufania dotyczący kwalifikowanych usług zaufania pozwoliłby na wyraźne odróżnienie kwalifikowanych usług zaufania od innych usług zaufania, przyczyniając się tym samym do przejrzystości na rynku. Używanie unijnego znaku zaufania przez kwalifikowanych dostawców usług zaufania powinno być dobrowolne i nie powinno prowadzić do jakiegokolwiek wymogu innego niż wymogi przewidziane w niniejszym rozporządzeniu.

(48) Mimo iż w celu zapewnienia wzajemnego uznawania podpisów elektronicznych konieczny jest wysoki poziom bezpieczeństwa, w niektórych przypadkach, na przykład w kontekście decyzji Komisji 2009/767/WE ([10]), akceptowane powinny być również podpisy elektroniczne o niższym poziomie bezpieczeństwa.

(49) Niniejsze rozporządzenie powinno wprowadzić zasadę, że nie należy kwestionować skutku prawnego podpisu elektronicznego z tego powodu, że podpis ten ma postać elektroniczną lub że nie spełnia wszystkich wymogów kwalifikowanego podpisu elektronicznego. Jednakże to w prawie krajowym należy zdefiniować skutek prawny podpisów elektronicznych, z wyjątkiem wymogów przewidzianych w niniejszym rozporządzeniu, zgodnie z którymi kwalifikowany podpis elektroniczny powinien mieć skutek prawny równoważny podpisowi własnoręcznemu.

(50) Ponieważ właściwe organy w państwach członkowskich używają obecnie różnych formatów zaawansowanych podpisów elektronicznych do elektronicznego podpisywania swoich dokumentów, państwa członkowskie powinny zapewnić możliwość obsługi pod względem technicznym co najmniej kilku formatów zaawansowanego podpisu elektronicznego przy odbiorze dokumentów podpisanych elektronicznie. Podobnie, kiedy właściwe organy w państwach członkowskich używają zaawansowanych pieczęci elektronicznych, należałoby zapewnić możliwość obsługi co najmniej kilku formatów zaawansowanej pieczęci elektronicznej.

(51) Podpisującemu należy umożliwić powierzanie kwalifikowanych urządzeń do składania podpisu elektronicznego stronie trzeciej pod warunkiem wdrożenia odpowiednich mechanizmów i procedur zapewniających, aby podpisujący miał wyłączną kontrolę nad używaniem swoich danych służących do składania podpisu elektronicznego i aby urządzenie użytkowane było ze spełnieniem wymogów dotyczących kwalifikowanego podpisu elektronicznego.

(52) Coraz powszechniejsze będzie składanie podpisu elektronicznego na odległość, w przypadku którego środowiskiem składania podpisu elektronicznego zarządza dostawca usług zaufania w imieniu podpisującego, gdyż wiąże się ono z licznymi korzyściami gospodarczymi. Jednakże w celu zapewnienia, aby takie podpisy elektroniczne były prawnie uznawane na równi z podpisami elektronicznymi składanymi w środowisku, nad którym całkowicie panuje użytkownik, dostawcy usługi składania podpisu elektronicznego na odległość powinni stosować szczególne procedury zarządzania i szczególne administracyjne procedury bezpieczeństwa, używać wiarygodnych systemów i produktów, w tym bezpiecznych kanałów komunikacji elektronicznej, aby zagwarantować niezawodność środowiska składania podpisu elektronicznego oraz korzystanie z tego środowiska pod wyłączną kontrolą podpisującego. W przypadku kwalifikowanego podpisu elektronicznego składanego za pomocą urządzenia do składania podpisu elektronicznego na odległość należy stosować wymogi mające zastosowanie do kwalifikowanych dostawców usług zaufania, określone w niniejszym rozporządzeniu.

(53) Zawieszenie kwalifikowanych certyfikatów jest utrwaloną praktyką operacyjną stosowaną przez dostawców usług zaufania w wielu państwach członkowskich, którą należy odróżnić od unieważnienia i która wiąże się z czasową utratą ważności certyfikatu. Ze względu na pewność prawa status zawieszenia certyfikatu musi być zawsze jasno wskazany. W tym celu dostawcy usług zaufania powinni mieć obowiązek jasnego wskazania statusu certyfikatu, a w razie jego zawieszenia – dokładnego okresu, na jaki certyfikat został zawieszony. Niniejsze rozporządzenie nie powinno nakładać na dostawców usług zaufania ani na państwa członkowskie obowiązku stosowania zawieszenia, ale powinno przewidzieć przepisy dotyczące przejrzystości, w przypadku gdy taka praktyka jest możliwa.

(54) Transgraniczna interoperacyjność i transgraniczne uznawanie kwalifikowanych certyfikatów stanowią warunek wstępny transgranicznego uznawania kwalifikowanych podpisów elektronicznych. Dlatego kwalifikowane certyfikaty nie powinny podlegać żadnym obowiązkowym wymogom przekraczającym wymogi określone w niniejszym rozporządzeniu. Jednak na szczeblu krajowym należy dopuścić zawieranie w kwalifikowanych certyfikatach szczególnych atrybutów, takich jak unikalne identyfikatory, pod warunkiem że takie szczególne atrybuty nie utrudniają transgranicznej interoperacyjności i transgranicznego uznawania kwalifikowanych certyfikatów i

podpisów elektronicznych.

(55) Certyfikacja bezpieczeństwa informatycznego oparta na normach międzynarodowych, takich jak ISO 15408 i powiązane metody oceny i ustalenia dotyczące wzajemnego uznawania, jest ważnym narzędziem weryfikacji bezpieczeństwa kwalifikowanych urządzeń do składania podpisu elektronicznego i należy ją propagować. Jednakże innowacyjne rozwiązania i usługi, takie jak mobilny podpis i podpisywanie w chmurze, polegają na technicznych i organizacyjnych rozwiązaniach, jakimi są kwalifikowane urządzenia do składania podpisu elektronicznego, w odniesieniu do których mogą jeszcze nie być dostępne normy bezpieczeństwa lub pierwsza certyfikacja bezpieczeństwa informatycznego jeszcze trwa. Poziom bezpieczeństwa takich kwalifikowanych urządzeń do składania podpisu elektronicznego można by poddawać ocenie przy użyciu alternatywnych procedur tylko w przypadku, gdy takie normy bezpieczeństwa nie są dostępne lub gdy pierwsza certyfikacja bezpieczeństwa informatycznego jeszcze trwa. Procedury te powinny być porównywalne z normami certyfikacji bezpieczeństwa informatycznego w zakresie, w jakim ich poziomy bezpieczeństwa są równoważne. Procedury te mogłaby ułatwić wzajemna ocena.

(56) Niniejsze rozporządzenie określa wymogi dla kwalifikowanych urządzeń do składania podpisu elektronicznego w celu zapewnienia funkcjonalności zaawansowanych podpisów elektronicznych. Niniejsze rozporządzenie nie obejmuje całego środowiska systemowego, w którym działają takie urządzenia. Dlatego zakres certyfikacji kwalifikowanych urządzeń do składania podpisów powinien być ograniczony do sprzętu i oprogramowania systemowego używanego do zarządzania danymi służącymi do składania podpisu tworzonymi, przechowywanymi lub przetwarzanymi w ramach urządzenia do składania podpisu oraz do ochrony tych danych. Zgodnie z wyszczególnieniem w odpowiednich normach zakres obowiązku certyfikacji nie powinien obejmować aplikacji służących do składania podpisu.

(57) Aby zagwarantować pewność prawa w odniesieniu do ważności podpisu, niezbędne jest wyszczególnienie elementów kwalifikowanego podpisu elektronicznego, które powinny być ocenione przez stronę ufającą dokonującą walidacji. Ponadto wyszczególnienie wymogów dla kwalifikowanych dostawców usług zaufania mogących świadczyć kwalifikowane usługi walidacji na rzecz stron ufających, które same nie chcą lub nie są w stanie dokonać walidacji kwalifikowanych podpisów elektronicznych, powinno zachęcić sektory prywatny i publiczny do inwestowania w takie usługi. Dzięki tym obu elementom walidacja kwalifikowanych podpisów elektronicznych powinna być łatwa i wygodna dla wszystkich stron na poziomie Unii.

(58) Gdy transakcja wymaga od osoby prawnej użycia kwalifikowanej pieczęci elektronicznej, akceptowalny powinien być również kwalifikowany podpis elektroniczny upoważnionego przedstawiciela osoby prawnej.

(59) Pieczęcie elektroniczne powinny służyć jako dowód wydania danego dokumentu elektronicznego przez daną osobę prawną, dając pewność co do pochodzenia i integralności dokumentu.

(60) Dostawcy usług zaufania wydający kwalifikowane certyfikaty pieczęci elektronicznych powinni wdrożyć niezbędne środki, aby móc ustalić tożsamość osoby fizycznej reprezentującej osobę prawną, której świadczony jest kwalifikowany certyfikat pieczęci elektronicznej, gdy taka identyfikacja jest niezbędna na szczeblu krajowym w kontekście postępowań sądowych lub administracyjnych.

(61) Niniejsze rozporządzenie powinno zapewnić długoterminową konserwację informacji w celu zapewnienia prawnej ważności podpisów elektronicznych i pieczęci elektronicznych przez wydłużone okresy oraz zagwarantowania możliwości ich walidacji bez względu na przyszłe zmiany technologiczne.

(62) Aby zapewnić bezpieczeństwo kwalifikowanych elektronicznych znaczników czasu, niniejsze rozporządzenie powinno wprowadzić wymóg używania zaawansowanej pieczęci elektronicznej lub zaawansowanego podpisu elektronicznego lub innych równoważnych metod. Można przewidzieć, że dzięki innowacjom mogą powstać nowe technologie, które mogą zapewnić znacznikom czasu równoważny poziom bezpieczeństwa. W każdym przypadku, gdy używana jest metoda inna niż zaawansowana pieczęć elektroniczna lub zaawansowany podpis elektroniczny, do kwalifikowanego dostawcy usługi zaufania powinno należeć wykazanie w raporcie z oceny zgodności, że taka metoda zapewnia równoważny poziom bezpieczeństwa i spełnia obowiązki określone w niniejszym rozporządzeniu.

(63) Dokumenty elektroniczne są ważne dla dalszego rozwoju transgranicznych transakcji elektronicznych na rynku wewnętrznym. Niniejsze rozporządzenie powinno wprowadzić zasadę, że nie należy kwestionować skutku prawnego dokumentu elektronicznego z tego powodu, że dokument ten ma postać elektroniczną, tak aby zapewnić, aby transakcja elektroniczna nie została odrzucona wyłącznie z tego powodu, że dokument ma postać elektroniczną.

(64) Zajmując się formatami zaawansowanych podpisów i pieczęci elektronicznych, Komisja powinna opierać się na istniejących praktykach, standardach i przepisach, w szczególności decyzji Komisji 2011/130/UE ([11]).

(65) Pieczęcie elektroniczne mogą być używane nie tylko do uwierzytelnienia dokumentu wydanego przez osobę prawną, lecz również do uwierzytelnienia wszelkich zasobów cyfrowych osoby prawnej, takich jak kod oprogramowania lub serwery.

(66) 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.

(67) Usługi uwierzytelniania witryn internetowych zapewniają środki, za pomocą których odwiedzający daną witrynę internetową może być pewny, że za tą witryną internetową stoi prawdziwy i prawowity podmiot. Usługi te przyczyniają się do budowy zaufania do prowadzenia przedsiębiorstwa *online*, ponieważ użytkownicy będą mieli zaufanie do witryny internetowej, która została uwierzytelniona. Świadczenie i używanie usług uwierzytelniania witryny internetowej jest całkowicie dobrowolne. Jednak aby uwierzytelnianie witryny internetowej stało się środkiem wzbudzającym zaufanie, zapewniającym użytkownikowi lepsze doświadczenie i wspierającym wzrost na rynku wewnętrznym, niniejsze rozporządzenie powinno określać minimalne obowiązki w zakresie bezpieczeństwa i odpowiedzialności dla dostawców i ich usług. W tym celu uwzględnione zostały wyniki istniejących inicjatyw prowadzonych przez branżę, na przykład Forum Organów Certyfikacji/Twórców Przeglądarek – Forum CA/B. Dodatkowo niniejsze rozporządzenie nie powinno utrudniać używania innych środków lub metod uwierzytelniania witryny internetowej nieobjętych niniejszym rozporządzeniem ani nie powinno uniemożliwiać tego, aby dostawcy usług uwierzytelniania witryn internetowych z państw trzecich świadczyli swoje usługi klientom w Unii. Jednak usługi uwierzytelniania witryny internetowej świadczone przez dostawcę z państwa trzeciego można uznać za

kwalifikowane, zgodnie z niniejszym rozporządzeniem, wyłącznie wtedy, gdy zawarta została umowa międzynarodowa między Unią a krajem siedziby tego dostawcy.

(68) Pojęcie „osób prawnych” zgodnie z postanowieniami Traktatu o funkcjonowaniu Unii Europejskiej (TFUE) dotyczącymi prowadzenia przedsiębiorstwa pozostawia podmiotom gospodarczym swobodę wyboru formy prawnej, którą uznają za odpowiednią dla prowadzenia swojej działalności. Dlatego też termin „osoby prawne” w rozumieniu TFUE oznacza wszystkie podmioty ustanowione na mocy prawa państwa członkowskiego lub podlegające temu prawu, niezależnie od ich formy prawnej.

(69) Zachęca się instytucje, organy, urzędy i agencje Unii do uznawania identyfikacji elektronicznej i usług zaufania objętych niniejszym rozporządzeniem do celów współpracy administracyjnej korzystającej, w szczególności, z istniejących dobrych praktyk i wyników bieżących projektów w obszarach objętych niniejszym rozporządzeniem.

(70) W celu uzupełnienia w elastyczny i szybki sposób niektórych szczegółowych i technicznych aspektów niniejszego rozporządzenia należy przekazać Komisji uprawnienia do przyjmowania aktów zgodnie z art. 290 TFUE w odniesieniu do kryteriów, które mają spełniać organy odpowiedzialne za certyfikację kwalifikowanych urządzeń do składania podpisu elektronicznego. Szczególnie ważne jest, aby w czasie prac przygotowawczych Komisja prowadziła stosowne konsultacje, w tym na poziomie ekspertów. Przygotowując i opracowując akty delegowane, Komisja powinna zapewnić jednoczesne, terminowe i odpowiednie przekazywanie stosownych dokumentów Parlamentowi Europejskiemu i Radzie.

(71) W celu zapewnienia jednolitych warunków wykonywania niniejszego rozporządzenia należy powierzyć Komisji uprawnienia wykonawcze, w szczególności w odniesieniu do określenia numerów referencyjnych norm, których stosowanie prowadzi do powstania domniemania spełnienia niektórych wymogów przewidzianych w niniejszym rozporządzeniu. Uprawnienia te powinny być wykonywane zgodnie z rozporządzeniem Parlamentu Europejskiego i Rady (UE) nr 182/2011 ([12]).

(72) Przy przyjmowaniu aktów delegowanych lub wykonawczych Komisja powinna w należyty sposób uwzględniać normy i specyfikacje techniczne opracowywane przez europejskie i międzynarodowe organizacje i organy normalizacyjne, w szczególności Europejski Komitet Normalizacyjny (CEN), Europejski Instytut Norm Telekomunikacyjnych (ETSI), Międzynarodową Organizację Normalizacyjną (ISO) lub Międzynarodowy Związek Telekomunikacyjny (ITU), tak aby zapewnić wysoki poziom bezpieczeństwa i interoperacyjności identyfikacji elektronicznej i usług zaufania.

(73) Ze względu na pewność i przejrzystość prawa należy uchylić dyrektywę 1999/93/WE.

(74) Aby zagwarantować pewność prawa operatorom rynku stosującym już kwalifikowane certyfikaty wydane osobom fizycznym zgodnie z dyrektywą 1999/93/WE, należy przewidzieć odpowiedni okres przejściowy. Podobnie należy ustanowić środki przejściowe w odniesieniu do bezpiecznych urządzeń do składania podpisu, których zgodność została ustalona zgodnie z dyrektywą 1999/93/WE, a także w odniesieniu do podmiotów świadczących usługi certyfikacyjne, wydających kwalifikowane certyfikaty przed dniem 1 lipca 2016 r. Ponadto należy również zapewnić Komisji środki do przyjmowania aktów wykonawczych i delegowanych przed tym dniem.

(75) Daty rozpoczęcia stosowania określone w niniejszym rozporządzeniu nie wpływają na istniejące obowiązki, które już dotyczą państw członkowskich na mocy prawa Unii, w szczególności na mocy dyrektywy 2006/123/WE.

(76) Ponieważ cele niniejszego rozporządzenia nie mogą być osiągnięte w sposób wystarczający przez państwa członkowskie, natomiast ze względu na skalę działań możliwe jest ich lepsze osiągnięcie na poziomie Unii, może ona przyjąć środki zgodnie z zasadą pomocniczości określoną w art. 5 Traktatu o Unii Europejskiej. Zgodnie z zasadą proporcjonalności, określoną w tym artykule, niniejsze rozporządzenie nie wykracza poza to, co jest konieczne do osiągnięcia tych celów.

(77) Zgodnie z art. 28 ust. 2 rozporządzenia (WE) nr 45/2001 Parlamentu Europejskiego i Rady ([13]) przeprowadzono konsultacje z Europejskim Inspektorem Ochrony Danych, który wydał opinię w dniu 27 września 2012 r. ([14]),

PRZYJMUJĄ NINIEJSZE ROZPORZĄDZENIE:

ROZDZIAŁ I
PRZEPISY OGÓLNE

Artykuł 1

Przedmiot

W celu zapewnienia właściwego funkcjonowania rynku wewnętrznego i w dążeniu do osiągnięcia odpowiedniego poziomu bezpieczeństwa środków identyfikacji elektronicznej i usług zaufania niniejsze rozporządzenie:

a) określa warunki uznawania przez państwa członkowskie środków identyfikacji elektronicznej osób fizycznych i prawnych, objętych notyfikowanym systemem identyfikacji elektronicznej innego państwa członkowskiego;

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

c) ustanawia ramy prawne dla podpisów elektronicznych, pieczęci elektronicznych, elektronicznych znaczników czasu, dokumentów elektronicznych, usług rejestrowanego doręczenia elektronicznego i usług certyfikacyjnych uwierzytelniania witryn internetowych.

Artykuł 2

Zakres stosowania

1. Niniejsze rozporządzenie ma zastosowanie do systemów identyfikacji elektronicznej, które zostały notyfikowane przez państwo członkowskie, oraz do dostawców usług zaufania mających siedzibę w Unii.

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

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.

Artykuł 3

Definicje

Do celów niniejszego rozporządzenia stosuje się następujące definicje:

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

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

3) „dane identyfikujące osobę” oznaczają zestaw danych umożliwiających ustalenie tożsamości osoby fizycznej lub prawnej, lub osoby fizycznej reprezentującej osobę prawną;

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

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

6) „strona ufająca” oznacza osobę fizyczną lub prawną, która polega na identyfikacji elektronicznej lub usłudze zaufania;

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

8) „podmiot prawa publicznego” oznacza podmiot zdefiniowany w art. 2 ust. 1 pkt 4 dyrektywy Parlamentu Europejskiego i Rady 2014/24/UE ([15]);

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

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

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

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

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

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

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

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

   a) tworzenie, weryfikację i walidację podpisów elektronicznych, pieczęci elektronicznych lub elektronicznych znaczników czasu, usług rejestrowanego doręczenia elektronicznego oraz certyfikatów powiązanych z tymi usługami; lub

   b) tworzenie, weryfikację i walidację certyfikatów uwierzytelniania witryn internetowych; lub

   c) konserwację elektronicznych podpisów, pieczęci lub certyfikatów powiązanych z tymi usługami;

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

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;

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

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

21) „produkt” oznacza sprzęt lub oprogramowanie lub odpowiednie komponenty sprzętu lub oprogramowania, które są przeznaczone do wykorzystania w świadczeniu usług zaufania;

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

41) „walidacja” oznacza proces weryfikacji i potwierdzenia ważności podpisu elektronicznego lub pieczęci.

Artykuł 4

Zasada rynku wewnętrznego

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

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

Artykuł 5

Przetwarzanie i ochrona danych

1. Przetwarzanie danych osobowych prowadzone jest zgodnie z przepisami dyrektywy 95/46/WE.

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

ROZDZIAŁ II
IDENTYFIKACJA ELEKTRONICZNA

Artykuł 6

Wzajemne uznawanie

1. Jeżeli zgodnie z prawem krajowym lub zgodnie z krajową praktyką administracyjną dostęp do usługi *online* świadczonej przez podmiot sektora publicznego w jednym państwie członkowskim wymaga identyfikacji elektronicznej przy użyciu środka identyfikacji elektronicznej oraz uwierzytelnienia, w tym pierwszym państwie członkowskim na potrzeby transgranicznego uwierzytelnienia dla tej usługi *online* uznaje się środek identyfikacji elektronicznej wydany w innym państwie członkowskim, pod warunkiem że spełnione są następujące warunki:

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

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

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

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

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

Artykuł 7

Systemy identyfikacji elektronicznej kwalifikujące się do notyfikowania

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

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

(i) przez notyfikujące państwo członkowskie;

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

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

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

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

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

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

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

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

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

g) co najmniej sześć miesięcy przed notyfikacją na podstawie art. 9 ust. 1 notyfikujące państwo członkowskie przekazuje innym państwom członkowskim do celów wykonania obowiązku na mocy art. 12 ust. 5 opis tego systemu zgodnie z warunkami proceduralnymi ustanowionymi w aktach wykonawczych, o których mowa w art. 12 ust. 7;

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

Artykuł 8

Poziomy bezpieczeństwa systemów identyfikacji elektronicznej

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

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

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

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

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

3. Do dnia 18 września 2015 r., przy uwzględnieniu odpowiednich standardów międzynarodowych i z zastrzeżeniem ust. 2, Komisja określi w drodze aktów wykonawczych minimalne techniczne specyfikacje, standardy i procedury, w odniesieniu do których określone zostaną niski, średni i wysoki poziom bezpieczeństwa dla środka identyfikacji elektronicznej do celów ust. 1.

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

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

b) procedury wydawania wnioskowanego środka identyfikacji elektronicznej;

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

d) jednostki wydającej środek identyfikacji elektronicznej;

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

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

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

Artykuł 9

Notyfikacja

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

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

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

(i) strony wydającej środki identyfikacji elektronicznej; oraz

(ii) strony przeprowadzającej procedurę uwierzytelniania;

c) organ lub organy odpowiedzialne za system identyfikacji elektronicznej;

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

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

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

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

2. Rok od daty rozpoczęcia stosowania aktów wykonawczych, o których mowa w art. 8 ust. 3 i art. 12 ust. 8, Komisja opublikuje w *Dzienniku Urzędowym Unii Europejskiej* wykaz systemów identyfikacji elektronicznej, które zostały notyfikowane na mocy ust. 1 niniejszego artykułu, oraz podstawowe informacje na ich temat.

3. Jeżeli Komisja otrzyma notyfikację po upływie okresu, o którym mowa w ust. 2, publikuje w *Dzienniku Urzędowym Unii Europejskiej* zmiany w wykazie, o którym mowa w ust. 2, w terminie dwóch miesięcy od daty otrzymania tej notyfikacji.

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

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

Artykuł 10

Naruszenie bezpieczeństwa

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

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

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

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

2.

Artykuł 11

Odpowiedzialność

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

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

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

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

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

Artykuł 12

Współpraca i interoperacyjność

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

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

3. Ramy interoperacyjności spełniają następujące kryteria:

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

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

c) ułatwiają wdrożenie zasady uwzględniania ochrony prywatności już w fazie projektowania; oraz

d) zapewniają, aby dane osobowe były przetwarzane zgodnie z dyrektywą 95/46/WE.

4. Ramy interoperacyjności zawierają:

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

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

c) odniesienie do minimalnych wymogów technicznych dotyczących interoperacyjności;

d) odniesienie do minimalnego zbioru danych identyfikujących osobę unikalnie reprezentujących osobę fizyczną lub prawną, dostępnego w ramach systemów identyfikacji elektronicznej;

e) regulamin wewnętrzny;

f) ustalenia dotyczące rozstrzygania sporów; oraz

g) wspólne operacyjne standardy bezpieczeństwa.

5. Państwa członkowskie współpracują ze sobą, mając na uwadze następujące kwestie:

a) interoperacyjność systemów identyfikacji elektronicznej notyfikowanych na podstawie art. 9 ust. 1 i systemów identyfikacji elektronicznej, które państwa członkowskie zamierzają notyfikować; oraz

b) bezpieczeństwo systemów identyfikacji elektronicznej.

6. Współpraca między państwami członkowskimi obejmuje:

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

b) wymianę informacji, doświadczeń i dobrych praktyk w zakresie pracy z poziomami bezpieczeństwa systemów identyfikacji elektronicznej określonych w art. 8;

c) wzajemną ocenę systemów identyfikacji elektronicznej objętych niniejszym rozporządzeniem; oraz

d) analizę istotnych zmian w sytuacji w sektorze identyfikacji elektronicznej.

7. Do dnia 18 marca 2015 r. Komisja ustanowi w drodze aktów wykonawczych niezbędne proceduralne warunki ułatwiania współpracy między państwami członkowskimi, o której mowa w ust. 5 i 6, w celu zapewnienia wysokiego poziomu zaufania i bezpieczeństwa, stosownie do poziomu ryzyka.

8. Do dnia 18 września 2015 r., do celów określenia jednolitych warunków realizacji wymogu, o którym mowa w ust. 1, z zastrzeżeniem kryteriów określonych w ust. 3 i z uwzględnieniem wyników współpracy między państwami członkowskimi, Komisja przyjmie akty wykonawcze dotyczące ram interoperacyjności określonych w ust. 4.

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

ROZDZIAŁ III
USŁUGI ZAUFANIA

SEKCJA 1
Przepisy ogólne

Artykuł 13

Odpowiedzialność i ciężar dowodu

1. Bez uszczerbku dla ust. 2, 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.

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

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

Artykuł 14

Aspekty międzynarodowe

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

2. Umowy, o których mowa w ust. 1, zapewniają w szczególności, aby:

a) 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 organizacjach międzynarodowych, z którymi zawarta została umowa, oraz przez świadczone przez nich usługi zaufania;

b) 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 organizacjach międzynarodowych, z którymi zawarta została umowa.

Artykuł 15

Dostępność dla osób niepełnosprawnych

Gdy jest to wykonalne, świadczone usługi zaufania i produkty przeznaczone dla użytkownika końcowego stosowane do świadczenia tych usług są dostępne dla osób niepełnosprawnych.

Artykuł 16

Sankcje

Państwa członkowskie ustanawiają przepisy o sankcjach mających zastosowanie w przypadku naruszeń niniejszego rozporządzenia. Przewidziane sankcje muszą być skuteczne, proporcjonalne i odstraszające.

SEKCJA 2
Nadzór

Artykuł 17

Organ nadzoru

1. Państwa członkowskie wyznaczają organ nadzoru z siedzibą na swoim terytorium lub, za obopólnym porozumieniem z innym państwem członkowskim, organ nadzoru z siedzibą w tym innym państwie członkowskim. Organ ten jest odpowiedzialny za zadania nadzoru w wyznaczającym państwie członkowskim.

Organom nadzoru przyznaje się uprawnienia i odpowiednie zasoby niezbędne do wykonywania ich zadań.

2. Państwa członkowskie notyfikują Komisji nazwy i adresy wyznaczonych przez siebie organów nadzoru.

3. Organ nadzoru odgrywa następującą rolę:

a) sprawuje nadzór nad kwalifikowanymi dostawcami usług zaufania mającymi siedzibę na terytorium wyznaczającego państwa członkowskiego w celu zapewnienia – za pomocą działań nadzorczych *ex ante* i *ex post* – aby kwalifikowani dostawcy usług zaufania i świadczone przez nich kwalifikowane usługi zaufania spełniały wymogi określone w niniejszym rozporządzeniu;

b) podejmuje, w razie konieczności, działania w odniesieniu do niekwalifikowanych dostawców usług zaufania mających siedzibę na terytorium wyznaczającego państwa członkowskiego – za pomocą działań nadzorczych *ex post* – gdy dowiaduje się, że niekwalifikowani

dostawcy usług zaufania lub świadczone przez nich usługi zaufania rzekomo nie spełniają wymogów określonych w niniejszym rozporządzeniu.

4. Do celów ust. 3 i z zastrzeżeniem ograniczeń w nim określonych, zadania organu nadzoru obejmują w szczególności:

a) współpracę z innymi organami nadzoru i udzielanie im pomocy zgodnie z art. 18;

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

c) informowanie innych organów nadzoru i społeczeństwa o naruszeniach bezpieczeństwa lub utracie integralności zgodnie z art. 19 ust. 2;

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

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

f) współpracę z organami ochrony danych, w szczególności przez informowanie ich, bez zbędnej zwłoki, o wynikach audytów kwalifikowanych dostawców usług zaufania, w przypadku gdy, jak się wydaje, doszło do naruszenia przepisów dotyczących ochrony danych osobowych;

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

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

i) weryfikacja istnienia i prawidłowego stosowania przepisów dotyczących planów zakończenia działalności, w przypadkach gdy kwalifikowany dostawca usług zaufania zaprzestaje swojej działalności, w tym tego, w jaki sposób zapewnia się dalszą dostępność informacji zgodnie z art. 24 ust. 2 lit. h);

j) wymaganie, aby dostawcy usług zaufania eliminowali wszelkie przypadki niespełnienia wymogów określonych w niniejszym rozporządzeniu.

5. Państwa członkowskie mogą wymagać, by organ nadzoru utworzył, utrzymywał i aktualizował infrastrukturę zaufania zgodnie z warunkami określonymi w prawie krajowym.

6. Do dnia 31 marca każdego roku każdy organ nadzoru przekazuje Komisji sprawozdanie z jego głównych działań w poprzednim roku kalendarzowym wraz z zestawieniem notyfikacji dotyczących naruszeń otrzymanych od dostawców usług zaufania zgodnie z art. 19 ust. 2.

7. Komisja udostępnia państwom członkowskim roczne sprawozdanie, o którym mowa w ust. 6.

8. Komisja może w drodze aktów wykonawczych określić formaty i procedury dotyczące sprawozdania, o którym mowa w ust. 6. Te akty wykonawcze przyjmuje się zgodnie z procedurą sprawdzającą, o której mowa w art. 48 ust. 2.

Artykuł 18

Wzajemna pomoc

1. Organy nadzoru prowadzą współpracę, w ramach której wymieniają się dobrymi praktykami.

Organ nadzoru, na uzasadniony wniosek innego organu nadzoru, udziela temu organowi pomocy, tak aby działania organów nadzoru były prowadzone w spójny sposób. Wzajemna pomoc może obejmować w szczególności wnioski o informacje i środki nadzorcze, takie jak wnioski o przeprowadzenie inspekcji związanych z raportami z oceny zgodności, o których mowa w art. 20 i 21.

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

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

b) pomoc, której dotyczy wniosek, nie jest proporcjonalna do działań nadzorczych organu nadzoru prowadzonych zgodnie z art. 17;

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

3. W stosownych przypadkach państwa członkowskie mogą upoważnić swoje odpowiednie organy nadzoru do prowadzenia wspólnych dochodzeń, w których biorą udział pracownicy z organów nadzoru innych państw członkowskich. Ustalenia i procedury dotyczące takich wspólnych działań są uzgadniane i określane przez zainteresowane państwa członkowskie zgodnie z ich prawem krajowym.

Artykuł 19

Wymogi w zakresie bezpieczeństwa mające zastosowanie do dostawców usług zaufania

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

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

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

W stosownych przypadkach, w szczególności jeżeli naruszenie bezpieczeństwa lub utrata integralności dotyczą dwóch lub większej liczby

państw członkowskich, zawiadomiony organ nadzoru powiadamia organy nadzoru w pozostałych zainteresowanych państwach członkowskich oraz ENISA.

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

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

4. Komisja może w drodze aktów wykonawczych:

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

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

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

SEKCJA 3

Kwalifikowane usługi zaufania

Artykuł 20

Nadzór nad kwalifikowanymi dostawcami usług zaufania

1. Kwalifikowani dostawcy usług zaufania podlegają audytowi, na ich własny koszt co najmniej raz na 24 miesiące, przeprowadzanemu przez jednostkę oceniającą zgodność. Celem audytu jest potwierdzenie, że kwalifikowani dostawcy usług zaufania oraz świadczone przez nich kwalifikowane usługi zaufania spełniają wymogi określone w niniejszym rozporządzeniu. Kwalifikowani dostawcy usług zaufania przedkładają powstały w ten sposób raport z oceny zgodności organowi nadzoru w terminie trzech dni roboczych od jego otrzymania.

2. Bez uszczerbku dla ust. 1, organ nadzoru może w dowolnym momencie przeprowadzić audyt – lub zwrócić się do jednostki oceniającej zgodność o przeprowadzenie oceny zgodności – kwalifikowanych dostawców usług zaufania, na koszt tych dostawców usług zaufania, aby potwierdzić, że dostawcy ci oraz świadczone przez nich kwalifikowane usługi zaufania spełniają wymogi określone w niniejszym rozporządzeniu. W przypadku gdy wydaje się, że zostały naruszone przepisy dotyczące ochrony danych, organ nadzoru informuje o wynikach swoich audytów organy ochrony danych.

3. W przypadku gdy organ nadzoru nakłada na kwalifikowanego dostawcę usług zaufania wymóg wyeliminowania przypadków niespełnienia wymogów określonych w niniejszym rozporządzeniu i ten dostawca nie podejmie odpowiednich działań, 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, i informuje organ, o którym mowa w art. 22 ust. 3, do celów zaktualizowania zaufanych list, o których mowa w art. 22 ust. 1. Organ nadzoru informuje kwalifikowanego dostawcę usług zaufania o odebraniu jego statusu kwalifikowanego lub statusu kwalifikowanego danej usługi.

4. Komisja może w drodze aktów wykonawczych podać numery referencyjne następujących norm:

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

b) norm dotyczących zasad audytów, zgodnie z którymi jednostki oceniające zgodność będą przeprowadzać oceny zgodności kwalifikowanych dostawców usług zaufania, o których mowa w ust. 1.

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

Artykuł 21

Inicjowanie kwalifikowanej usługi zaufania

1. W przypadku gdy dostawcy usług zaufania nieposiadający statusu kwalifikowanych dostawców usług zaufania zamierzają rozpocząć świadczenie kwalifikowanych usług zaufania, zgłaszają organowi nadzoru swój zamiar wraz z raportem z oceny zgodności wydanym przez jednostkę oceniającą zgodność.

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.

Jeżeli organ nadzoru stwierdzi, że dostawca usług zaufania i świadczone przez niego usługi zaufania spełniają wymogi, o których mowa w akapicie pierwszym, organ nadzoru przyznaje dostawcy status kwalifikowanego dostawcy usług zaufania i status kwalifikowanych usług zaufania świadczonym przez niego usługom oraz informuje organ, 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.

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

4. Komisja może w drodze aktów wykonawczych określić formaty i procedury na użytek ust. 1 i 2. Te akty wykonawcze przyjmuje się zgodnie z procedurą sprawdzającą, o której mowa w art. 48 ust. 2.

Artykuł 22

Zaufane listy

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

2. Państwa członkowskie sporządzają, prowadzą i publikują – w zabezpieczony sposób – elektronicznie podpisane lub opatrzone pieczęcią

elektroniczną zaufane listy, o których mowa w ust. 1, w postaci dostosowanej do automatycznego przetwarzania.

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

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

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

Artykuł 23

Znak zaufania UE dla kwalifikowanych usług zaufania

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

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

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

Artykuł 24

Wymogi dla kwalifikowanych dostawców usług zaufania

1. Wydając kwalifikowany certyfikat dla usługi zaufania, kwalifikowany dostawca usług zaufania weryfikuje, za pomocą odpowiednich środków i zgodnie z prawem krajowym, tożsamość i, w stosownym przypadku, wszelkie specjalne atrybuty osoby fizycznej lub prawnej, której wydaje kwalifikowany certyfikat.

Informacje, o których mowa w akapicie pierwszym, są weryfikowane przez kwalifikowanego dostawcę usług zaufania albo bezpośrednio, albo polegając na stronie trzeciej zgodnie z prawem krajowym:

a) przez fizyczną obecność osoby fizycznej lub upoważnionego przedstawiciela osoby prawnej; lub

b) zdalnie, przy użyciu środka identyfikacji elektronicznej, w przypadku którego przed wydaniem kwalifikowanego certyfikatu zapewniono fizyczną obecność osoby fizycznej lub upoważnionego przedstawiciela osoby prawnej i który spełnia wymogi określone w art. 8 w odniesieniu do średniego lub wysokiego poziomu bezpieczeństwa; lub

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

d) przy użyciu innych metod identyfikacji uznanych na szczeblu krajowym, które zapewniają pewność równoważną, pod względem wiarygodoności, fizycznej obecności. Równoważna pewność musi być potwierdzona przez jednostkę oceniającą zgodność.

2. Dostawca kwalifikowanych usług zaufania świadczący kwalifikowane usługi zaufania:

a) informuje organ nadzoru o wszelkich zmianach w świadczeniu kwalifikowanych usług zaufania oraz o zamiarze zaprzestania swej działalności;

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

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

d) przed wejściem w stosunek umowny informuje, w jasny i szczegółowy sposób, 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 i zapewniają techniczne bezpieczeństwo i wiarygodność procesów przez niego obsługiwanych;

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

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

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

   (iii) można było sprawdzać autentyczność danych;

g) podejmuje odpowiednie środki zapobiegające fałszowaniu i kradzieży danych;

h) rejestruje i udostępnia przez odpowiedni okres, w tym po zaprzestaniu działalności przez kwalifikowanego dostawcę usług zaufania, wszelkie odpowiednie informacje dotyczące danych wydanych i otrzymanych przez kwalifikowanego dostawcę usług zaufania, w szczególności do celów przedstawienia dowodów w postępowaniach sądowych i do celów zapewnienia ciągłości usług. Rejestracja może odbywać się drogą elektroniczną;

i) ma aktualny plan zakończenia działalności, aby zapewnić ciągłość usług zgodnie z przepisami zweryfikowanymi przez organ nadzoru na mocy art. 17 ust. 4 lit. i);

j) zapewnia zgodne z prawem przetwarzanie danych osobowych zgodnie z dyrektywą 95/46/WE;

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

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

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

5. Komisja może w drodze aktów wykonawczych podać numery referencyjne norm dotyczących wiarygodnych systemów i produktów, które spełniają wymogi określone w ust. 2 lit. e) i f) niniejszego artykułu. W przypadku gdy wiarygodne systemy i produkty spełniają te standardy, 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.

SEKCJA 4

Podpisy elektroniczne

Artykuł 25

Skutki prawne podpisów elektronicznych

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

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

3. Kwalifikowany podpis elektroniczny oparty na kwalifikowanym certyfikacie wydanym w jednym państwie członkowskim jest uznawany za kwalifikowany podpis elektroniczny we wszystkich pozostałych państwach członkowskich.

Artykuł 26

Wymogi dla zaawansowanych podpisów elektronicznych

Zaawansowany podpis elektroniczny musi spełniać następujące wymogi:

a) jest unikalnie przyporządkowany podpisującemu;

b) umożliwia ustalenie tożsamości podpisującego;

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

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

Artykuł 27

Podpisy elektroniczne w usługach publicznych

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

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

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

4. Komisja może w drodze aktów wykonawczych podać numery referencyjne norm dotyczących zaawansowanych podpisów elektronicznych. W przypadku gdy zaawansowany podpis elektroniczny spełnia te normy, domniemywa się zgodność z wymogami dotyczącymi zaawansowanych podpisów elektronicznych, o których mowa w ust. 1 i 2 niniejszego artykułu i w art. 26. Te akty wykonawcze przyjmuje się zgodnie z procedurą sprawdzającą, o której mowa w art. 48 ust. 2.

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

Artykuł 28

Kwalifikowane certyfikaty podpisów elektronicznych

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

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

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

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

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

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

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

6. Komisja może w drodze aktów wykonawczych podać numery referencyjne norm dotyczących kwalifikowanych certyfikatów podpisów elektronicznych. W przypadku gdy kwalifikowany certyfikat podpisu elektronicznego spełnia te normy, 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.

Artykuł 29

Wymogi dla kwalifikowanych urządzeń do składania podpisu elektronicznego

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

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

Artykuł 30

Certyfikacja kwalifikowanych urządzeń do składania podpisu elektronicznego

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

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

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

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

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

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

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

Artykuł 31

Publikacja listy certyfikowanych kwalifikowanych urządzeń do składania podpisu elektronicznego

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

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

3. Komisja może w drodze aktów wykonawczych określić formaty i procedury mające zastosowanie na użytek ust. 1. Te akty wykonawcze przyjmuje się zgodnie z procedurą sprawdzającą, o której mowa w art. 48 ust. 2.

Artykuł 32

Wymogi dla walidacji kwalifikowanych podpisów elektronicznych

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

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

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

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

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

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

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

g) integralność podpisanych danych nie została naruszona;

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

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

3. Komisja może w drodze aktów wykonawczych podać numery referencyjne norm dotyczących walidacji kwalifikowanych podpisów elektronicznych. Jeżeli walidacja kwalifikowanych podpisów elektronicznych spełnia te normy, 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.

Artykuł 33

Kwalifikowana usługa walidacji kwalifikowanych podpisów elektronicznych

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

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

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

2. Komisja może w drodze aktów wykonawczych podać numery referencyjne norm dotyczących kwalifikowanej usługi walidacji, o której mowa w ust. 1. W przypadku gdy usługa walidacji kwalifikowanych podpisów elektronicznych spełnia te normy, 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.

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. Komisja może w drodze aktów wykonawczych podać numery referencyjne norm dotyczących kwalifikowanej usługi konserwacji kwalifikowanych podpisów elektronicznych. W przypadku gdy ustalenia w zakresie kwalifikowanej usługi konserwacji kwalifikowanych podpisów elektronicznych spełniają te normy, 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.

SEKCJA 5

Pieczęcie elektroniczne

Artykuł 35

Skutki prawne pieczęci elektronicznych

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

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

3. Kwalifikowana pieczęć elektroniczna oparta na kwalifikowanym certyfikacie wydanym w jednym państwie członkowskim jest uznawana za kwalifikowaną pieczęć elektroniczną we wszystkich pozostałych państwach członkowskich.

Artykuł 36

Wymogi dla zaawansowanych pieczęci elektronicznych

Zaawansowana pieczęć elektroniczna musi spełniać następujące wymogi:

a) jest unikalnie przyporządkowana podmiotowi składającemu pieczęć;

b) umożliwia ustalenie tożsamości podmiotu składającego pieczęć;

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

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

Artykuł 37

Pieczęcie elektroniczne w usługach publicznych

1. Jeżeli państwo członkowskie wymaga zaawansowanej pieczęci elektronicznej do skorzystania z usługi *online* oferowanej przez podmiot sektora publicznego lub w jego imieniu, to państwo członkowskie uznaje zaawansowane pieczęcie elektroniczne, zaawansowane pieczęcie

elektroniczne oparte na kwalifikowanym certyfikacie pieczęci elektronicznych i kwalifikowane pieczęcie elektroniczne co najmniej w formatach lub wykorzystujące metody określone w aktach wykonawczych, o których mowa w ust. 5.

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

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

4. Komisja może w drodze aktów wykonawczych podać numery referencyjne norm dotyczących zaawansowanych pieczęci elektronicznych. W przypadku gdy zaawansowana pieczęć elektroniczna spełnia te normy, domniemywa się zgodność z wymogami dotyczącymi zaawansowanych pieczęci elektronicznych, o których mowa w ust. 1 i 2 niniejszego artykułu i w art. 36. Te akty wykonawcze przyjmuje się zgodnie z procedurą sprawdzającą, o której mowa w art. 48 ust. 2.

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

Artykuł 38

Kwalifikowane certyfikaty pieczęci elektronicznej

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

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

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

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

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

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

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

6. Komisja może w drodze aktów wykonawczych podać numery referencyjne norm dotyczących kwalifikowanych certyfikatów pieczęci elektronicznych. W przypadku gdy kwalifikowany certyfikat pieczęci elektronicznej spełnia te normy, domniemywa się zgodność z wymogami określonymi w załączniku III. Te akty wykonawcze przyjmuje się zgodnie z procedurą sprawdzającą, o której mowa w art. 48 ust. 2.

Artykuł 39

Kwalifikowane urządzenia do składania pieczęci elektronicznej

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

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

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

Artykuł 40

Walidacja i konserwacja kwalifikowanych pieczęci elektronicznych

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

SEKCJA 6

Elektroniczne znaczniki czasu

Artykuł 41

Skutki prawne elektronicznych znaczników czasu

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

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

3. Kwalifikowany elektroniczny znacznik wydany w jednym państwie członkowskim jest uznawany za kwalifikowany elektroniczny znacznik czasu we wszystkich państwach członkowskich.

Artykuł 42

Wymogi dla kwalifikowanych elektronicznych znaczników czasu

1. Kwalifikowany elektroniczny znacznik czasu musi spełniać następujące wymogi:

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

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

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

2. Komisja może w drodze aktów wykonawczych podać numery referencyjne norm dotyczących powiązania daty i czasu z danymi oraz precyzyjnych źródeł czasu. W przypadku gdy powiązanie daty i czasu z danymi i precyzyjne źródło czasu spełniają te normy, 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.

SEKCJA 7

Usługi rejestrowanego doręczenia elektronicznego

Artykuł 43

Skutek prawny usługi rejestrowanego doręczenia elektronicznego

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

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

Artykuł 44

Wymogi dla kwalifikowanych usług rejestrowanego doręczenia elektronicznego

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

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

b) z dużą dozą pewności zapewniają identyfikację nadawcy;

c) zapewniają identyfikację adresata przed dostarczeniem danych;

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

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

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

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

2. Komisja może w drodze aktów wykonawczych podać numery referencyjne norm dotyczących procedur wysyłania i otrzymywania danych. W przypadku gdy proces wysyłania i otrzymywania danych spełnia te normy, 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.

SEKCJA 8

Uwierzytelnianie witryn internetowych

Artykuł 45

Wymogi dla kwalifikowanych certyfikatów uwierzytelniania witryn internetowych

1. Kwalifikowane certyfikaty uwierzytelniania witryn internetowych muszą spełniać wymogi określone w załączniku IV.

2. Komisja może w drodze aktów wykonawczych podać numery referencyjne norm dotyczących kwalifikowanych certyfikatów uwierzytelniania witryn internetowych. W przypadku gdy kwalifikowany certyfikat uwierzytelniania witryn internetowych spełnia te normy, domniemywa się zgodność z wymogami określonymi w załączniku IV. Te akty wykonawcze przyjmuje się zgodnie z procedurą sprawdzającą, o której mowa w art. 48 ust. 2.

ROZDZIAŁ IV

DOKUMENTY ELEKTRONICZNE

Artykuł 46

Skutki prawne dokumentów elektronicznych

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

ROZDZIAŁ V

PRZEKAZANIE UPRAWNIEŃ I PRZEPISY WYKONAWCZE

Artykuł 47

Wykonywanie przekazanych uprawnień

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

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

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

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

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

Artykuł 48

Procedura komitetowa

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

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

ROZDZIAŁ VI
PRZEPISY KOŃCOWE

Artykuł 49

Przegląd

Komisja dokona przeglądu stosowania niniejszego rozporządzenia i przekaże sprawozdanie Parlamentowi Europejskiemu i Radzie nie później niż dnia 1 lipca 2020 r. Komisja oceni w szczególności, czy należy zmienić zakres stosowania niniejszego rozporządzenia lub jego poszczególnych przepisów, w tym art. 6, art. 7 lit. f), art. 34, 43, 44 i 45, biorąc pod uwagę doświadczenia zdobyte przy stosowaniu niniejszego rozporządzenia, a także rozwój technologiczny, sytuację rynkową i prawną.

Do sprawozdania, o którym mowa w akapicie pierwszym, załączone zostaną w stosownych przypadkach wnioski ustawodawcze.

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.

Artykuł 50

Uchylenie

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

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

Artykuł 51

Środki przejściowe

1. Bezpieczne urządzenia do składania podpisu, których zgodność ustalono zgodnie z art. 3 ust. 4 dyrektywy 1999/93/WE, uznaje się za kwalifikowane urządzenia do składania podpisu elektronicznego na mocy niniejszego rozporządzenia.

2. Kwalifikowane certyfikaty wydane osobom fizycznym na mocy dyrektywy 1999/93/WE uznaje się za kwalifikowane certyfikaty podpisów elektronicznych na mocy niniejszego rozporządzenia do czasu ich wygaśnięcia.

3. Podmiot świadczący usługi certyfikacyjne, wydający kwalifikowane certyfikaty na mocy dyrektywy 1999/93/WE, przekazuje raport z oceny zgodności organowi nadzoru jak najszybciej, ale nie później niż dnia 1 lipca 2017 r. Do czasu przekazania takiego raportu z oceny zgodności i zakończenia oceny przez organ nadzoru podmiot świadczący usługi certyfikacyjne jest uważany za kwalifikowanego dostawcę usług zaufania w rozumieniu niniejszego rozporządzenia.

4. Jeżeli podmiot świadczący usługi certyfikacyjne, wydający kwalifikowane certyfikaty na mocy dyrektywy 1999/93/WE, nie przekaże raportu z oceny zgodności organowi nadzoru w terminie, o którym mowa w ust. 3, wówczas ten podmiot świadczący usługi certyfikacyjne, od dnia 2 lipca 2017 r., nie jest uważany za kwalifikowanego dostawcę usług zaufania w rozumieniu niniejszego rozporządzenia

Artykuł 52

Wejście w życie

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

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

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

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

mowa w art. 8 ust. 3 i art. 12 ust. 8;

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

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

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

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

Sporządzono w Brukseli dnia 23 lipca 2014 r.

W imieniu Parlamentu

M. SCHULZ

Przewodniczący

W imieniu Rady

S. GOZI

Przewodniczący

([1]) Dz.U. C 351 z 15.11.2012, s. 73.

([2]) Stanowisko Parlamentu Europejskiego z dnia 3 kwietnia 2014 r. (dotychczas nieopublikowane w Dzienniku Urzędowym) i decyzja Rady z dnia 23 lipca 2014 r.

([3]) Dyrektywa Parlamentu Europejskiego i Rady 1999/93/WE z dnia 13 grudnia 1999 r. w sprawie wspólnotowych ram w zakresie podpisów elektronicznych (Dz.U. L 13 z 19.1.2000, s. 12).

([4]) Dz.U. C 50 E z 21.2.2012, s. 1.

([5]) Dyrektywa 2006/123/WE Parlamentu Europejskiego i Rady z dnia 12 grudnia 2006 r. dotycząca usług na rynku wewnętrznym (Dz.U. L 376 z 27.12.2006, s. 36).

([6]) Dyrektywa Parlamentu Europejskiego i Rady 2011/24/UE z dnia 9 marca 2011 r. w sprawie stosowania praw pacjentów w transgranicznej opiece zdrowotnej (Dz.U. L 88 z 4.4.2011, s. 45).

([7]) Dyrektywa 95/46/WE Parlamentu Europejskiego i Rady z dnia 24 października 1995 r. w sprawie ochrony osób fizycznych w zakresie przetwarzania danych osobowych i swobodnego przepływu tych danych (Dz.U. L 281 z 23.11.1995, s. 31).

([8]) Decyzja Rady 2010/48/WE z dnia 26 listopada 2009 r. w sprawie zawarcia przez Wspólnotę Europejską Konwencji Narodów Zjednoczonych o prawach osób niepełnosprawnych (Dz.U. L 23 z 27.1.2010, s. 35).

([9]) Rozporządzenie Parlamentu Europejskiego i Rady (WE) nr 765/2008 z dnia 9 lipca 2008 r. ustanawiające wymagania w zakresie akredytacji i nadzoru rynku odnoszące się do warunków wprowadzania produktów do obrotu i uchylające rozporządzenie (EWG) nr 339/93 (Dz.U. L 218 z 13.8.2008, s. 30).

([10]) Decyzja Komisji 2009/767/WE z dnia 16 października 2009 r. ustanawiająca środki ułatwiające korzystanie z procedur realizowanych drogą elektroniczną poprzez „pojedyncze punkty kontaktowe" zgodnie z dyrektywą 2006/123/WE Parlamentu Europejskiego i Rady dotyczącą usług na rynku wewnętrznym (Dz.U. L 274 z 20.10.2009, s. 36).

([11]) Decyzja Komisji 2011/130/UE z dnia 25 lutego 2011 r. w sprawie ustalenia minimalnych wymagań dotyczących transgranicznego przetwarzania dokumentów podpisanych elektronicznie przez właściwe organy zgodnie z dyrektywą 2006/123/WE Parlamentu Europejskiego i Rady dotyczącą usług na rynku wewnętrznym (Dz.U. L 53 z 26.2.2011, s. 66).

([12]) Rozporządzenie Parlamentu Europejskiego i Rady (UE) nr 182/2011 z dnia 16 lutego 2011 r. ustanawiające przepisy i zasady ogólne dotyczące trybu kontroli przez państwa członkowskie wykonywania uprawnień wykonawczych przez Komisję (Dz.U. L 55 z 28.2.2011, s. 13).

([13]) Rozporządzenie (WE) nr 45/2001 Parlamentu Europejskiego i Rady z dnia 18 grudnia 2000 r. o ochronie osób fizycznych w związku z przetwarzaniem danych osobowych przez instytucje i organy wspólnotowe i o swobodnym przepływie takich danych (Dz.U. L 8 z 12.1.2001, s. 1).

([14]) Dz.U. C 28 z 30.1.2013, s. 6.

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

ZAŁĄCZNIK I

WYMOGI DLA KWALIFIKOWANYCH CERTYFIKATÓW PODPISÓW ELEKTRONICZNYCH

Kwalifikowane certyfikaty podpisów elektronicznych zawierają następujące informacje:

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

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

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

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

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

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

e) dane dotyczące początku i końca okresu ważności certyfikatu;

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

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

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

i) miejsce usług, z którego można skorzystać w celu złożenia zapytania o status ważności kwalifikowanego certyfikatu;

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

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.

3. Dane służące do składania podpisu elektronicznego mogą być generowane lub zarządzane w imieniu podpisującego wyłącznie przez kwalifikowanego dostawcę usług zaufania.

4. Bez uszczerbku dla pkt 1 lit. d) kwalifikowani dostawcy usług zaufania zarządzający danymi służącymi do składania podpisu elektronicznego w imieniu podpisującego mogą kopiować dane służące do składania podpisu elektronicznego wyłącznie w celu utworzenia kopii zapasowej, pod warunkiem że spełnione są następujące wymogi:

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

   b) liczba skopiowanych zbiorów danych nie przekracza minimum niezbędnego do zapewnienia ciągłości usługi.

ZAŁĄCZNIK III

WYMOGI DLA KWALIFIKOWANYCH CERTYFIKATÓW PIECZĘCI ELEKTRONICZNYCH

Kwalifikowane certyfikaty pieczęci elektronicznych zawierają:

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

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

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

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

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

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

e) dane dotyczące początku i końca okresu ważności certyfikatu;

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

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

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

i) miejsce usług, z których można skorzystać w celu złożenia zapytania o status ważności kwalifikowanego certyfikatu;

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

ZAŁĄCZNIK IV

WYMOGI DLA KWALIFIKOWANYCH CERTYFIKATÓW UWIERZYTELNIANIA WITRYN INTERNETOWYCH

Kwalifikowane certyfikaty uwierzytelniania witryn internetowych zawierają:

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

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

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

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

c) w odniesieniu do osób fizycznych: co najmniej imię i nazwisko osoby, której wydano certyfikat, lub pseudonim. Jeżeli używany jest pseudonim, wymaga to wyraźnego wskazania;

w odniesieniu do osób prawnych: co najmniej nazwę osoby prawnej, której wydano certyfikat, i, w stosownym przypadku, numer rejestrowy zgodnie z oficjalnym rejestrem;

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

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

f) dane dotyczące początku i końca okresu ważności certyfikatu;

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

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

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

j) miejsce usług statusu ważności certyfikatu, z których można skorzystać w celu złożenia zapytania o status ważności kwalifikowanego certyfikatu.

Top