KOMISJA EUROPEJSKA

Bruksela, dnia 4.6.2012 r.
COM(2012) 238 final

2012/0146 (COD)

Wniosek

ROZPORZĄDZENIE PARLAMENTU EUROPEJSKIEGO I RADY

w sprawie identyfikacji elektronicznej i usług zaufania w odniesieniu do transakcji elektronicznych na rynku wewnętrznym

(Tekst mający znaczenie dla EOG)

{SWD(2012) 135 final}
{SWD(2012) 136 final}

UZASADNIENIE

1. KONTEKST WNIOSKU

W niniejszym uzasadnieniu wyjaśniono proponowane ramy prawne, których celem jest zwiększenie zaufania do transakcji elektronicznych na rynku wewnętrznym.

Budowanie zaufania do internetu jest kluczowym elementem rozwoju gospodarczego. Brak zaufania sprawia, że konsumenci, przedsiębiorstwa i organy administracji odnoszą się z wahaniem do przeprowadzania transakcji elektronicznych i korzystania z nowych usług.

W Europejskiej agendzie cyfrowej[1] określono istniejące bariery dla rozwoju cyfrowego Europy i zaproponowano akty prawne dotyczące podpisów elektronicznych (główne działanie 3) oraz wzajemnego uznawania elektronicznej identyfikacji i elektronicznego uwierzytelniania (główne działanie 16), które mają ustanowić precyzyjne ramy prawne w celu wyeliminowania rozdrobnienia i braku interoperacyjności, wzmocnienia obywatelstwa cyfrowego i zapobiegania cyberprzestępczości. Wprowadzenie przepisów prawnych zapewniających wzajemne uznawanie elektronicznej identyfikacji i elektronicznego uwierzytelniania w całej UE oraz przegląd dyrektywy w sprawie podpisów elektronicznych stanowią również kluczowe działania przewidziane w Akcie o jednolitym rynku[2] w celu utworzenia jednolitego rynku cyfrowego. W Planie działania na rzecz stabilności i wzrostu[3] podkreślono kluczowe znaczenie dla rozwoju gospodarki cyfrowej, jakie będzie mieć przyszła podstawa prawna w zakresie wzajemnego uznawania i akceptowania elektronicznej identyfikacji i elektronicznego uwierzytelniania ponad granicami.

Proponowane ramy prawne, które obejmują rozporządzenie Parlamentu Europejskiego i Rady w sprawie identyfikacji elektronicznej i usług zaufania w odniesieniu do transakcji elektronicznych na rynku wewnętrznym, mają umożliwiać bezpieczne i płynne interakcje drogą elektroniczną między przedsiębiorstwami, obywatelami i organami administracji publicznej, zwiększając przez to skuteczność publicznych i prywatnych usług online, e-biznesu i handlu elektronicznego w UE.

Obowiązujący akt prawny UE – dyrektywa 1999/93/WE w sprawie wspólnotowych ram w zakresie podpisów elektronicznych[4] – obejmuje zasadniczo tylko podpisy elektroniczne. Brakuje szczegółowych transgranicznych i międzysektorowych ram UE, które odnosiłyby się do bezpiecznych, wiarygodnych i łatwych w użyciu transakcji elektronicznych oraz obejmowałyby identyfikację elektroniczną, uwierzytelnianie elektroniczne i podpisy elektroniczne.

Celem działania jest wzmocnienie i rozszerzenie istniejących przepisów w taki sposób, aby obejmowały wzajemne uznawanie i akceptowanie na szczeblu UE krajowych systemów identyfikacji elektronicznej i innych podstawowych elektronicznych usług zaufania, które są z nimi powiązane.

---

1 COM(2010) 245 z 19.5.2010.
2 COM(2011) 206 wersja ostateczna z 13.4.2011.
3 COM(2011) 669 z 12.10.2011.
4 Dz.U.L 13 z 19.1.2000, s. 12.

2. WYNIKI KONSULTACJI Z ZAINTERESOWANYMI STRONAMI I OCENY SKUTKÓW

Niniejsza inicjatywa jest wynikiem szeroko zakrojonych konsultacji dotyczących przeglądu obecnych ram prawnych dotyczących podpisów elektronicznych; w ramach tych konsultacji Komisja uzyskała opinie państw członkowskich, Parlamentu Europejskiego oraz innych zainteresowanych stron[5]. Internetowe konsultacje społeczne uzupełnił „Panel testowy MŚP" mający na celu określenie konkretnych opinii i potrzeb MŚP, a także inne konsultacje przeprowadzone ze stosownymi zainteresowanymi stronami[6] [7]. Komisja zainicjowała również szereg analiz dotyczących identyfikacji elektronicznej, uwierzytelniania elektronicznego, podpisów elektronicznych oraz powiązanych z nimi usług zaufania (eIAS).

W czasie konsultacji okazało się, że zdecydowana większość zainteresowanych stron widzi potrzebę przeglądu obecnych ram w celu uzupełnienia luk w prawie pozostawionych przez dyrektywę w sprawie podpisów elektronicznych. W ich odczuciu pozwoliłoby to lepiej reagować na wyzwania wynikające z szybkiego rozwoju nowych technologii (zwłaszcza w dziedzinie stacjonarnego dostępu do sieci i dostępu mobilnego) oraz nasilonej globalizacji, przy jednoczesnym utrzymaniu technologicznej neutralności ram prawnych.

Zgodnie z polityką lepszego stanowienia prawa Komisja przeprowadziła ocenę skutków opcji politycznych. Oceniono trzy zestawy wariantów politycznych odnoszące się odpowiednio do 1) zakresu nowych ram, 2) instrumentu prawnego i 3) wymaganego poziomu nadzoru[8]. Okazało się, że preferowanym wariantem jest zwiększenie pewności prawa, usprawnienie koordynacji krajowego nadzoru, zapewnienie wzajemnego uznawania i akceptowania systemów identyfikacji elektronicznej oraz włączenie powiązanych podstawowych usług zaufania. Z oceny skutków wynikło, że w ten sposób można osiągnąć istotne zwiększenie pewności prawa, bezpieczeństwa i zaufania w obszarze transgranicznych transakcji elektronicznych, co z kolei przyczyni się do zmniejszenia rozdrobnienia rynku.

---

5 Szczegółowe informacje na temat konsultacji znajdują się na stronie internetowej: http://ec.europa.eu/information_society/policy/esignature/eu_legislation/revision.

6 W dniu 10 marca 2011 r. zorganizowano warsztaty z udziałem zainteresowanych przedstawicieli sektorów publicznego i prywatnego oraz środowiska akademickiego w celu omówienia środków legislacyjnych, które należy wprowadzić, aby sprostać istniejącym wyzwaniom. Inicjatywa miała formę interaktywnego forum służącego do wymiany poglądów i do przedstawienia różnych stanowisk w kwestiach podniesionych podczas konsultacji społecznych. Wiele organizacji spontanicznie nadesłało swoje stanowiska.

7 Należy zaznaczyć, że polska prezydencja UE zorganizowała następujące spotkania z państwami członkowskimi: w Warszawie w dniu 9 listopada 2011 r. w sprawie podpisu elektronicznego i w Poznaniu w dniu 17 listopada 2011 r. w sprawie identyfikacji elektronicznej. W dniu 25 stycznia 2012 r. Komisja zorganizowała warsztaty dla państw członkowskich w celu omówienia pozostałych kwestii dotyczących identyfikacji elektronicznej, uwierzytelniania elektronicznego i podpisów elektronicznych.

8 W ramach pierwszego zestawu przeanalizowano cztery warianty: uchylenie dyrektywy w sprawie podpisów elektronicznych; brak zmian w prowadzonej polityce; zwiększenie pewności prawa, usprawnienie koordynacji krajowego nadzoru wraz z zapewnieniem wzajemnego uznawania i akceptowania identyfikacji elektronicznej w całej UE; a jako czwarty wariant – rozszerzenie i włączenie niektórych powiązanych usług zaufania. Drugi zestaw obejmował ocenę względnych zalet możliwości wprowadzenia uregulowań za pośrednictwem jednego lub dwóch instrumentów oraz za pośrednictwem dyrektywy zamiast rozporządzenia. W ramach trzeciego zestawu przeanalizowano możliwości związane z wdrożeniem krajowych systemów nadzoru opartych na wspólnych podstawowych wymaganiach dotyczących nadzoru zamiast unijnego systemu nadzoru. Każdy wariant został oceniony przy udziale grupy, w skład której wchodziły wszystkie zainteresowane dyrekcje generalne Komisji, pod kątem skuteczności w osiąganiu celów polityki, gospodarczego wpływu na zainteresowane strony (w tym na budżet instytucji UE), skutków społecznych i środowiskowych oraz skutków w postaci obciążeń administracyjnych.

3. ASPEKTY PRAWNE WNIOSKU

3.1 Podstawa prawna

Podstawą niniejszego wniosku jest art. 114 TFUE, który dotyczy przyjmowania środków w celu znoszenia istniejących barier w funkcjonowaniu rynku wewnętrznego. Obywatele, przedsiębiorstwa i organy administracji będą mogły korzystać ponad granicami ze wzajemnego uznawania i akceptowania identyfikacji elektronicznej, uwierzytelniania elektronicznego i podpisu elektronicznego, a także z innych usług zaufania, w sytuacjach kiedy będzie zachodzić potrzeba uzyskania dostępu do elektronicznych procedur lub zrealizowania elektronicznych transakcji.

Uważa się, że rozporządzenie jest najstosowniejszym instrumentem prawnym. Bezpośrednia możliwość stosowania rozporządzenia zgodnie z art. 288 TFUE doprowadzi do ograniczenia rozdrobnienia prawnego i zagwarantuje lepszą pewność prawa poprzez wprowadzenie zharmonizowanego zbioru przepisów podstawowych przyczyniających się do funkcjonowania rynku wewnętrznego.

3.2 Pomocniczość i proporcjonalność

Aby działanie UE uznać za uzasadnione, konieczne jest przestrzeganie zasady pomocniczości:

a) Transnarodowy charakter problemu (kryterium konieczności)

Transnarodowy charakter identyfikacji elektronicznej, uwierzytelniania elektronicznego i podpisu elektronicznego sprawia, że konieczne jest podjęcie działań na poziomie UE. Wewnętrzne (tj. krajowe) działania nie byłyby wystarczające dla osiągnięcia celów i zrealizowania zadań wyznaczonych w strategii Europa 2020[9]. Natomiast z doświadczenia wynika, że środki krajowe w rzeczywistości tworzą bariery dla ogólnounijnej interoperacyjności podpisów elektronicznych i że obecnie mają taki sam wpływ na identyfikację elektroniczną, uwierzytelnianie elektroniczne i powiązane usługi zaufania. UE powinna zatem stworzyć ramy umożliwiające interoperacyjność transgraniczną i usprawnić koordynację między krajowymi systemami nadzoru. Identyfikacji elektronicznej nie można jednak uwzględnić w rozporządzeniu, którego dotyczy wniosek, w taki sam ogólny sposób, jak w przypadku pozostałych elektronicznych usług zaufania, ponieważ wydawanie środków identyfikacji jest prerogatywą krajową. We wniosku skupiono się zatem wyłącznie na transgranicznych aspektach identyfikacji elektronicznej.

Rozporządzenie, którego dotyczy wniosek, stwarza równe szanse dla przedsiębiorstw świadczących usługi zaufania, gdyż w chwili obecnej istniejące różnice w krajowych uregulowaniach prawnych często oznaczają brak pewności prawa i dodatkowe obciążenia administracyjne. Uzyskanie większej pewności prawa możliwe jest dzięki wyraźnemu podjęciu zobowiązań do akceptowania kwalifikowanych usług zaufania przez państwa członkowskie, co dodatkowo zachęci przedsiębiorców do prowadzenia działalności za granicą. Przykładowo, przedsiębiorstwa będą mogły uczestniczyć drogą elektroniczną w przetargach publicznych ogłaszanych przez poszczególne państwa członkowskie bez obaw, że ich podpisy elektroniczne zostaną zablokowane ze względu na szczególne wymogi krajowe i problemy związane z brakiem interoperacyjności. Podobnie, przedsiębiorstwa będą mieć możliwość elektronicznego podpisywania umów ze swoimi odpowiednikami w innych

[9] Komunikat Komisji: *Europa 2020.* Strategia na rzecz inteligentnego i zrównoważonego rozwoju sprzyjającego włączeniu społecznemu, COM(2010) 2020, 3.3.2010.

państwach członkowskich bez obaw, że utrudnią im to inne wymogi prawne dotyczące takich usług zaufania jak pieczęcie elektroniczne, dokumenty elektroniczne i elektroniczne znaczniki czasu. Podczas wysyłania wezwań do wykonania umowy z jednego państwa członkowskiego do drugiego zapewniona będzie ich ważność prawna w obu państwach członkowskich. Bardziej wiarygodny będzie również handel w środowisku elektronicznym, ponieważ kupujący będą mieć możliwość sprawdzenia, czy korzystają ze strony internetowej, która rzeczywiście jest stroną sprzedawcy, czy też jest może stroną fałszywą.

Wzajemnie uznawane środki identyfikacji elektronicznej oraz powszechnie akceptowane podpisy elektroniczne ułatwią transgraniczne świadczenie licznych usług na rynku wewnętrznym i umożliwią przedsiębiorstwom prowadzenie działań za granicą bez konieczności zmagania się przeszkodami wynikającymi z kontaktów z organami administracji publicznej. W praktyce będzie to oznaczało znaczne zwiększenie efektywności działań administracyjnych – zarówno dla przedsiębiorstw, jak i dla obywateli. Przykładowo, student będzie mógł się zapisać na studia w innym kraju drogą elektroniczną, obywatel będzie mógł przez internet złożyć deklarację podatkową w innym kraju, a pacjent będzie mieć elektroniczny dostęp do swoich danych medycznych. Jeżeli nie wprowadzony zostanie wzajemnie uznawany środek identyfikacji elektronicznej, lekarz nie będzie mieć dostępu do danych niezbędnych do podjęcia leczenia pacjenta i konieczne będzie ponowne przeprowadzenie tych samych badań.

b) Wartość dodana (test efektywności)

Cele przedstawione powyżej nie zostały obecnie osiągnięte poprzez dobrowolną koordynację między państwami członkowskimi i nie wydaje się, aby miało to nastąpić w najbliższej przyszłości. Taki stan rzeczy prowadzi do powielania działań i wyznaczania odmiennych norm, wpływa na transnarodowe aspekty efektów zewnętrznych wynikających z ICT oraz powoduje utrudnienia administracyjne związane z ustanowieniem takiej koordynacji w drodze porozumień dwustronnych i wielostronnych.

Ponadto konieczność rozwiązania takich problemów jak: a) brak pewności prawa wynikający z niejednolitych przepisów krajowych będących efektem rozbieżnych wykładni dyrektywy w sprawie podpisu elektronicznego oraz b) brak interoperacyjności między systemami podpisu elektronicznego funkcjonującymi na szczeblu krajowym jako skutek niejednolitego stosowania norm technicznych, wymaga takiej koordynacji między państwami członkowskimi UE, jaką można skuteczniej prowadzić na szczeblu UE.

3.3 Szczegółowe omówienie wniosku

3.3.1 ROZDZIAŁ I – PRZEPISY OGÓLNE

W art. 1 określono przedmiot rozporządzenia.

W art. 2 określono zakres rozporządzenia.

Artykuł 3 zawiera definicje terminów użytych w rozporządzeniu. Niektóre definicje pochodzą z dyrektywy 1999/93/WE, inne zostały doprecyzowane i uzupełnione nowymi elementami, a oprócz tego dodano również nowe definicje.

W art. 4 określono zasady rynku wewnętrznego w kontekście terytorialnego stosowania rozporządzenia. Wyraźnie wspomniano o braku ograniczeń w zakresie swobody świadczenia usług i swobodnego przepływu produktów.

3.3.2 ROZDZIAŁ II – IDENTYFIKACJA ELEKTRONICZNA

W art. 5 przewidziano wzajemne uznawanie i akceptowanie środków identyfikacji elektronicznej stanowiących część systemu, który będzie zgłoszony Komisji zgodnie z warunkami określonymi w rozporządzeniu. Większość państw członkowskich UE posiada pewną formę systemu identyfikacji elektronicznej. Formy te różnią się jednak w wielu aspektach. Brak wspólnej podstawy prawnej nakładającej na każde państwo członkowskie obowiązek uznawania i akceptowania środków identyfikacji elektronicznej wydanych w innych państwach członkowskich w celu zapewnienia dostępu do usług online wraz z nieodpowiednią transgraniczną interoperacyjnością krajowych systemów identyfikacji elektronicznej tworzą bariery, które nie pozwalają obywatelom i przedsiębiorstwom korzystać w pełni z jednolitego rynku cyfrowego. Wzajemne uznawanie i akceptowanie każdego środka identyfikacji elektronicznej objętego systemem zgłoszonym na podstawie niniejszego rozporządzenia jest równoznaczne ze zniesieniem wspomnianych barier prawnych.

Rozporządzenie nie nakłada na państwa członkowskie obowiązku wprowadzania lub zgłaszania systemów identyfikacji elektronicznej, lecz nakazuje uznawać i akceptować zgłoszone środki identyfikacji elektronicznej dla tych usług, w przypadku których identyfikacja elektroniczna jest wymagana, aby można było uzyskać dostęp na szczeblu krajowym. Potencjalne korzyści skali wynikające z transgranicznego stosowania zgłoszonych środków identyfikacji elektronicznej oraz elektronicznych systemów uwierzytelniania mogą zachęcić państwa członkowskie do zgłaszania swoich systemów identyfikacji elektronicznej. W art. 6 wyznaczono pięć warunków dotyczących zgłaszania systemów identyfikacji elektronicznej.

Państwa członkowskie mogą zgłaszać systemy identyfikacji elektronicznej, które akceptują zgodnie z swoją jurysdykcją w przypadkach, w których identyfikacja elektroniczna jest wymagana na potrzeby usług publicznych. Zgodnie z dodatkowym wymaganiem odpowiednie środki identyfikacji elektronicznej muszą być wydawane przez państwo członkowskie zgłaszające system, w jego imieniu lub co najmniej na jego odpowiedzialność.

Państwa członkowskie muszą zapewnić jednoznaczne powiązanie między danymi związanymi z identyfikacją elektroniczną a osobą, której identyfikacja ta dotyczy. Ten obowiązek nie oznacza, że jedna osoba nie może korzystać z kliku środków identyfikacji elektronicznej, lecz wszystkie takie środki muszą być powiązane z tą samą osobą.

Wiarygodność identyfikacji elektronicznej zależy od dostępności środków uwierzytelniania (tzn. możliwości sprawdzenia ważności danych powiązanych z identyfikacją elektroniczną). Rozporządzenie nakłada na zgłaszające państwa członkowskie obowiązek nieodpłatnego zapewnienia stronom trzecim uwierzytelniania online. Mechanizm uwierzytelniania musi być dostępny bez przerwy. Stronom ufającym polegającym się na takim uwierzytelnieniu nie należy narzucać żadnych szczegółowych wymagań technicznych w zakresie sprzętu lub oprogramowania. Ten przepis nie ma zastosowania do wymagań mających zastosowanie do użytkowników (posiadaczy) środków identyfikacji elektronicznej, które są niezbędne z technicznego punktu widzenia do używania środków identyfikacji elektronicznej, takich jak czytniki kart.

Państwa członkowskie muszą przyjąć odpowiedzialność za jednoznaczność powiązania (tj. za to, aby dane identyfikacyjne przypisane jednej osobie nie zostały przypisane żadnej innej osobie) i za mechanizm uwierzytelniający (tj. za możliwość sprawdzenia ważności danych związanych z identyfikacją elektroniczną). Odpowiedzialność państw członkowskich nie

obejmuje innych aspektów procesu identyfikacji ani żadnych transakcji wymagających identyfikacji.

W art. 7 przedstawiono zasady zgłaszania Komisji systemów identyfikacji elektronicznej.

Celem art. 8 jest zapewnienie interoperacyjności technicznej zgłoszonych systemów identyfikacji w ramach podejścia opartego na koordynacji, w tym za pomocą aktów delegowanych.

3.3.3 ROZDZIAŁ III – USŁUGI ZAUFANIA

3.3.3.1 Sekcja 1 – Przepisy ogólne

W art. 9 określono zasady dotyczące odpowiedzialności dostawców niekwalifikowanych usług zaufania i dostawców kwalifikowanych usług zaufania. Opiera się on na art. 6 dyrektywy 1999/93/WE i rozszerza uprawnienia do odszkodowania za szkodę spowodowaną przez działającego bez należytej staranności dostawcę usług zaufania, który nie postępuje zgodnie z dobrymi praktykami z zakresu bezpieczeństwa, co prowadzi do naruszenia bezpieczeństwa mającego poważny wpływ na usługę.

W art. 10 opisano mechanizm uznawania i akceptowania kwalifikowanych usług zaufania świadczonych przez dostawcę z siedzibą w państwie trzecim. Opiera się on na art. 7 dyrektywy 1999/93/WE, lecz zachowuje jedyny praktycznie wykonalny wariant, zgodnie z którym dopuszcza się takie uznawanie na podstawie umowy międzynarodowej między Unią Europejską a państwami trzecimi lub organizacjami międzynarodowymi.

W art. 11 określono zasady ochrony i minimalizacji danych. Opiera się on na art. 8 dyrektywy 1999/93/WE.

Na mocy art. 12 udostępnia się usługi zaufania osobom niepełnosprawnym.

3.3.3.2 Sekcja 2 – Nadzór

W art. 13 nałożono na państwa członkowskie obowiązek powołania organów nadzorczych, na podstawie art. 3 ust. 3 dyrektywy 1999/93/WE, a jednocześnie sprecyzowano i rozszerzono zakres ich kompetencji w odniesieniu do dostawców usług zaufania i dostawców kwalifikowanych usług zaufania.

W art. 14 wprowadzono bezpośredni mechanizm wzajemnej pomocy między organami nadzorczymi w państwach członkowskich w celu ułatwienia transgranicznego nadzoru nad dostawcami usług zaufania. Ustanowiono w nim przepisy dotyczące wspólnych działań i prawa organów nadzorczych do uczestnictwa w takich działaniach.

W art. 15 nałożono na dostawców niekwalifikowanych usług zaufania i dostawców kwalifikowanych usług zaufania obowiązek wdrożenia odpowiednich środków technicznych i organizacyjnych na potrzeby bezpieczeństwa ich działalności. Ponadto właściwe organy nadzorcze muszą być informowane o wszelkich przypadkach naruszenia bezpieczeństwa. W stosownych przypadkach organy te przekazują informacje organom nadzorczym innych państw członkowskich i podają je do publicznej wiadomości bezpośrednio lub za pośrednictwem zainteresowanego dostawcy usług zaufania.

W art. 16 określono warunki nadzorowania dostawców kwalifikowanych usług zaufania oraz usług świadczonych przez tych dostawców. Na dostawców kwalifikowanych usług zaufania nałożono obowiązek poddawania się corocznemu audytowi przeprowadzanemu przez uznany i niezależny organ, po to aby organ nadzorczy zyskał potwierdzenie, że dostawcy wypełniają zobowiązania ustanowione na mocy rozporządzenia. Ponadto w art. 16 ust. 2 przyznano organowi nadzorczemu prawo do przeprowadzania audytów na miejscu w dowolnym czasie w odniesieniu do dostawców kwalifikowanych usług zaufania. Organ nadzorczy jest również uprawniony do wydawania dostawcom kwalifikowanych usług zaufania wiążących instrukcji dotyczących usuwania, w proporcjonalny sposób, wszelkich przypadków niespełnienia wymagań stwierdzonych podczas audytu bezpieczeństwa.

Artykuł 17 dotyczy działania organu nadzorczego podejmowanego na wniosek dostawcy usług zaufania, który zamierza uruchomić kwalifikowaną usługę zaufania.

W art. 18 przewidziano sporządzanie zaufanych list[10] zawierających informacje o dostawcach kwalifikowanych usług zaufania objętych nadzorem oraz o oferowanych przez nich usługach. Informacje muszą być publicznie dostępne za pośrednictwem wspólnego szablonu w celu ułatwienia ich automatycznego użycia i zapewnienia odpowiedniego poziomu szczegółowości.

W art. 19 określono wymagania, które dostawcy kwalifikowanych usług zaufania muszą spełniać, aby mogli być za takich uznani. Artykuł opiera się na załączniku II dyrektywy 1999/93/WE.

3.3.3.3 Sekcja 3 – Podpis elektroniczny

W art. 20 określono zasady dotyczące prawnego skutku podpisów elektronicznych osób fizycznych. Doprecyzowano i rozszerzono art. 5 dyrektywy 1999/93/WE wprowadzający bezpośredni obowiązek nadawania kwalifikowanym podpisom elektronicznym takich samych skutków prawnych, jakie wywołują podpisy własnoręczne. Ponadto państwa członkowskie muszą zapewnić transgraniczne akceptowanie kwalifikowanych podpisów elektronicznych w kontekście świadczenia usług publicznych i nie mogą wprowadzać dodatkowych wymagań, które mogłyby tworzyć przeszkody w używaniu takich podpisów.

W art. 21 określono wymagania dotyczące kwalifikowanych certyfikatów podpisów. Doprecyzowano załącznik I do dyrektywy 1999/93/WE poprzez usunięcie przepisów, które nie działały w praktyce (np. granice wartości transakcji).

W art. 22 określono wymagania dotyczące urządzeń do składania kwalifikowanego podpisu elektronicznego. Doprecyzowano wymagania związane z bezpiecznymi urządzeniami do składania podpisu, ustanowione w art. 3 ust. 5 dyrektywy 1999/93/WE, które obecnie na mocy niniejszego rozporządzenia należy traktować jako urządzenia do składania kwalifikowanego podpisu. Sprecyzowano również, że zakres funkcji urządzenia do składania podpisu może być znacznie szerszy niż tylko funkcje urządzenia zawierającego dane dotyczące składania podpisu. Komisja może również ustalić numery referencyjne norm dotyczących wymagań bezpieczeństwa w odniesieniu do urządzeń.

[10] Zaufane listy ustanowione na mocy decyzji Komisji 2009/767/WE zmienionej decyzją Komisji 2010/425/UE stanowią podstawę dla nowej decyzji Komisji w sprawie zaufanych list na mocy niniejszego rozporządzenia.

Na podstawie art. 3 ust. 4 dyrektywy 1999/93/WE w art. 23 wprowadzono również koncepcję certyfikacji urządzeń do składania kwalifikowanego podpisu elektronicznego w celu ustalenia ich zgodności z wymaganiami bezpieczeństwa ustanowionymi w załączniku II. Wszystkie państwa członkowskie muszą uznać, że urządzenia spełniają wymagania, jeżeli procedurę certyfikacji przeprowadził organ certyfikujący wyznaczony przez jedno z państw członkowskich. Zgodnie z art. 24 Komisja opublikuje pozytywną listę takich certyfikowanych urządzeń. Komisja może również ustalić numery referencyjne norm oceny bezpieczeństwa produktów informatycznych, o których mowa w art. 23 ust. 1.

Art. 24 dotyczy publikacji przez Komisję listy urządzeń do składania kwalifikowanego podpisu elektronicznego, po zgłoszeniu przez państwa członkowskie, że urządzenia te spełniają odpowiednie wymogi.

Artykuł 25 stanowi rozszerzenie zaleceń sformułowanych w załączniku IV do dyrektywy 1999/93/WE dotyczących wiążących wymagań w zakresie weryfikacji kwalifikowanych podpisów elektronicznych i ma na celu zwiększenie pewności prawa w odniesieniu do takiej weryfikacji.

W art. 26 określono warunki dotyczące kwalifikowanych usług weryfikacji.

W art. 27 określono warunek długoterminowego przechowywania kwalifikowanego podpisu elektronicznego. Jest to możliwe dzięki zastosowaniu procedur i technologii umożliwiających przedłużenie wiarygodności danych służących do weryfikacji kwalifikowanego podpisu elektronicznego poza okres ich technologicznej ważności, kiedy cyberprzestępcy mogą łatwo dokonać fałszerstwa.

3.3.3.4 Sekcja 4 – Pieczęcie elektroniczne

Art. 28 dotyczy skutków prawnych pieczęci elektronicznych osób fizycznych. Dla kwalifikowanej pieczęci elektronicznej ustanowiono specjalne domniemanie prawne, które gwarantuje autentyczność i integralność dokumentów elektronicznych, z którymi jest ona powiązana.

W art. 29 określono wymagania dotyczące kwalifikowanych certyfikatów pieczęci elektronicznych.

W art. 30 określono wymogi dotyczące certyfikacji urządzeń do wystawiania kwalifikowanych pieczęci elektronicznych i publikacji list tych urządzeń.

W art. 31 wyznaczono warunek weryfikacji i przechowywania kwalifikowanych pieczęci elektronicznych.

3.3.3.5 Sekcja 5 – Elektroniczny znacznik czasu

Art. 32 dotyczy skutków prawnych elektronicznych znaczników czasu. Dla kwalifikowanych elektronicznych znaczników czasu ustanowiono specjalne domniemanie prawne w odniesieniu do pewności czasu.

W art. 33 określono wymagania dotyczące kwalifikowanych elektronicznych znaczników czasu.

3.3.3.6 Sekcja 6 – Dokumenty elektroniczne

W art. 34 określono skutki prawne i warunki akceptowania dokumentów elektronicznych. Istnieje specjalne domniemanie prawne dotyczące autentyczności i integralności każdego dokumentu elektronicznego podpisanego za pomocą kwalifikowanego podpisu elektronicznego lub opatrzonego kwalifikowaną pieczęcią elektroniczną. Jeśli chodzi o akceptowanie dokumentów elektronicznych, w sytuacji gdy do celu świadczenia usługi publicznej wymagany jest oryginalny dokument lub uwierzytelniony odpis, przynajmniej dokumenty elektroniczne wydane przez osoby uprawnione do wydawania stosownych dokumentów i uznawane za oryginały lub uwierzytelnione odpisy zgodnie z przepisami krajowymi państwa członkowskiego pochodzenia akceptuje się w pozostałych państwach członkowskich bez konieczności spełnienia dodatkowych wymogów.

3.3.3.7 Sekcja 7 – Usługi przekazu elektronicznego

Artykuł 35 dotyczy skutków prawnych danych wysyłanych lub otrzymywanych przy użyciu usług przekazu elektronicznego. W przypadku kwalifikowanych usług przekazu elektronicznego przyjmuje się specjalne domniemanie prawne dotyczące integralności danych, które są wysyłane lub otrzymywane, oraz dokładności czasu wysłania lub otrzymania danych. W artykule przewidziano również wzajemne uznawanie kwalifikowanych usług przekazu elektronicznego na szczeblu UE.

W art. 36 określono wymagania dotyczące kwalifikowanych usług przekazu elektronicznego.

3.3.3.8 Sekcja 8 – Uwierzytelnianie witryn internetowych

Celem tej sekcji jest zapewnienie gwarancji uwierzytelnienia witryny internetowej w odniesieniu do właściciela witryny.

W art. 37 określono wymagania dotyczące kwalifikowanych certyfikatów uwierzytelniania witryn internetowych, które można wykorzystywać do zagwarantowania uwierzytelnienia witryny internetowej. Kwalifikowany certyfikat uwierzytelniania witryn internetowych zapewnia minimum wiarygodnych informacji na temat witryny internetowej i prawnego istnienia jej właściciela.

3.3.4 ROZDZIAŁ IV – AKTY DELEGOWANE

Artykuł 38 zawiera standardowe przepisy dotyczące korzystania z uprawnień, o których mowa w art. 290 TFUE (akty delegowane). W ten sposób prawodawca może przekazać Komisji uprawnienia do przyjęcia aktów o charakterze nieustawodawczym o zasięgu ogólnym, które uzupełniają lub zmieniają inne niż istotne elementy aktu ustawodawczego.

3.3.5 ROZDZIAŁ V – AKTY WYKONAWCZE

Artykuł 39 zawiera przepisy dotyczące procedury komitetowej niezbędnej do powierzenia Komisji uprawnień wykonawczych w przypadkach, gdy zgodnie z art. 291 TFUE konieczne są jednolite warunki wykonywania prawnie wiążących aktów Unii. Zastosowanie ma procedura sprawdzająca.

3.3.6 ROZDZIAŁ VI – PRZEPISY KOŃCOWE

W art. 40 nałożono na Komisję obowiązek przeprowadzenia oceny rozporządzenia i sporządzenia stosownego sprawozdania.

W art. 41 uchylono dyrektywę 1999/93/WE i przewidziano sprawne przejście z istniejącej infrastruktury podpisu elektronicznego na nowe wymagania zawarte w rozporządzeniu.

W art. 42 określono datę wejścia życie rozporządzenia.

4. WPŁYW NA BUDŻET

Konkretny wpływ wniosku na budżet dotyczy zadań powierzonych Komisji Europejskiej, zgodnie z oceną skutków finansowych regulacji towarzyszącą niniejszemu wnioskowi.

Niniejszy wniosek nie ma wpływu na wydatki operacyjne.

Ocena finansowych skutków regulacji towarzysząca wnioskowi dotyczącemu rozporządzenia obejmuje wpływ samego rozporządzenia na budżet.

2012/0146 (COD)

Wniosek

ROZPORZĄDZENIE PARLAMENTU EUROPEJSKIEGO I RADY

w sprawie identyfikacji elektronicznej i usług zaufania w odniesieniu do transakcji elektronicznych na rynku wewnętrznym

(Tekst mający znaczenie dla EOG)

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[11],

po zasięgnięciu opinii Europejskiego Inspektora Ochrony Danych[12],

stanowiąc zgodnie ze zwykłą procedurą ustawodawczą,

a także mając na uwadze, co następuje:

(1) Budowanie zaufania do internetu jest kluczowym elementem rozwoju gospodarczego. Brak zaufania sprawia, że konsumenci, przedsiębiorstwa i organy administracji odnoszą się z wahaniem do przeprowadzania transakcji elektronicznych i korzystania z nowych usług.

(2) Celem niniejszego rozporządzenia jest zwiększenie zaufania do transakcji elektronicznych na rynku wewnętrznym poprzez zapewnienie bezpiecznych i płynnych interakcji elektronicznych między przedsiębiorstwami, obywatelami i organami publicznymi, co pozwoli podnieść skuteczność publicznych i prywatnych usług online, e-biznesu i handlu elektronicznego w Unii.

(3) Dyrektywa Parlamentu Europejskiego i Rady 1999/93/WE z dnia 13 grudnia 1999 r. w sprawie wspólnotowych ram w zakresie podpisów elektronicznych[13] obejmuje głównie podpisy elektroniczne, nie zapewnia natomiast szczegółowych ram transgranicznych i międzysektorowych, które odnosiłyby się do bezpiecznych, wiarygodnych i łatwych do realizacji transakcji elektronicznych. Niniejsze rozporządzenie umacnia i poszerza dorobek tej dyrektywy.

---

11 Dz.U. C , , s. .

12 Dz.U. C , , s. .

13 Dz.U.L 13 z 19.1.2000, s. 12.

(4) W przygotowanej przez Komisję Europejskiej agendzie cyfrowej[14] stwierdzono, że rozdrobnienie rynku cyfrowego, brak interoperacyjności i rosnąca liczba cyberprzestępstw stanowią główne przeszkody w pozytywnym cyklu rozwoju gospodarki cyfrowej. W sprawozdaniu na temat obywatelstwa za 2010 r. Komisja ponownie podkreśliła konieczność rozwiązania głównych problemów, które uniemożliwiają obywatelom Europy czerpanie korzyści z jednolitego rynku cyfrowego i transgranicznych usług cyfrowych[15].

(5) Rada Europejska wezwała Komisję do utworzenia jednolitego rynku cyfrowego do 2015 r.[16] w celu osiągnięcia szybkiego postępu w kluczowych obszarach gospodarki cyfrowej oraz propagowania w pełni zintegrowanego jednolitego rynku cyfrowego[17] poprzez ułatwianie transgranicznego korzystania z usług online, ze szczególnym uwzględnieniem ułatwiania bezpiecznej identyfikacji i bezpiecznego uwierzytelniania.

(6) Rada wezwała Komisję do wsparcia rozwoju jednolitego rynku cyfrowego poprzez tworzenie warunków sprzyjających wzajemnemu transgranicznemu uznawaniu głównych aktywatorów, takich jak elektroniczna identyfikacja, dokumenty elektroniczne, podpisy elektroniczne i elektroniczne usługi przesyłowe, oraz sprzyjających interoperacyjności usług administracji elektronicznej w całej UE[18].

(7) Parlament Europejski podkreślił znaczenie bezpieczeństwa usług elektronicznych, zwłaszcza podpisów elektronicznych, i potrzebę stworzenia infrastruktury klucza publicznego (PKI) na poziomie ogólnoeuropejskim, a także wezwał Komisję do ustanowienia bramy europejskich organów weryfikacyjnych w celu zapewnienia transgranicznej interoperacyjności podpisów elektronicznych i podniesienia bezpieczeństwa transakcji przeprowadzanych przy użyciu Internetu[19].

(8) Dyrektywa 2006/123/WE Parlamentu Europejskiego i Rady z dnia 12 grudnia 2006 r. dotycząca usług na rynku wewnętrznym[20] nakłada na państwa członkowskie obowiązek utworzenia pojedynczych punktów kontaktowych, aby zapewnić możliwość łatwego wypełnienia wszystkich procedur i formalności dotyczących podejmowania i prowadzenia działalności usługowej na odległość i drogą elektroniczną poprzez odpowiedni pojedynczy punkt kontaktowy i w odpowiednich organach. Wiele usług online dostępnych za pośrednictwem pojedynczych punktów kontaktowych wymaga identyfikacji elektronicznej, uwierzytelnienia i podpisu.

(9) W większości przypadków dostawcy usług z innego państwa członkowskiego nie mogą korzystać ze swojej identyfikacji elektronicznej w celu zapewnienia sobie dostępu do tych usług, ponieważ krajowe systemy identyfikacji elektronicznej w ich kraju nie są uznawane i akceptowane w innych państwach członkowskich. Taka

---

14 COM(2010) 245 wersja ostateczna/2.

15 Sprawozdanie na temat obywatelstwa UE – 2010 r.: Usuwanie przeszkód w zakresie praw obywatelskich UE, COM(2010) 603 wersja ostateczna, pkt 2.2.2, s. 13.

16 4/2/2011: EUCO 2/1/11.

17 23/10/2011: EUCO 52/1/11.

18 Konkluzje Rady w sprawie europejskiego planu działań na rzecz administracji elektronicznej na lata 2011–2015, 3093. posiedzenie Rady ds. Transportu, Telekomunikacji i Energii, Bruksela 27 maja 2011 r.

19 Rezolucja Parlamentu Europejskiego z 21.9.2010 w sprawie pełnego ukształtowania rynku wewnętrznego w handlu elektronicznym, 21.9.10, P7_TA(2010)0320, i rezolucja Parlamentu Europejskiego z 15.6.2010 w sprawie zarządzania internetem: kolejne działania, P7_TA(2010)0208.

20 Dz.U.L 376 z 27.12.2006, s. 36.

bariera elektroniczna nie pozwala dostawcom usług w pełni korzystać z rynku wewnętrznego. Wzajemnie uznawane i akceptowane środki elektronicznej identyfikacji ułatwią transgraniczne świadczenie licznych usług na rynku wewnętrznym i umożliwią przedsiębiorstwom prowadzenie działań za granicą bez konieczności zmagania się przeszkodami wynikającymi z kontaktów z organami administracji publicznej.

(10) Dyrektywa Parlamentu Europejskiego i Rady 2011/24/UE z dnia 9 marca 2011 r. w sprawie stosowania praw pacjentów w transgranicznej opiece zdrowotnej[21] 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 i akceptowania identyfikacji elektronicznej i uwierzytelniania elektronicznego jest niezbędne, aby transgraniczna opieka zdrowotna dla obywateli Europy stała się rzeczywistością. Kiedy obywatele wyjeżdżają w celu podjęcia leczenia, ich dane medyczne muszą być dostępne w kraju, w którym prowadzone jest leczenie. Aby to umożliwić, konieczne jest stworzenie solidnych, bezpiecznych i wiarygodnych ram identyfikacji elektronicznej.

(11) Jednym z celów niniejszego rozporządzenia jest zniesienie istniejących barier w transgranicznym stosowaniu środków identyfikacji elektronicznej stosowanych w państwach członkowskich w celu uzyskania dostępu przynajmniej do usług publicznych. Celem niniejszego rozporządzenia nie jest ingerowanie w systemy zarządzania tożsamością elektroniczną i w powiązane z nimi infrastruktury ustanowione w państwach członkowskich. Jego celem jest zagwarantowanie bezpiecznej identyfikacji elektronicznej i bezpiecznego elektronicznego uwierzytelniania do celów korzystania z transgranicznych usług online oferowanych przez państwa członkowskie.

(12) 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 zgłaszania swoich systemów identyfikacji elektronicznej. Państwa członkowskie mogą same zdecydować, czy zgłosić wszystkie systemy identyfikacji elektronicznej stosowane na szczeblu krajowym do celów uzyskiwania dostępu przynajmniej do publicznych usług online lub konkretnych usług, czy zgłosić niektóre z tych systemów, czy też nie zgłaszać ich w ogóle.

(13) W rozporządzeniu należy ustanowić warunki dotyczące tego, które środki identyfikacji elektronicznej muszą być akceptowane i w jaki sposób należy zgłaszać 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 i akceptowaniu środków identyfikacji elektronicznej objętych zgłoszonymi systemami. Zasada wzajemnego uznawania i akceptacji powinna mieć zastosowanie, jeżeli zgłaszające państwo członkowskie spełniło warunki zgłaszania, a zgłoszenie zostało

[21] Dz.U.L 88 z 4.4.2011, s. 45.

opublikowane w *Dzienniku Urzędowym Unii Europejskiej*. Jednak dostęp do takich usług online i ich ostateczne udostępnienie wnioskodawcy powinny być ściśle powiązane z prawem do korzystania z takich usług na warunkach określonych w przepisach krajowych.

(14) Państwa członkowskie powinny mieć możliwość zdecydowania, czy w wydawanie środków identyfikacji elektronicznej należy zaangażować sektor prywatny oraz czy sektorowi prywatnemu należy umożliwić korzystanie ze środków identyfikacji elektronicznej objętych zgłoszonym systemem, w sytuacjach gdy identyfikacja jest konieczna, aby uzyskać dostęp do usług online i transakcji elektronicznych. Możliwość korzystania z takich środków identyfikacji elektronicznej sprawiłaby, iż sektor prywatny mógłby korzystać ze środków identyfikacji elektronicznej i elektronicznego uwierzytelniania stosowanych już powszechnie w wielu państwach członkowskich przynajmniej w celu uzyskiwania dostępu do usług publicznych, a przedsiębiorstwom i obywatelom ułatwiłaby transgraniczny dostęp do usług online. Aby ułatwić transgraniczne korzystanie ze środków identyfikacji elektronicznej przez sektor prywatny, możliwość uwierzytelniania zapewniona przez państwa członkowskie powinna być dostępna dla stron ufających bez rozróżniania między sektorem publicznym i sektorem prywatnym.

(15) Transgraniczne stosowanie środków identyfikacji elektronicznej objętych zgłoszonym systemem nakłada na państwa członkowskie obowiązek współpracy w zakresie zapewnienia interoperacyjności technicznej. Wyklucza to wszelkie krajowe szczegółowe przepisy techniczne nakładające na strony z innych krajów np. obowiązek instalowania specjalnego sprzętu lub oprogramowania w celu sprawdzenia i zatwierdzenia zgłoszonej identyfikacji elektronicznej. Z drugiej strony nieuniknione są techniczne wymagania wobec użytkowników, wynikające ze specyfikacji nieodłącznie powiązanych ze stosowaniem tokena (np. kart elektronicznych).

(16) Współpraca między państwami członkowskimi powinna mieć na celu zapewnienie interoperacyjności technicznej zgłoszonych 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, której celem powinno być wzajemne uznawanie systemów przez państwa członkowskie.

(17) W niniejszym rozporządzeniu należy również ustanowić ogólne ramy prawne dotyczące korzystania z elektronicznych usług zaufania. Nie należy jednak wprowadzać ogólnego obowiązku ich używania. W szczególności rozporządzenie nie powinno obejmować świadczenia usług opierających się na dobrowolnych porozumieniach zawartych na mocy prawa prywatnego. Nie powinno ono również obejmować aspektów związanych z zawieraniem i ważnością umów lub innych zobowiązań prawnych w przypadkach, w których istnieją wymagania dotyczące formy wprowadzone na mocy prawa krajowego lub unijnego.

(18) Aby wspierać ogólne transgraniczne korzystanie z elektronicznych usług zaufania, należy zapewnić możliwość używania ich jako dowodu w postępowaniach sądowych we wszystkich państwach członkowskich.

(19) 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 zatwierdzenia ich na szczeblu krajowym jako kwalifikowane usługi zaufania.

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

(21) 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 wymagania niniejszego rozporządzenia.

(22) Aby zwiększyć zaufanie obywateli do rynku wewnętrznego i promować korzystanie z usług i produktów zaufania, należy wprowadzić pojęcia kwalifikowanych usług zaufania i dostawcy kwalifikowanych usług zaufania w celu wskazania wymagań i obowiązków mających zapewnić wysoki poziom bezpieczeństwa wszystkich świadczonych lub wykorzystywanych kwalifikowanych usług i produktów zaufania.

(23) Zgodnie z zobowiązaniami podjętymi na mocy obowiązującej w UE Konwencji ONZ o prawach osób niepełnosprawnych osoby niepełnosprawne powinny mieć możliwość korzystania z usług zaufania i produktów przeznaczonych dla użytkownika końcowego stosowanych w ramach świadczenia tych usług na takich samych zasadach, co inni konsumenci.

(24) Dostawca usług zaufania jest administratorem danych osobowych, a zatem musi spełniać wymagania określone w dyrektywie 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[22]. W szczególności gromadzenie danych należy ograniczyć do minimum, uwzględniając przy tym cel świadczonej usługi.

(25) Organy nadzorcze powinny współpracować z organami ochrony danych i wymieniać się z nimi informacjami, aby zagwarantować, że dostawcy usług należycie przestrzegają przepisów dotyczących ochrony danych. Wymiana informacji powinna obejmować zwłaszcza incydenty związane z bezpieczeństwem oraz przypadki naruszenia bezpieczeństwa danych osobowych.

(26) 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.

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

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

---

[22] Dz.U.L 281 z 23.11.1995, s. 31.

(29) 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.

(30) Aby Komisja i państwa członkowskie mogły ocenić skuteczność mechanizmu zgłaszania naruszeń wprowadzonego niniejszym rozporządzeniem, organy nadzorcze są zobowiązane dostarczyć Komisji i Europejskiej Agencji ds. Bezpieczeństwa Sieci i Informacji (ENISA) zbiorcze informacje.

(31) Aby Komisja i państwa członkowskie mogły ocenić skutki niniejszego rozporządzenia, organy nadzorcze powinny być zobowiązane do dostarczania danych statystycznych dotyczących korzystania z kwalifikowanych usług zaufania.

(32) Aby Komisja i państwa członkowskie mogły ocenić skuteczność usprawnionego mechanizmu nadzoru wprowadzonego niniejszym rozporządzeniem, organy nadzorcze powinny być zobowiązane do składania sprawozdań ze swojej działalności. Sprawozdania te w znaczący sposób ułatwią wymianę dobrych praktyk między organami nadzorczymi i umożliwią sprawdzenie, czy podstawowe wymogi dotyczące nadzoru są jednolicie i skutecznie wdrażane we wszystkich państwach członkowskich.

(33) Aby zapewnić stabilność i trwałość kwalifikowanych usług zaufania oraz zwiększać zaufanie użytkowników do ciągłości kwalifikowanych usług zaufania, organy nadzorcze powinny zagwarantować przechowywanie i dostępność danych dostawców kwalifikowanych usług zaufania przez odpowiedni okres, nawet wtedy, gdy dostawca usług kwalifikowanych zaufania przestanie istnieć.

(34) Aby ułatwić nadzór nad dostawcami kwalifikowanych usług zaufania, np. 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 nadzorczymi w państwach członkowskich.

(35) Dostawcy usług zaufania są odpowiedzialni za spełnianie wymogów określonych w niniejszym rozporządzeniu i dotyczących świadczenia usług zaufania, zwłaszcza kwalifikowanych usług zaufania. Organy nadzorcze są odpowiedzialne za nadzorowanie tego, w jaki sposób dostawcy usług zaufania spełniają te wymagania.

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

(37) Zaufane listy są istotnym elementem procesu budowania zaufania wśród podmiotów rynkowych, ponieważ wskazują kwalifikowany status dostawcy usługi podczas nadzoru; z drugiej strony nie są one niezbędne w celu osiągnięcia kwalifikowanego statusu i świadczenia kwalifikowanych usług zaufania, które wynikają ze spełnienia wymogów niniejszego rozporządzenia.

(38) Po tym, jak kwalifikowana usługa zaufania zostanie zgłoszona, nie może zostać odrzucona przez stosowny organ sektora publicznego podczas realizacji procedury lub formalności administracyjnej ze względu na fakt, iż nie jest uwzględniona w zaufanych listach sporządzonych przez państwa członkowskie. Do celów niniejszego aktu organ sektora publicznego oznacza każdy organ publiczny lub inny podmiot, któremu powierzono świadczenie usług administracji elektronicznej, takich jak np. deklaracje podatkowe online, wnioski o wydanie odpisu aktu urodzenia, udział w elektronicznych przetargach publicznych itd.

(39) Mimo iż w celu zapewnienia wzajemnego uznawania podpisów elektronicznych konieczny jest wysoki poziom bezpieczeństwa, w niektórych przypadkach, np. w kontekście decyzji Komisji 2009/767/WE z dnia 16 października 2009 r. ustanawiającej 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[23], powinno się również akceptować podpisy elektroniczne o niższym zabezpieczeniu.

(40) Podpisującemu należy umożliwić powierzanie urządzeń do składania kwalifikowanego podpisu elektronicznego stronie trzeciej, pod warunkiem wdrożenia odpowiednich mechanizmów i procedur gwarantujących, że podpisujący posiada wyłączną kontrolę nad używaniem swoich danych służących do składania podpisu elektronicznego, i że użycie urządzenia spełnia wymagania dotyczące kwalifikowanego podpisu.

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

(42) Kiedy transakcja wymaga od osoby prawnej użycia kwalifikowanej pieczęci elektronicznej, akceptowalny powinien być również kwalifikowany podpis elektroniczny uprawnionego przedstawiciela osoby prawnej.

(43) Pieczęcie elektroniczne powinny służyć jako dowód wydania dokumentu elektronicznego przez osobę prawną, gwarantując pochodzenie i integralność dokumentu.

(44) Niniejsze rozporządzenie powinno zapewnić długoterminowe przechowywanie informacji, tj. prawną ważność podpisu elektronicznego i pieczęci elektronicznych przez wydłużone okresy, dając gwarancję możliwości ich weryfikacji bez względu na przyszłe zmiany technologiczne.

(45) Aby usprawnić transgraniczne korzystanie z dokumentów elektronicznych, w niniejszym rozporządzeniu należy określić skutki prawne dokumentów

[23] Dz.U.L 274 z 20.10.2009, s. 36.

elektronicznych, które należy uznawać za równoważne z dokumentami papierowymi, w zależności od oceny dotyczącej ryzyka i pod warunkiem, że zapewniono autentyczność i integralność dokumentów. Z punku widzenia dalszego rozwoju transgranicznych transakcji elektronicznych na rynku wewnętrznym ważne jest również, by oryginalne dokumenty elektroniczne lub uwierzytelnione odpisy wydawane przez odpowiednie właściwe organy w państwie członkowskim zgodnie z przepisami krajowymi były akceptowane jako takie również w innych państwach członkowskich. Niniejsze rozporządzenie nie powinno mieć wpływu na prawo państw członkowskich do stanowienia o tym, co stanowi oryginał lub odpis na poziomie krajowym, lecz powinno zapewnić możliwość stosowania ich jako takich również w kontekście transgranicznym.

(46) Ponieważ właściwe organy w państwach członkowskich używają obecnie różnych formatów zaawansowanych podpisów elektronicznych do elektronicznego podpisywania dokumentów, należy zadbać o to, by państwa członkowskie mogły obsługiwać pod względem technicznym co najmniej kilka formatów zaawansowanego podpisu elektronicznego przy odbiorze dokumentów podpisanych elektronicznie. Podobnie, kiedy właściwe organy w państwach członkowskich używają zaawansowanych pieczęci elektronicznych, należy zapewnić im możliwość obsługi co najmniej kilku formatów zaawansowanej pieczęci elektronicznej.

(47) Pieczęcie elektroniczne mogą być używane nie tylko do uwierzytelnienia dokumentu wydanego przez osobę prawną, lecz również do uwierzytelnienia wszelkich zasobów cyfrowych osoby prawnej, np. kodu oprogramowania lub serwerów.

(48) Umożliwienie uwierzytelniania witryn internetowych oraz ich właścicieli utrudni fałszowanie witryn internetowych, a tym samym ograniczy oszustwa.

(49) W celu uzupełnienia niektórych szczegółowych i technicznych aspektów rozporządzenia w elastyczny i szybki sposób należy przekazać Komisji uprawnienia do przyjęcia aktów zgodnie z art. 290 Traktatu o funkcjonowaniu Unii Europejskiej w odniesieniu do interoperacyjności identyfikacji elektronicznej, środków bezpieczeństwa wymaganych w przypadku dostawców usług zaufania, uznanych i niezależnych organów odpowiedzialnych za przeprowadzanie audytów dostawców usług, zaufanych list, wymogów dotyczących poziomu bezpieczeństwa podpisów elektronicznych, wymogów dotyczących kwalifikowanych certyfikatów podpisów elektronicznych oraz ich weryfikacji i przechowywania, organów odpowiedzialnych za certyfikację urządzeń do składania kwalifikowanego podpisu elektronicznego, wymogów dotyczących poziomu bezpieczeństwa pieczęci elektronicznych i kwalifikowanych certyfikatów pieczęci elektronicznych, a także w odniesieniu do interoperacyjności usług przekazu. Szczególnie ważne jest, aby w czasie prac przygotowawczych Komisja prowadziła stosowne konsultacje, w tym na poziomie ekspertów.

(50) Przygotowując i opracowując akty delegowane, Komisja powinna zapewnić jednoczesne, terminowe i odpowiednie przekazywanie stosownych dokumentów Parlamentowi Europejskiemu i Radzie.

(51) W celu zapewnienia jednolitych warunków wykonywania niniejszego rozporządzenia należy powierzyć Komisji uprawnienia wykonawcze, zwłaszcza w odniesieniu do określenia numerów referencyjnych norm, które umożliwią domniemanie spełnienia

niektórych wymogów przewidzianych w niniejszym rozporządzeniu lub określonych w aktach delegowanych. Uprawnienia te powinny być wykonywane zgodnie z rozporządzeniem Parlamentu Europejskiego i Rady (UE) nr 182/2011 z dnia 16 lutego 2011 r. ustanawiającego przepisy i zasady ogólne dotyczące trybu kontroli przez państwa członkowskie wykonywania uprawnień wykonawczych przez Komisję[24].

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

(53) Aby zapewnić pewność prawa podmiotom rynkowym stosującym już kwalifikowane certyfikaty wydane zgodnie z dyrektywą 1999/93/WE, należy przewidzieć odpowiedni okres przejściowy. Należy również zapewnić Komisji środki do przyjmowania aktów wykonawczych i delegowanych przed upływem tego terminu.

(54) Ponieważ cele niniejszego rozporządzenia nie mogą być osiągnięte w wystarczającym stopniu przez państwa członkowskie, natomiast z uwagi na skalę niezbędnych działań można je w większym stopniu osiągnąć na poziomie unijnym, Unia może 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 tego celu, w szczególności w odniesieniu do roli Komisji jako koordynatora działań krajowych,

PRZYJMUJĄ NINIEJSZE ROZPORZĄDZENIE:

ROZDZIAŁ I

PRZEPISY OGÓLNE

Artykuł 1

Przedmiot

1. Niniejsze rozporządzenie ustanawia zasady dotyczące identyfikacji elektronicznej i elektronicznych usług zaufania w odniesieniu do transakcji elektronicznych w celu zapewnienia odpowiedniego funkcjonowania rynku wewnętrznego.

2. Rozporządzenie określa warunki uznawania i akceptowania przez państwa członkowskie środków identyfikacji elektronicznej osób fizycznych i prawnych, objętych zgłoszonym systemem identyfikacji elektronicznej innego państwa członkowskiego.

3. Rozporządzenie ustanawia ramy prawne dla podpisów elektronicznych, pieczęci elektronicznych, elektronicznych znaczników czasu, dokumentów elektronicznych, usług przekazu elektronicznego i uwierzytelniania witryn internetowych.

4. Niniejsze rozporządzenie gwarantuje, że do swobodnego obrotu na rynku wewnętrznym dopuszczane są usługi i produkty zaufania spełniające wymogi niniejszego rozporządzenia.

Artykuł 2

Zakres

[24] Dz.U.L 55 z 28.2.2011, s. 13.

1. Niniejsze rozporządzenie stosuje się w odniesieniu do usług identyfikacji elektronicznej świadczonych przez państwa członkowskie, w ich imieniu lub na ich odpowiedzialność oraz w odniesieniu do dostawców usług zaufania posiadających siedzibę w Unii.

2. Niniejsze rozporządzenie nie stosuje się do świadczenia elektronicznych usług zaufania opierających się na dobrowolnych porozumieniach zawartych na mocy prawa prywatnego.

3. Niniejsze rozporządzenie nie obejmuje aspektów związanych z zawieraniem i ważnością umów lub innych zobowiązań prawnych, w przypadku których istnieją wymagania dotyczące formy wprowadzone na mocy prawa krajowego lub unijnego.

Artykuł 3

Definicje

Do celów niniejszego rozporządzenia stosuje się następujące definicje:

1) „identyfikacja elektroniczna” oznacza proces używania danych identyfikujących osobę w formie elektronicznej, w sposób jednoznaczny reprezentujący osobę fizyczną lub prawną;

2) „środek identyfikacji elektronicznej” oznacza materialną lub niematerialną jednostkę zawierającą dane, o których mowa w pkt 1) niniejszego artykułu, używaną w celu uzyskania dostępu do usług online, o których mowa w art. 5;

3) „system identyfikacji elektronicznej” oznacza system identyfikacji elektronicznej, w ramach którego wydaje się środki identyfikacji elektronicznej osobom, o których mowa w pkt 1) niniejszego artykułu;

4) „uwierzytelnianie” oznacza proces elektroniczny, który umożliwia weryfikację identyfikacji elektronicznej osoby fizycznej lub prawnej lub pochodzenia i integralności danych elektronicznych;

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

6) „podpis elektroniczny” oznacza dane w formie elektronicznej dodane do innych danych elektronicznych lub logicznie z nimi powiązane i służące podpisującemu do składania podpisu;

7) „zaawansowany podpis elektroniczny” oznacza podpis elektroniczny, który spełnia następujące wymagania:

a) jest przyporządkowany wyłącznie podpisującemu;

b) umożliwia ustalenie tożsamości podpisującego;

c) jest składany przy użyciu danych służących do składania podpisu elektronicznego, które podpisujący może wykorzystać z dużą dozą zaufania i nad którymi ma wyłączną kontrolę; oraz

d) jest w taki sposób powiązany z danymi, do których się odnosi, że każda późniejsza zmiana danych jest wykrywalna;

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

9) „dane służące do składania podpisu elektronicznego” oznaczają niepowtarzalne dane, które podpisujący wykorzystuje do złożenia podpisu elektronicznego;

10) „certyfikat” oznacza poświadczenie elektroniczne, które łączy – odpowiednio – podpis elektroniczny lub dane z weryfikacji pieczęci osoby fizycznej lub osoby prawnej z certyfikatem i które potwierdza te dane jako dane tej osoby;

11) „kwalifikowany certyfikat podpisu elektronicznego” oznacza poświadczenie stosowane do potwierdzania podpisów elektronicznych, które jest wydawane przez dostawcę kwalifikowanych usług zaufania i które spełnia wymagania określone w załączniku I;

12) „usługa zaufania” oznacza każdą elektroniczną usługę polegającą na tworzeniu, kontroli, weryfikacji i przechowywaniu podpisów elektronicznych, pieczęci elektronicznych, elektronicznych znaczników czasu, dokumentów elektronicznych, usług przekazu elektronicznego, usług uwierzytelniania witryn internetowych i certyfikatów elektronicznych, w tym certyfikatów podpisów elektronicznych i pieczęci elektronicznych;

13) „kwalifikowana usługa zaufania” oznacza usługę zaufania, która spełnia stosowne wymagania ustanowione w niniejszym rozporządzeniu;

14) „dostawca usług zaufania” oznacza osobę fizyczną lub prawną, która świadczy jedną usługę zaufania lub więcej takich usług;

15) „dostawca kwalifikowanych usług zaufania” oznacza dostawcę usług zaufania, który spełnia wymagania ustanowione w niniejszym rozporządzeniu;

16) „produkt” oznacza sprzęt komputerowy lub oprogramowanie, lub ich odpowiednie komponenty, które są przeznaczone do wykorzystania w ramach świadczenia usług zaufania;

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

18) „urządzenie do składania kwalifikowanego podpisu elektronicznego” oznacza urządzenie do składania podpisu elektronicznego, które spełnia wymagania określone w załączniku II;

19) „podmiot wystawiający pieczęć” oznacza osobę prawną, która wystawia pieczęć elektroniczną;

20) „pieczęć elektroniczna” oznacza dane w formie elektronicznej dodane do innych danych elektronicznych lub logicznie z nimi powiązane, aby zagwarantować pochodzenie i integralność powiązanych danych;

21) „zaawansowana pieczęć elektroniczna” oznacza pieczęć elektroniczną, która spełnia następujące wymagania:

a) jest przyporządkowania wyłącznie podmiotowi wystawiającemu pieczęć;

b) umożliwia ustalenie tożsamości podmiotu wystawiającego pieczęć;

c) jest tworzona przy użyciu danych służących do wystawiania pieczęci elektronicznej, które podmiot wystawiający pieczęć posiadający duży poziom zaufania może wykorzystać do wystawienia pieczęci elektronicznej; oraz

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

22) „kwalifikowana pieczęć elektroniczna” oznacza zaawansowaną pieczęć elektroniczną, która została wystawiona za pomocą urządzenia do wystawiania kwalifikowanych pieczęci elektronicznych i która opiera się na kwalifikowanym certyfikacie pieczęci elektronicznej;

23) „dane służące do wystawiania pieczęci elektronicznej” oznaczają niepowtarzalne dane, które podmiot wystawiający pieczęć wykorzystuje do wystawienia pieczęci elektronicznej;

24) „kwalifikowany certyfikat pieczęci elektronicznej” oznacza poświadczenie stosowane do potwierdzenia pieczęci elektronicznej, które jest wydawane przez dostawcę kwalifikowanych usług zaufania i które spełnia wymagania określone w załączniku III;

25) „elektroniczny znacznik czasu” oznacza dane w formie elektronicznej, które wiążą inne dane elektroniczne z określonym czasem, stanowiąc dowód na to, że te dane istniały w tym czasie;

26) „kwalifikowany elektroniczny znacznik czasu” oznacza elektroniczny znacznik czasu, który spełnia wymagania określone w art. 33;

27) „dokument elektroniczny” oznacza dokument w dowolnym formacie elektronicznym;

28) „usługa przekazu elektronicznego” oznacza usługę umożliwiającą przesłanie danych drogą elektroniczną i zapewniającą dowody związane z posługiwaniem się przesyłanymi danymi, w tym dowód wysłania lub odbioru danych, oraz chroniącą przesyłane dane przed ryzykiem utraty, kradzieży, uszkodzenia lub wszelkiego nieupoważnionego naruszenia;

29) „kwalifikowana usługa przekazu elektronicznego” oznacza usługę przekazu elektronicznego, która spełnia wymagania określone w art. 36;

30) „kwalifikowany certyfikat uwierzytelniania witryn internetowych” oznacza poświadczenie, które jest stosowane do uwierzytelniania witryn internetowych i przyporządkowuje witrynę internetową osobie, której wydano certyfikat wystawiony przez dostawcę kwalifikowanych usług zaufania i spełniający wymagania określone w załączniku IV;

31) „dane służące do weryfikacji” oznaczają dane używane do weryfikacji podpisu elektronicznego lub pieczęci elektronicznej.

Artykuł 4

Zasada rynku wewnętrznego

1. Nie ogranicza się świadczenia usług zaufania na terytorium państwa członkowskiego przez dostawcę usług zaufania posiadającego siedzibę w innym państwie członkowskim z powodów objętych zakresem niniejszego rozporządzenia.

2. Produkty spełniające wymagania niniejszego rozporządzenia dopuszcza się do swobodnego obrotu na rynku wewnętrznym.

ROZDZIAŁ II

IDENTYFIKACJA ELEKTRONICZNA

Artykuł 5

Wzajemne uznawanie i akceptowanie

Jeżeli zgodnie z prawem krajowym lub praktyką administracyjną dostęp do usługi online wymaga identyfikacji elektronicznej przy użyciu środka identyfikacji elektronicznej oraz uwierzytelnienia, na potrzeby dostępu do tej usługi uznaje się i akceptuje wszystkie środki identyfikacji elektronicznej wydane w innym państwie członkowskim i objęte systemem uwzględnionym na liście publikowanej przez Komisję zgodnie z procedurą, o której mowa w art. 7.

Artykuł 6

Warunki zgłaszania systemów identyfikacji elektronicznej

1. Systemy identyfikacji elektronicznej kwalifikują się do zgłoszenia zgodnie z art. 7, jeżeli spełnione są następujące warunki:

a) środki identyfikacji elektronicznej zostały wydane przez zgłaszające państwo członkowskie, w jego imieniu lub na jego odpowiedzialność;

b) środki identyfikacji elektronicznej mogą być używane w celu zapewnienia dostępu przynajmniej do usług publicznych wymagających identyfikacji elektronicznej w zgłaszającym państwie członkowskim;

c) zgłaszające państwo członkowskie gwarantuje, że dane osobowe związane z identyfikacją są jednoznacznie przypisywane do osoby fizycznej lub prawnej, o której mowa w art. 3 pkt 1);

d) zgłaszające państwo członkowskie gwarantuje dostępność mechanizmów uwierzytelniania online w dowolnym czasie i nieodpłatnie, tak aby wszystkie strony ufające mogły dokonać weryfikacji danych identyfikujących osobę otrzymanych w formie elektronicznej. Państwa członkowskie nie nakładają żadnych specjalnych wymagań technicznych na strony ufające posiadające siedzibę poza ich terytorium, które zamierzają dokonać takiego uwierzytelnienia. Jeżeli nastąpi naruszenie lub częściowe uszkodzenie zgłoszonego systemu identyfikacji lub mechanizmu uwierzytelniania, państwo członkowskie bezzwłocznie zawiesza lub wycofuje zgłoszony system identyfikacji lub mechanizm uwierzytelniania, lub jego uszkodzone części, i powiadamia o tym pozostałe państwa członkowskie i Komisję zgodnie z art. 7;

e) zgłaszające państwo członkowskie bierze odpowiedzialność za:

– (i) jednoznaczne przypisanie danych identyfikujących osobę, o których mowa w lit. c), oraz za

– (ii) mechanizm uwierzytelniania wymieniony w lit. d).

2. Przepisy ust. 1 lit. e) pozostają bez uszczerbku dla odpowiedzialności stron transakcji, na potrzeby której zastosowano środki identyfikacji elektronicznej objęte zgłoszonym systemem.

Artykuł 7

Zgłoszenie

1. Państwa członkowskie, które zgłaszają systemy identyfikacji elektronicznej, bezzwłocznie przekazują Komisji następujące informacje i ewentualne późniejsze zmiany:

a) opis zgłaszanego systemu identyfikacji elektronicznej;

b) organy odpowiedzialne za zgłaszany system identyfikacji elektronicznej;

c) informację o tym, kto zarządza rejestracją jednoznacznych identyfikatorów osób;

d) opis mechanizmu uwierzytelniającego;

e) ustalenia dotyczące zawieszania lub wycofywania zgłoszonego systemu identyfikacji lub mechanizmu uwierzytelniającego, lub ich uszkodzonych części.

2. Sześć miesięcy po wejściu w życie niniejszego rozporządzenia Komisja publikuje w *Dzienniku Urzędowym Unii Europejskiej* listę systemów identyfikacji elektronicznej, które zostały zgłoszone zgodnie z ust. 1, oraz podstawowe informacje na ich temat.

3. W przypadku gdy Komisja otrzymuje zgłoszenie po upływie okresu, o którym mowa w ust. 2, wprowadza ona zmiany na liście w ciągu trzech miesięcy.

4. Komisja może – w drodze aktów wykonawczych – określać okoliczności, formaty i procedury dotyczące zgłoszenia, o którym mowa w ust. 1 i 3. Te akty wykonawcze przyjmowane są zgodnie z procedurą sprawdzającą, o której mowa w art. 39 ust. 2.

Artykuł 8

Koordynacja

1. Państwa członkowskie współpracują w celu zapewnienia interoperacyjności i zwiększenia bezpieczeństwa środków identyfikacji elektronicznej objętych zgłoszonym systemem.

2. Komisja ustanawia w drodze aktów wykonawczych niezbędne zasady ułatwiania współpracy między państwami członkowskimi, o której mowa w ust. 1, w celu zapewnienia wysokiego poziomu zaufania i bezpieczeństwa, stosownie do poziomu ryzyka. Akty wykonawcze dotyczą zwłaszcza wymiany informacji, doświadczeń i dobrych praktyk dotyczących systemów identyfikacji elektronicznej, wzajemnej oceny zgłoszonych systemów identyfikacji elektronicznej oraz analizy stosownych zmian zachodzących w sektorze identyfikacji elektronicznej dokonywanej przez właściwe organy państw członkowskich. Te akty wykonawcze są przyjmowane zgodnie z procedurą sprawdzającą, o której mowa w art. 39 ust. 2.

3. Komisja jest uprawniona do przyjęcia aktów delegowanych, zgodnie z art. 38, dotyczących ułatwiania transgranicznej interoperacyjności środków identyfikacji elektronicznej poprzez określanie minimalnych wymagań technicznych.

ROZDZIAŁ III

USŁUGI ZAUFANIA

Sekcja 1

Przepisy ogólne

Artykuł 9

Odpowiedzialność

1. Dostawca usług zaufania odpowiada za wszystkie bezpośrednie szkody poniesione przez osobę fizyczną lub prawną w wyniku niedopełnienia zobowiązań określonych w art. 15 ust. 1, chyba że dostawca usług zaufania może udowodnić, iż działał z zachowaniem należytej staranności.

2. Dostawca kwalifikowanych usług zaufania odpowiada za wszystkie bezpośrednie szkody poniesione przez osobę fizyczną lub prawną w wyniku niedopełnienia zobowiązań określonych niniejszym rozporządzeniu, zwłaszcza w art. 19, chyba że dostawca kwalifikowanych usług zaufania może udowodnić, iż działał z zachowaniem należytej staranności.

Artykuł 10

Dostawcy usług zaufania z państw trzecich

1. Kwalifikowane usługi zaufania i kwalifikowane certyfikaty dostarczone przez dostawców kwalifikowanych usług zaufania z siedzibą w państwie trzecim akceptuje się jako kwalifikowane usługi zaufania i kwalifikowane certyfikaty dostarczone przez dostawców kwalifikowanych usług zaufania z siedzibą na terytorium Unii Europejskiej, jeżeli kwalifikowane usługi zaufania lub kwalifikowane certyfikaty pochodzące z państwa trzeciego są uznawane na mocy porozumienia między Unią Europejską a państwem trzecim lub organizacjami międzynarodowymi zgodnie z art. 218 TFUE.

2. W odniesieniu do ust. 1 takie porozumienia zapewniają spełnienie przez dostawców usług zaufania w państwach trzecich lub organizacjach międzynawowych wymagań mających zastosowanie do kwalifikowanych usług zaufania i kwalifikowanych certyfikatów dostarczanych przez dostawców kwalifikowanych usług zaufania z siedzibą na terytorium Unii, zwłaszcza w odniesieniu do ochrony danych osobowych, bezpieczeństwa i nadzoru.

Artykuł 11

Przetwarzanie i ochrona danych

1. Dostawcy usług zaufania i organy nadzorcze zapewniają rzetelne i zgodne z prawem przetwarzanie danych osobowych, zgodnie z dyrektywą 95/46/WE.

2. Dostawcy usług zaufania przetwarzają dane osobowe zgodnie z dyrektywą 95/46/WE. Takie przetwarzanie danych jest ściśle ograniczone do minimalnej ilości danych potrzebnych do wydania i zachowania certyfikatu lub do świadczenia powiązanej usługi zaufania.

3. Dostawcy usług zaufania gwarantują poufność i integralność danych odnoszących się do osoby, na rzecz której świadczona jest usługa zaufania.

4. Bez uszczerbku dla skutków prawnych używania pseudonimów w prawie krajowym państwa członkowskie nie zabraniają dostawcom usług zaufania podawania pseudonimu w certyfikatach podpisów elektronicznych w miejsce nazwiska podpisującego.

Artykuł 12

Dostępność dla osób niepełnosprawnych

Świadczone usługi zaufania i produkty przeznaczone dla użytkownika końcowego są dostępne dla osób niepełnosprawnych w każdym przypadku, kiedy jest to możliwe.

Sekcja 2

Nadzór

Artykuł 13

Organ nadzorczy

1. Państwa członkowskie wyznaczają właściwy organ z siedzibą na swoim terytorium lub, za obopólną zgodą, z siedzibą w innym państwie członkowskim na odpowiedzialność wyznaczającego państwa członkowskiego. Organom nadzorczym przyznaje się wszelkie uprawnienia nadzorcze i dochodzeniowe, które są niezbędne do wykonywania powierzonych im zadań.

2. Organ nadzorczy odpowiada za wypełnianie następujących zadań:

a) monitorowanie dostawców usług zaufania mających siedzibę na terytorium wyznaczającego państwa członkowskiego, aby zapewnić spełnienie przez nich wszystkich wymagań ustanowionych w art. 15;

b) sprawowanie nadzoru nad dostawcami kwalifikowanych usług zaufania mającymi siedzibę na terytorium wyznaczającego państwa członkowskiego i nad świadczonymi przez nich kwalifikowanymi usługami zaufania, aby zagwarantować, że dostawcy ci i świadczone przez nich kwalifikowane usługi zaufania spełniają stosowane wymagania ustanowione w niniejszym rozporządzeniu;

c) zapewnienie zachowywania i dostępności przez odpowiedni okres odpowiednich informacji i danych, o których mowa w art. 19 ust. 2 lit. g), zapisywanych przez dostawców kwalifikowanych usług zaufania po zakończeniu działań podjętych przez dostawcę kwalifikowanych usług zaufania, w celu zagwarantowania ciągłości usługi.

3. Do końca pierwszego kwartału następnego roku kalendarzowego każdy organ nadzorczy składa Komisji i państwom członkowskim coroczne sprawozdanie z działalności nadzorczej w poprzednim roku kalendarzowym. Sprawozdanie zawiera co najmniej:

a) informacje o działalności nadzorczej;

b) zestawienie zgłoszeń dotyczących naruszeń otrzymanych od dostawców usług zaufania zgodnie z art. 15 ust. 2;

c) dane statystyczne dotyczące sprzedaży i korzystania z kwalifikowanych usług zaufania, w tym informacje na temat samych dostawców kwalifikowanych usług zaufania, świadczonych przez nich kwalifikowanych usług zaufania oraz wykorzystywanych przez nich produktów, a także ogólny opis ich klientów.

4. Państwa członkowskie zgłaszają Komisji i pozostałym państwom członkowskim nazwy i adresy swoich wyznaczonych organów nadzorczych.

5. Komisja jest uprawniona do przyjęcia aktów delegowanych, zgodnie z art. 38, dotyczących określania procedur mających zastosowanie do zadań, o których mowa w ust. 2.

6. Komisja może – w drodze aktów wykonawczych – określać okoliczności, formaty i procedury dotyczące sprawozdania, o którym mowa w ust. 3. Te akty wykonawcze są przyjmowane zgodnie z procedurą sprawdzającą, o której mowa w art. 39 ust. 2.

Artykuł 14

Wzajemna pomoc

1. Organy nadzorcze prowadzą współpracę, w ramach której wymieniają się dobrymi praktykami i w możliwie najkrótszym czasie przekazują sobie odpowiednie informacje i udzielają sobie wzajemnej pomocy, tak aby ich działalność mogła być prowadzona w spójny sposób. Wzajemna pomoc obejmuje zwłaszcza wnioski o informacje i środki nadzorcze, takie jak wnioski o przeprowadzenie inspekcji związanych z audytami bezpieczeństwa, o których mowa w art. 15, 16 i 17.

2. Organ nadzorczy, do którego kierowany jest wniosek o pomoc, nie może odmówić zastosowania się do niego, chyba że:

a) nie jest kompetentny do rozpatrzenia tego wniosku; lub

b) zastosowanie się do wniosku byłoby niezgodne z niniejszym rozporządzeniem.

3. W stosownych przypadkach organy nadzorcze mogą prowadzić wspólne dochodzenia, w których biorą udział pracownicy z organów nadzorczych innych państw członkowskich.

Organ nadzorczy państwa członkowskiego, w którym prowadzone ma być dochodzenie, może przekazać zadania związane z dochodzeniem pracownikom wspomaganego organu nadzorczego, zgodnie z własnymi przepisami krajowymi. Z takich uprawnień można korzystać wyłącznie pod nadzorem i w obecności pracowników z przyjmującego organu nadzorczego. Pracownicy wspomaganego organu nadzorczego podlegają prawu krajowemu przyjmującego organu nadzorczego. Przyjmujący organ nadzorczy ponosi odpowiedzialność za działania podejmowane przez pracowników wspomaganego organu nadzorczego.

4. Komisja może – w drodze aktów wykonawczych – określać formaty i procedury dotyczące wzajemnej pomocy przewidzianej w niniejszym artykule. Te akty wykonawcze są przyjmowane zgodnie z procedurą sprawdzającą, o której mowa w art. 39 ust. 2.

Artykuł 15

Wymagania w zakresie bezpieczeństwa mające zastosowanie do dostawców usług zaufania

1. Dostawcy usług zaufania z siedzibą na terytorium Unii przyjmują odpowiednie środki techniczne i organizacyjne w celu zarządzania ryzykiem, na jakie narażone jest bezpieczeństwo świadczonych przez nich usług zaufania. Zgodnie ze stanem wiedzy naukowej i technicznej środki te zapewniają poziom bezpieczeństwa dostosowany do stopnia ryzyka. W szczególności należy podjąć środki zapobiegające incydentom związanym z bezpieczeństwem lub minimalizujące ich wpływ oraz należy informować zainteresowane strony o negatywnych skutkach takich incydentów.

Bez uszczerbku dla art. 16 ust. 1 każdy dostawca usług zaufania może przedłożyć organowi nadzorczemu sprawozdanie z audytu bezpieczeństwa przeprowadzonego przez uznany i niezależny organ, aby potwierdzić wdrożenie odpowiednich środków bezpieczeństwa.

2. Dostawcy usług zaufania zgłaszają wszelkie przypadki naruszenia bezpieczeństwa lub utraty integralności – które mają znaczący wpływ na świadczoną usługę zaufania i zawarte w niej dane osobowe – właściwemu organowi nadzorczemu, właściwemu organowi krajowemu ds. bezpieczeństwa informacji i innym odpowiednim stronom trzecim, takim jak organy ds. ochrony danych, bez nieuzasadnionej zwłoki i – jeśli jest to możliwe – nie później niż w ciągu 24 godzin od momentu otrzymania informacji o tym naruszeniu lub o tej utracie integralności.

W stosownych przypadkach, zwłaszcza gdy naruszenie bezpieczeństwa lub utrata integralności dotyczy dwóch lub większej liczby państw członkowskich, zainteresowany organ nadzorczy powiadamia organy nadzorcze w pozostałych państwach członkowskich oraz Europejską Agencję ds. Bezpieczeństwa Sieci i Informacji (ENISA).

Zainteresowany organ nadzorczy może również podać zaistniałe fakty do wiadomości publicznej lub nałożyć taki obowiązek na dostawcę usług zaufania, jeżeli uzna, że ujawnienie naruszenia leży w interesie publicznym.

3. Co roku organ nadzorczy przekazuje ENISA i Komisji zestawienie zgłoszeń dotyczących naruszeń otrzymanych od dostawców usług zaufania.

4. W celu wdrożenia postanowień ust. 1 i 2 właściwy organ nadzorczy jest uprawniony do wydawania wiążących instrukcji dostawcom usług zaufania.

5. Komisja jest uprawniona do przyjęcia aktów delegowanych, zgodnie z art. 38, dotyczących dalszego doprecyzowania środków, o których mowa w ust. 1.

6. Komisja może – w drodze aktów wykonawczych – określać okoliczności, formaty i procedury, w tym również terminy, mające zastosowanie do celów, o których mowa w ust. 1–3. Te akty wykonawcze są przyjmowane zgodnie z procedurą sprawdzającą, o której mowa w art. 39 ust. 2.

Artykuł 16

Nadzór nad dostawcami kwalifikowanych usług zaufania

1. Raz do roku dostawcy kwalifikowanych usług zaufania podlegają audytowi przeprowadzanemu przez uznany i niezależny organ, aby potwierdzić, że dostawcy ci oraz świadczone przez nich kwalifikowane usługi zaufania spełniają wymagania określone w niniejszym rozporządzeniu, oraz przedkładają powiązane sprawozdanie z audytu bezpieczeństwa organowi nadzorczemu.

2. Bez uszczerbku dla przepisów ust. 1 organ nadzorczy, z własnej inicjatywy albo w odpowiedzi na wniosek Komisji, może w dowolnym momencie przeprowadzić audyt dostawców kwalifikowanych usług zaufania, aby potwierdzić, że dostawcy ci oraz świadczone prze nich usługi zaufania wciąż spełniają warunki określone w niniejszym rozporządzeniu. W przypadkach gdy zachodzi podejrzenie, iż naruszono przepisy dotyczące ochrony danych osobowych, organ nadzorczy informuje organy ds. ochrony danych o wynikach audytów.

3. Organ nadzorczy jest uprawniony do wydawania wiążących instrukcji dostawcom kwalifikowanych usług zaufania, aby wyeliminować wszelkie przypadki niedopełniania wymagań wskazane w sprawozdaniu z audytu bezpieczeństwa.

4. W odniesieniu do ust. 3, jeżeli dostawca kwalifikowanych usług zaufania nie wyeliminuje takiego uchybienia w czasie wyznaczonym przez organ nadzorczy, traci status kwalifikowanego dostawcy usług i zostaje poinformowany przez organ nadzorczy, że jego status zostanie odpowiednio zmieniony w zaufanych listach, o których mowa w art. 18.

5. Komisja jest uprawniona do przyjęcia aktów delegowanych, zgodnie z art. 38, dotyczących określania warunków uznawania niezależnych organów przeprowadzających audyty, o których mowa w ust. 1 niniejszego artykułu oraz w art. 15 ust. 1 i w art. 17 ust. 1.

6. Komisja może – w drodze aktów wykonawczych – określać okoliczności, procedury i formaty mające zastosowanie do celów, o których mowa w ust. 1, 2 i 4. Te akty wykonawcze są przyjmowane zgodnie z procedurą sprawdzającą, o której mowa w art. 39 ust. 2.

Artykuł 17

Inicjowanie kwalifikowanej usługi zaufania

1. Dostawcy kwalifikowanych usług zaufania zgłaszają organowi nadzorczemu zamiar świadczenia kwalifikowanej usługi zaufania oraz przedkładają organowi nadzorczemu sprawozdanie z audytu bezpieczeństwa przeprowadzonego przez uznany i niezależny organ, zgodnie z art. 16 ust. 1. Dostawcy kwalifikowanych usług zaufania mogą rozpocząć świadczenie kwalifikowanej usługi zaufania po przedłożeniu organowi nadzorczemu zgłoszenia i sprawozdania z audytu bezpieczeństwa.

2. Po przedłożeniu organowi nadzorczemu stosownych dokumentów zgodnie z ust. 1 dostawcy kwalifikowanych usług zaufania są umieszczani na zaufanych listach, o których mowa w art. 18, co oznacza, że zgłoszenie zostało przedłożone.

3. Organ nadzorczy sprawdza, czy dostawca kwalifikowanych usług zaufania i świadczone przez niego usługi zaufania spełniają wymagania niniejszego rozporządzenia.

Po pozytywnym zakończeniu weryfikacji, jednak nie później niż jeden miesiąc od daty dokonania zgłoszenia zgodnie z ust. 1, organ nadzorczy wskazuje w zaufanych listach kwalifikowany status dostawców kwalifikowanych usług i świadczonych przez nich kwalifikowanych usług zaufania.

Jeżeli weryfikacja nie jest zakończona w ciągu jednego miesiąca, organ nadzorczy informuje dostawcę kwalifikowanych usług zaufania o przyczynach opóźnienia oraz podaje termin, w jakim weryfikacja zostanie zakończona.

4. Kwalifikowana usługa zaufania będąca przedmiotem zgłoszenia, o którym mowa w ust. 1, nie może zostać odrzucona przez stosowny organ sektora publicznego podczas realizacji procedury lub formalności administracyjnej ze względu na fakt, iż nie jest uwzględniona w zaufanych listach, o których mowa w ust. 3.

5. Komisja może – w drodze aktów wykonawczych – określać okoliczności, formaty i procedury mające zastosowanie do celów, o których mowa w ust. 1, 2 i 3. Te akty wykonawcze są przyjmowane zgodnie z procedurą sprawdzającą, o której mowa w art. 39 ust. 2.

Artykuł 18

Zaufane listy

1. Każde państwo członkowskie sporządza, prowadzi i publikuje zaufane listy zawierające informacje dotyczące dostawców kwalifikowanych usług zaufania, w odniesieniu do których posiada kompetencje, wraz z informacjami dotyczącymi świadczonych przez nich kwalifikowanych usług zaufania.

2. Każde państwo członkowskie sporządza, prowadzi i publikuje w bezpieczny sposób elektronicznie podpisane lub zaopatrzone w pieczęć elektroniczną zaufane listy przewidziane w ust. 1, w formie dostosowanej do automatycznego przetwarzania.

3. Bez zbędnej zwłoki państwa członkowskie przekazują Komisji informacje o organie odpowiedzialnym za sporządzenie, prowadzenie i publikowanie krajowych list zaufania wraz ze szczegółowymi informacjami dotyczącymi miejsca publikacji tych list, certyfikatu użytego 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 formie dostosowanej do automatycznego przetwarzania, używając w tym celu zabezpieczonego kanału.

5. Komisja jest uprawniona do przyjęcia aktów delegowanych, zgodnie z art. 38, dotyczących określenia informacji, o których mowa w ust. 1.

6. Komisja może – w drodze aktów wykonawczych – określać specyfikacje techniczne i formaty dotyczące zaufanych list, mające zastosowanie do celów ust. 1–4. Te akty

wykonawcze są przyjmowane zgodnie z procedurą sprawdzającą, o której mowa w art. 39 ust. 2.

Artykuł 19

Wymagania dotyczące dostawców kwalifikowanych usług zaufania

1. Wydając kwalifikowany certyfikat, dostawca kwalifikowanych usług zaufania sprawdza, 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.

Tego rodzaju informacje sprawdza dostawca kwalifikowanych usług zaufania lub upoważniona strona trzecia działająca na odpowiedzialność dostawcy kwalifikowanych usług:

a) w drodze fizycznego stawienia się osoby fizycznej lub upoważnionego przedstawiciela osoby prawnej, lub

b) zdalnie, przy użyciu środka identyfikacji elektronicznej objętego zgłoszonym systemem, wydanego zgodnie z lit. a).

2. Dostawcy kwalifikowanych usług zaufania świadczący kwalifikowane usługi zaufania:

a) zatrudniają pracowników, którzy posiadają niezbędną wiedzę fachową, doświadczenie i kwalifikacje i którzy stosują procedury administracyjne i zarządcze odpowiadające europejskim lub międzynarodowym standardom oraz którzy przeszli odpowiednie szkolenia dotyczące bezpieczeństwa i ochrony danych osobowych;

b) są przygotowani na ryzyko związane z odpowiedzialnością za szkody poprzez utrzymywanie dostatecznej ilości zasobów finansowych lub wykupienie stosownego ubezpieczenia od odpowiedzialności;

c) przed wejściem w stosunek umowny informują wszystkie osoby pragnące skorzystać z kwalifikowanej usługi zaufania o dokładnych warunkach korzystania z tej usługi;

d) używają pewnych systemów i produktów, które są chronione przed zmianami i gwarantują techniczne bezpieczeństwo i wiarygodność procesów przez nie wspieranych;

e) używają pewnych systemów do przechowywania przekazanych im danych w sprawdzalnej formie, tak aby:

   – dane były publicznie dostępne dopiero po uzyskaniu zgody osoby, której dane zostały wydane,

   – tylko upoważnione osoby mogły wprowadzać dane i zmiany,

   – można było sprawdzać prawdziwość informacji;

f) podejmują środki zapobiegające fałszowaniu i kradzieży danych;

g) rejestrują przez odpowiedni okres wszelkie informacje dotyczące danych wydanych i otrzymanych przez dostawcę kwalifikowanych usług zaufania, w szczególności w celu przedstawienia dowodów w postępowaniach sądowych. Rejestracja może odbywać się drogą elektroniczną;

h) posiadają aktualny plan zakończenia, aby zapewnić ciągłość usług zgodnie z ustaleniami wydanymi przez organ nadzorczy na podstawie art. 13 ust. 2 lit. c);

i) zapewniają zgodne z prawem przetwarzanie danych osobowych, zgodnie z art. 11.

3. Dostawcy kwalifikowanych usług zaufania wydający kwalifikowane certyfikaty rejestrują w bazie danych certyfikatów przypadki cofnięcia certyfikatu w ciągu 10 minut od wejścia w życie decyzji o cofnięciu.

4. W odniesieniu do ust. 3 dostawcy kwalifikowanych usług zaufania wydający kwalifikowane certyfikaty dostarczają każdej stronie ufającej informacje o statusie ważności lub cofnięcia wydanych przez siebie kwalifikowanych certyfikatów. Informacje są udostępniane w dowolnym czasie co najmniej na podstawie certyfikatu w zautomatyzowany sposób który jest wiarygodny, nieodpłatny i skuteczny.

5. Komisja może ustanowić w drodze aktów wykonawczych numery referencyjne norm dotyczących wiarygodnych systemów i produktów. Jeżeli wiarygodne systemy i produkty spełniają te normy, zakłada się, że wymagania ustanowione w art. 19 są spełnione. Te akty wykonawcze są przyjmowane zgodnie z procedurą sprawdzającą, o której mowa w art. 39 ust. 2. Komisja publikuje takie akty w *Dzienniku Urzędowym Unii Europejskiej*.

Sekcja 3

Podpis elektroniczny

Artykuł 20

Skutki prawne i akceptowanie podpisów elektronicznych

1. Nie jest kwestionowany prawny skutek podpisu elektronicznego ani jego dopuszczalność jako dowód w postępowaniu sądowym wyłącznie z tego powodu, że ma formę elektroniczną.

2. Kwalifikowany podpis elektroniczny ma skutek prawny równoważny ze skutkiem prawnym podpisu własnoręcznego.

3. Kwalifikowane podpisy elektroniczne są uznawane i akceptowane we wszystkich państwach członkowskich.

4. Gdy wymagany jest – w szczególności przez państwo członkowskie na potrzeby uzyskania dostępu do usługi publicznej oferowanej przez organ publiczny online, na podstawie odpowiedniej oceny ryzyka związanego z taką usługą – podpis elektroniczny o poziomie bezpieczeństwa niższym niż kwalifikowany podpis elektroniczny, akceptowane są wszystkie podpisy elektroniczne o co najmniej takim samym poziomie bezpieczeństwa.

5. W przypadku transgranicznego dostępu do usługi oferowanej przez organ publiczny online państwa członkowskie nie wymagają podpisu elektronicznego o wyższym poziomie bezpieczeństwa niż kwalifikowany podpis elektroniczny.

6. Komisja jest uprawniona do przyjęcia aktów delegowanych, zgodnie z art. 38, dotyczących określenia różnych poziomów bezpieczeństwa podpisu elektronicznego, o których mowa w ust. 4.

7. Komisja może ustanowić w drodze aktów wykonawczych numery referencyjne norm dotyczących poziomów bezpieczeństwa podpisu elektronicznego. Jeżeli podpis spełnia te normy, zakłada się zgodność z poziomem bezpieczeństwa, określonym w akcie delegowanym przyjętym zgodnie z ust. 6. Te akty wykonawcze są przyjmowane zgodnie z procedurą sprawdzającą, o której mowa w art. 39 ust. 2. Komisja publikuje takie akty w *Dzienniku Urzędowym Unii Europejskiej*.

Artykuł 21

Kwalifikowane certyfikaty podpisów elektronicznych

1. Kwalifikowane certyfikaty podpisów elektronicznych spełniają wymagania określone w załączniku I.

2. Kwalifikowane certyfikaty podpisów elektronicznych nie podlegają obowiązkowym wymaganiom przekraczającym wymagania określone w załączniku I.

3. Jeżeli kwalifikowany certyfikat podpisu elektronicznego został cofnięty po aktywacji, traci ważność i w żadnym przypadku nie można przywrócić jego statusu poprzez odnowienie ważności.

4. Komisja jest uprawniona do przyjęcia aktów delegowanych, zgodnie z art. 38, dotyczących dalszego doprecyzowania wymagań określonych w załączniku I.

5. Komisja może ustanowić w drodze aktów wykonawczych numery referencyjne norm dotyczących kwalifikowanych certyfikatów podpisu elektronicznego. Jeżeli kwalifikowany certyfikat podpisu elektronicznego spełnia te normy, zakłada się zgodność z wymaganiami określonymi w załączniku I. Te akty wykonawcze są przyjmowane zgodnie z procedurą sprawdzającą, o której mowa w art. 39 ust. 2. Komisja publikuje takie akty w *Dzienniku Urzędowym Unii Europejskiej*.

Artykuł 22

Wymagania dotyczące urządzeń do składania kwalifikowanego podpisu elektronicznego

1. Urządzenia do składania kwalifikowanego podpisu elektronicznego spełniają wymagania określone w załączniku II.

2. Komisja może ustanowić w drodze aktów wykonawczych numery referencyjne norm dotyczących urządzeń do składania kwalifikowanego podpisu elektronicznego. Jeżeli urządzenie do składania kwalifikowanego podpisu elektronicznego spełnia te normy, zakłada się zgodność z wymaganiami określonymi w załączniku II. Te akty wykonawcze są

przyjmowane zgodnie z procedurą sprawdzającą, o której mowa w art. 39 ust. 2. Komisja publikuje takie akty w *Dzienniku Urzędowym Unii Europejskiej*.

Artykuł 23

Certyfikacja urządzeń do składania kwalifikowanego podpisu elektronicznego

1. Urządzenia do składania kwalifikowanego podpisu elektronicznego mogą być certyfikowane przez odpowiednie organy publiczne lub prywatne wyznaczone przez państwa członkowskie, pod warunkiem że zostały one poddane procedurze oceny pod względem bezpieczeństwa, przeprowadzanej zgodnie z jedną z norm dotyczących oceny bezpieczeństwa produktów informatycznych uwzględnioną na liście, która jest ustanawiana przez Komisję w drodze aktów wykonawczych. Te akty wykonawcze są przyjmowane zgodnie z procedurą sprawdzającą, o której mowa w art. 39 ust. 2. Komisja publikuje takie akty w *Dzienniku Urzędowym Unii Europejskiej*.

2. Państwa członkowskie zgłaszają Komisji i pozostałym państwom członkowskim nazwy i adresy organów publicznych lub prywatnych wyznaczonych przez nie zgodnie z ust. 1.

3. Komisja jest uprawniona do przyjęcia aktów delegowanych, zgodnie z art. 38, dotyczących ustanowienia specjalnych kryteriów, jakie muszą spełniać wyznaczone organy, o których mowa w ust. 1.

Artykuł 24

Publikacja listy certyfikowanych urządzeń do składania kwalifikowanego podpisu elektronicznego

1. Bez zbędnej zwłoki państwa członkowskie przekazują Komisji informacje o urządzeniach do składania kwalifikowanego podpisu elektronicznego, które uzyskały certyfikację organów, o których mowa w art. 23. Państwa członkowskie informują również Komisję bez zbędnej zwłoki o urządzeniach do składania podpisu elektronicznego, które nie są już certyfikowane.

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

3. Komisja może – w drodze aktów wykonawczych – określać okoliczności, formaty i procedury mające zastosowanie do celu, o którym mowa w ust. 1. Te akty wykonawcze są przyjmowane zgodnie z procedurą sprawdzającą, o której mowa w art. 39 ust. 2.

Artykuł 25

Wymagania dotyczące weryfikacji kwalifikowanych podpisów elektronicznych

1. Kwalifikowany podpis elektroniczny uznaje się za ważny, jeżeli można ustalić z dużą pewnością, że w trakcie podpisywania:

a) certyfikat, który towarzyszy podpisowi, jest certyfikatem kwalifikowanego podpisu elektronicznego spełniającym wymagania określone w załączniku I;

b) wymagany kwalifikowany certyfikat jest autentyczny i ważny;

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

d) zestaw danych jednoznacznie reprezentujących podpisującego jest prawidłowo dostarczony stronie ufającej;

e) jeżeli skorzystano z pseudonimu, zostaje to wyraźnie wskazane stronie ufającej;

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

g) integralność podpisanych danych nie została naruszona;

h) spełniono wymagania przewidziane w art. 3 pkt 7;

i) system wykorzystany do weryfikacji podpisu zapewnia stronie ufającej prawidłowy wynik procesu weryfikacji i umożliwia stronie ufającej wykrycie wszelkich kwestii związanych z bezpieczeństwem.

2. Komisja jest uprawniona do przyjęcia aktów delegowanych, zgodnie z art. 38, dotyczących dalszego doprecyzowania wymagań określonych w ust. 1.

3. Komisja może ustanowić w drodze aktów wykonawczych numery referencyjne norm dotyczących weryfikacji kwalifikowanych podpisów elektronicznych. Jeżeli weryfikacja kwalifikowanych podpisów elektronicznych spełnia te normy, zakłada się zgodność z wymaganiami określonymi w ust. 1. Te akty wykonawcze są przyjmowane zgodnie z procedurą sprawdzającą, o której mowa w art. 39 ust. 2. Komisja publikuje takie akty w *Dzienniku Urzędowym Unii Europejskiej*.

Artykuł 26

Kwalifikowana usługa weryfikacji kwalifikowanych podpisów elektronicznych

1. Kwalifikowaną usługę weryfikacji kwalifikowanych podpisów elektronicznych świadczy dostawca kwalifikowanych usług zaufania, który:

a) zapewnia weryfikację zgodnie z art. 25 ust. 1, oraz

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

2. Komisja może ustanowić w drodze aktów wykonawczych numery referencyjne norm dotyczących kwalifikowanej usługi weryfikacji, której mowa w ust. 1. Jeżeli usługa weryfikacji kwalifikowanego podpisu elektronicznego spełnia te normy, zakłada się zgodność z wymaganiami określonymi w ust. 1 lit. b). Te akty wykonawcze są przyjmowane zgodnie z procedurą sprawdzającą, o której mowa w art. 39 ust. 2. Komisja publikuje takie akty w *Dzienniku Urzędowym Unii Europejskiej*.

Artykuł 27

Przechowywanie kwalifikowanych podpisów elektronicznych

1. Usługę przechowywania kwalifikowanego podpisu elektronicznego świadczy dostawca kwalifikowanych usług zaufania, który stosuje procedury i technologie mogące przedłużyć wiarygodność danych służących do weryfikacji podpisu elektronicznego poza okres ich technologicznej ważności.

2. Komisja jest uprawniona do przyjęcia aktów delegowanych, zgodnie z art. 38, dotyczących dalszego doprecyzowania wymagań określonych w ust. 1.

3. Komisja może ustanowić w drodze aktów wykonawczych numery referencyjne norm dotyczących przechowywania kwalifikowanych podpisów elektronicznych. Jeżeli ustalenia w zakresie przechowywania kwalifikowanych podpisów elektronicznych spełniają te normy, zakłada się zgodność z wymaganiami określonymi w ust. 1. Te akty wykonawcze są przyjmowane zgodnie z procedurą sprawdzającą, o której mowa w art. 39 ust. 2. Komisja publikuje takie akty w *Dzienniku Urzędowym Unii Europejskiej*.

Sekcja 4

Pieczęcie elektroniczne

Artykuł 28

Skutki prawne pieczęci elektronicznej

1. Nie jest kwestionowany prawny skutek pieczęci elektronicznej ani jej dopuszczalność jako dowód w postępowaniu sądowym wyłącznie z tego powodu, że ma formę elektroniczną.

2. Kwalifikowana pieczęć elektroniczna umożliwia prawne domniemanie pochodzenia i integralności danych, do których jest dołączona.

3. Kwalifikowana pieczęć elektroniczna jest uznawana i akceptowana we wszystkich państwach członkowskich.

4. Gdy wymagana jest – w szczególności przez państwo członkowskie na potrzeby uzyskania dostępu do usługi publicznej oferowanej przez organ publiczny online, na podstawie odpowiedniej oceny ryzyka związanego z taką usługą – pieczęć elektroniczna o poziomie bezpieczeństwa niższym niż kwalifikowana pieczęć elektroniczna, akceptowane są wszystkie pieczęci elektroniczne o co najmniej takim samym poziomie bezpieczeństwa.

5. W przypadku transgranicznego dostępu do usługi oferowanej przez organ publiczny online państwa członkowskie nie wymagają pieczęci elektronicznej o wyższym poziomie bezpieczeństwa niż kwalifikowana pieczęć elektroniczna.

6. Komisja jest uprawniona do przyjęcia aktów delegowanych, zgodnie z art. 38, dotyczących określania różnych poziomów bezpieczeństwa pieczęci elektronicznych, o których mowa w ust. 4.

7. Komisja może ustanowić w drodze aktów wykonawczych numery referencyjne norm dotyczących poziomów bezpieczeństwa pieczęci elektronicznych. Jeżeli pieczęć spełnia te

normy, zakłada się zgodność z poziomem bezpieczeństwa, określonym w akcie delegowanym przyjętym zgodnie z ust. 6. Te akty wykonawcze są przyjmowane zgodnie z procedurą sprawdzającą, o której mowa w art. 39 ust. 2. Komisja publikuje takie akty w *Dzienniku Urzędowym Unii Europejskiej*.

Artykuł 29

Wymagania dotyczące kwalifikowanych certyfikatów pieczęci elektronicznych

1. Kwalifikowane certyfikaty pieczęci elektronicznych spełniają wymagania określone w załączniku III.

2. Kwalifikowane certyfikaty pieczęci elektronicznych nie podlegają obowiązkowym wymaganiom przekraczającym wymagania określone w załączniku III.

3. Jeżeli kwalifikowany certyfikat pieczęci elektronicznej został cofnięty po aktywacji, traci ważność i w żadnym przypadku nie można przywrócić jego statusu poprzez odnowienie ważności.

4. Komisja jest uprawniona do przyjmowania aktów delegowanych, zgodnie z art. 38, dotyczących dalszego doprecyzowania wymagań określonych w załączniku III.

5. Komisja może ustanowić w drodze aktów wykonawczych numery referencyjne norm dotyczących kwalifikowanych certyfikatów pieczęci elektronicznej. Jeżeli kwalifikowany certyfikat pieczęci elektronicznej spełnia te normy, zakłada się zgodność z wymaganiami określonymi w załączniku III. Te akty wykonawcze są przyjmowane zgodnie z procedurą sprawdzającą, o której mowa w art. 39 ust. 2. Komisja publikuje takie akty w *Dzienniku Urzędowym Unii Europejskiej*.

Artykuł 30

Urządzenia do wystawiania kwalifikowanych pieczęci elektronicznych

1. Artykuł 22 stosuje się odpowiednio do wymagań dotyczących urządzeń do wystawiania kwalifikowanych pieczęci elektronicznych.

2. Artykuł 23 stosuje się odpowiednio do certyfikacji urządzeń do wystawiania kwalifikowanych pieczęci elektronicznych.

3. Artykuł 24 stosuje się odpowiednio do publikacji listy urządzeń do wystawiania kwalifikowanych pieczęci elektronicznych.

Artykuł 31

Weryfikacja i przechowywanie kwalifikowanych pieczęci elektronicznych

Artykuły 25, 26 i 27 stosuje się odpowiednio do weryfikacji i przechowywania kwalifikowanych pieczęci elektronicznych.

Sekcja 5

Elektroniczny znacznik czasu

Artykuł 32

Skutki prawne elektronicznych znaczników czasu

1. Nie jest kwestionowany prawny skutek elektronicznego znacznika czasu ani jego dopuszczalność jako dowód w postępowaniu sądowym wyłącznie z tego powodu, że ma formę elektroniczną.

2. Kwalifikowany elektroniczny znacznik czasu umożliwia prawne domniemanie czasu, jaki wskazuje, i integralności danych, z którymi połączony jest wskazywany czas.

3. Kwalifikowany elektroniczny znacznik czasu jest uznawany i akceptowany we wszystkich państwach członkowskich.

Artykuł 33

Wymagania dotyczące kwalifikowanych elektronicznych znaczników czasu

1. Kwalifikowany elektroniczny znacznik czasu spełnia następujące wymagania:

a) jest precyzyjnie powiązany z uniwersalnym czasem koordynowanym (UTC), po to aby wykluczyć możliwość zmiany danych w niewykrywalny sposób;

b) jest oparty na precyzyjnym źródle czasu;

(c) jest wydany przez dostawcę kwalifikowanych usług zaufania;

d) jest podpisany zaawansowanym podpisem elektronicznym lub opatrzony zaawansowaną pieczęcią elektroniczną dostawcy kwalifikowanych usług zaufania, lub w inny równoważny sposób.

2. Komisja może ustanowić w drodze aktów wykonawczych numery referencyjne norm dotyczących precyzyjnego powiązania czasu z danymi oraz precyzyjnego źródła czasu. Jeżeli precyzyjne powiązanie czasu z danymi i precyzyjne źródło czasu spełniają te normy, zakłada się zgodność z wymaganiami, o których mowa w ust. 1. Te akty wykonawcze są przyjmowane zgodnie z procedurą sprawdzającą, o której mowa w art. 39 ust. 2. Komisja publikuje takie akty w *Dzienniku Urzędowym Unii Europejskiej*.

Sekcja 6

Dokumenty elektroniczne

Artykuł 34

Skutki prawne i akceptowanie dokumentów elektronicznych

1. Dokument elektroniczny uznaje się za równoważny dokumentowi papierowemu oraz dopuszczalny jako dowód w postępowaniu sądowym, z uwzględnieniem jego poziomu zabezpieczenia autentyczności i integralności.

2. Dokument zawierający kwalifikowany podpis elektroniczny lub kwalifikowaną pieczęć elektroniczną osoby, która jest uprawniona do wydawania stosownych dokumentów, umożliwia prawne domniemanie autentyczności i integralności, pod warunkiem że dokument nie zawiera dynamicznych elementów, które mogą go automatycznie zmienić.

3. W sytuacji gdy do celu świadczenia usługi publicznej online oferowanej przez organ sektora publicznego wymagany jest oryginalny dokument lub uwierzytelniony odpis, przynajmniej dokumenty elektroniczne wydane przez osoby uprawnione do wydawania stosownych dokumentów i uznawane za oryginały lub uwierzytelnione odpisy zgodnie z przepisami krajowymi państwa członkowskiego pochodzenia akceptuje się w pozostałych państwach członkowskich bez konieczności spełnienia dodatkowych wymogów.

4. Komisja może – w drodze aktów wykonawczych – określać formaty podpisów i pieczęci elektronicznych, które są zawsze akceptowane, gdy podpisany lub opatrzony pieczęcią dokument, o którym mowa w ust. 2, wymagany jest przez państwo członkowskie przy świadczeniu usługi online przez organ sektora publicznego. Te akty wykonawcze są przyjmowane zgodnie z procedurą sprawdzającą, o której mowa w art. 39 ust. 2.

Sekcja 7

Kwalifikowana usługa przekazu elektronicznego

Artykuł 35

Skutek prawny usługi przekazu elektronicznego

1. Dane wysyłane lub otrzymywane za pośrednictwem usługi przekazu elektronicznego są dopuszczalne jako dowód w postępowaniu sądowym w odniesieniu do integralności danych i pewności dnia i godziny wysłania lub otrzymania danych przez określonego adresata.

2. Dane wysyłane lub otrzymywane za pośrednictwem kwalifikowanej usługi przekazu elektronicznego umożliwiają prawne domniemanie integralności danych i dokładności dnia i godziny wysłania lub otrzymania danych wskazanych przez kwalifikowany system przekazu elektronicznego.

3. Komisja jest uprawniona do przyjęcia aktów delegowanych, zgodnie z art. 38, dotyczących określenia mechanizmów przesyłania i otrzymywania danych za pośrednictwem usług przekazu elektronicznego, które stosuje się w celu zwiększenia interoperacyjności między usługami przekazu elektronicznego.

Artykuł 36

Wymagania dotyczące kwalifikowanych usług przekazu elektronicznego

1. Kwalifikowane usługi przekazu elektronicznego spełniają następujące wymagania:

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

b) umożliwiają jednoznaczną identyfikację nadawcy i, w razie potrzeby, adresata;

c) proces wysyłania lub otrzymywania danych musi być zabezpieczony bezpiecznym podpisem elektronicznym lub bezpieczną pieczęcią elektroniczną dostawcy kwalifikowanych usług zaufania w taki sposób, by wykluczyć możliwość zmiany danych w niewykrywalny sposób;

d) każda zmiana danych niezbędna do wysłania lub otrzymania danych musi zostać wyraźnie wskazana nadawcy i adresatowi danych;

e) data wysłania, otrzymania i zmiany danych musi być wskazana za pomocą kwalifikowanego elektronicznego znacznika czasu;

f) w przypadku przesyłania danych między co najmniej dwoma dostawcami kwalifikowanych usług zaufania wymagania określone w lit. a) – e) stosują się do wszystkich dostawców kwalifikowanych usług zaufania.

2. Komisja może ustanowić w drodze aktów wykonawczych numery referencyjne norm dotyczących procesów wysyłania i otrzymywania danych. Jeżeli proces wysyłania i otrzymywania danych spełnia te normy, zakłada się zgodność z wymaganiami, o których mowa w ust. 1. Te akty wykonawcze są przyjmowane zgodnie z procedurą sprawdzającą, o której mowa w art. 39 ust. 2. Komisja publikuje takie akty w *Dzienniku Urzędowym Unii Europejskiej*.

Sekcja 8

Uwierzytelniane witryn internetowych

Artykuł 37

Wymagania dotyczące kwalifikowanych certyfikatów uwierzytelniania witryn internetowych

1. Kwalifikowane certyfikaty uwierzytelniania witryn internetowych spełniają wymagania określone w załączniku IV.

2. Kwalifikowane certyfikaty uwierzytelniania witryn internetowych uznaje się i akceptuje we wszystkich państwach członkowskich.

3. Komisja jest uprawniona do przyjęcia aktów delegowanych, zgodnie z art. 38, dotyczących dalszego doprecyzowania wymagań określonych w załączniku IV.

4. Komisja może ustanowić w drodze aktów wykonawczych numery referencyjne norm dotyczących kwalifikowanych certyfikatów uwierzytelniania witryn internetowych. Jeżeli kwalifikowany certyfikat uwierzytelnienia witryn internetowych spełnia te normy, zakłada się zgodność z wymaganiami określonymi w załączniku IV. Te akty wykonawcze są przyjmowane zgodnie z procedurą sprawdzającą, o której mowa w art. 39 ust. 2. Komisja publikuje takie akty w *Dzienniku Urzędowym Unii Europejskiej*.

ROZDZIAŁ IV

AKTY DELEGOWANE

Artykuł 38

Wykonywanie przekazanych uprawnień

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

2. Uprawnienia do przyjęcia aktów delegowanych, o których mowa w art. 8 ust. 3, art. 13 ust. 5, art. 15 ust. 5, art. 16 ust. 5, art. 18 ust. 5, art. 20 ust. 6, art. 21 ust. 4, art. 23 ust. 3, art. 25 ust. 2, art. 27 ust. 2, art. 28 ust. 6, art. 29 ust. 4, art. 30 ust. 2, art. 31, art. 35 ust. 3 oraz art. 37 ust. 3 powierza się Komisji na czas nieokreślony od dnia wejścia w życie niniejszego rozporządzenia.

3. Przekazanie uprawnień, o których mowa w art. 8 ust. 3, art. 13 ust. 5, art. 15 ust. 5, art. 16 ust. 5, art. 18 ust. 5, art. 20 ust. 6, art. 21 ust. 4, art. 23 ust. 3, art. 25 ust. 2, art. 27 ust. 2, art. 28 ust. 6, art. 29 ust. 4, art. 30 ust. 2, art. 31, art. 35 ust. 3 oraz art. 37 ust. 3 może zostać w dowolnym momencie odwołane przez Parlament Europejski lub przez Radę. Decyzja o odwołaniu kończy przekazanie określonych w niej uprawnień. Decyzja o odwołaniu staje się skuteczna od następnego dnia po jej opublikowaniu w *Dzienniku Urzędowym Unii Europejskiej* lub w określonym w tej decyzji późniejszym terminie. Nie wpływa ona na ważność jakichkolwiek 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. 8 ust. 3, art. 13 ust. 5, art. 15 ust. 5, art. 16 ust. 5, art. 18 ust. 5, art. 20 ust. 6, art. 21 ust. 4, art. 23 ust. 3, art. 25 ust. 2, art. 27 ust. 2, art. 28 ust. 6, art. 29 ust. 4, art. 30 ust. 2, art. 31, art. 35 ust. 3 oraz art. 37 ust. 3 wchodzi w życie tylko jeśli Parlament Europejski albo Rada nie wyraziły sprzeciwu w terminie dwóch miesięcy od przekazania tego aktu Parlamentowi Europejskiemu i Radzie, lub jeśli, 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.

ROZDZIAŁ V

AKTY WYKONAWCZE

Artykuł 39

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 182/2011.

ROZDZIAŁ VI

PRZEPISY KOŃCOWE

Artykuł 40

Sprawozdanie

Komisja składa Parlamentowi Europejskiemu i Radzie sprawozdanie w sprawie stosowania niniejszego rozporządzenia. Pierwsze sprawozdanie zostanie przedłożone nie później niż cztery lata po wejściu w życie niniejszego rozporządzenia. Następnie kolejne sprawozdania są przedkładane co cztery lata.

Artykuł 41

Uchylenie

1. Dyrektywa 1999/93/WE traci moc.

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

3. Bezpieczne urządzenia do składania podpisów, których zgodność określono zgodnie z art. 3 ust. 4 dyrektywy 1999/93/WE, uznaje się za kwalifikowane urządzenia do składania podpisów w rozumieniu niniejszego rozporządzenia.

4. Certyfikaty kwalifikowane wydane na mocy dyrektywy 1999/93/WE uznaje się za kwalifikowane certyfikaty podpisów elektronicznych w rozumieniu niniejszego rozporządzenia do czasu ich wygaśnięcia, ale nie dłużej niż przez pięć lat od wejścia w życie niniejszego rozporządzenia.

Artykuł 42

Wejście w życie

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

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

Sporządzono w Brukseli dnia […] r.

W imieniu Parlamentu Europejskiego	*W imieniu Rady*
Przewodniczący	*Przewodniczący*

ZAŁĄCZNIK I

Wymagania dotyczące kwalifikowanych certyfikatów podpisów elektronicznych

Kwalifikowane certyfikaty podpisów elektronicznych zawierają następujące informacje:

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

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

   – w przypadku osoby prawnej: nazwę i numer rejestracyjny zgodne z oficjalnym rejestrem,

   – w przypadku osoby fizycznej: imię i nazwisko;

c) zestaw danych jednoznacznie reprezentujących podpisującego, któremu został wydany certyfikat, w tym co najmniej imię i nazwisko podpisującego lub jego pseudonim – który jest identyfikowany jako taki;

d) dane służące do weryfikacji 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 dostawcy kwalifikowanych usług zaufania;

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

h) miejsce, w którym nieodpłatnie dostępny jest certyfikat potwierdzający zaawansowany podpis elektroniczny lub zaawansowaną pieczęć elektroniczną, o których mowa w lit. g);

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

j) jeżeli dane służące do składania podpisu elektronicznego powiązane z danymi służącymi do weryfikacji podpisu elektronicznego znajdują się w urządzeniu do składania kwalifikowanego podpisu elektronicznego, odpowiednie wskazanie tego faktu co najmniej w formie pozwalającej na automatyczne przetwarzanie.

ZAŁĄCZNIK II

Wymagania dotyczące urządzeń do składania kwalifikowanych podpisu

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

a) poufność danych służących do składania podpisu użytych do wygenerowania podpisu elektronicznego;

b) tylko jednorazowe wystąpienie danych służących do składania podpisu użytych do wygenerowania podpisu;

c) uniemożliwienie, na ile jest to wykonalne, pozyskania danych służących do składania podpisu użytych do wygenerowania podpisu oraz ochronę podpisu przed sfałszowaniem za pomocą aktualnie dostępnych technologii;

d) wiarygodną ochronę danych służących do składania podpisu użytych do wygenerowania podpisu przez uprawnionego podpisującego przed użyciem przez innych.

2. Urządzenia do składania kwalifikowanego 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 są generowane lub zarządzane w imieniu podpisującego przez dostawcę kwalifikowanych usług zaufania.

4. Dostawca kwalifikowanych usług zaufania zarządzający danymi służącymi do składania podpisu w imieniu podpisującego może kopiować dane służące do składania podpisu w celu utworzenia kopii zapasowej, o ile spełnione są następujące warunki:

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

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

ZAŁĄCZNIK III

Wymagania dotyczące kwalifikowanych certyfikatów pieczęci elektronicznych

Kwalifikowane certyfikaty pieczęci elektronicznych zawierają:

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

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

   – w przypadku osoby prawnej: nazwę i numer rejestracyjny zgodne z oficjalnym rejestrem,

   – w przypadku osoby fizycznej: imię i nazwisko;

c) zbiór danych jednoznacznie reprezentujących osobę prawną, której został wydany certyfikat, w tym co najmniej nazwę oraz numer rejestracyjny zgodne z oficjalnym rejestrem;

d) dane służące do weryfikacji pieczęci elektronicznej odpowiadają danym służącym do wystawiania pieczęci elektronicznej;

e) dane dotyczące początku i końca okresu ważności certyfikatu;

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

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

h) miejsce, w którym nieodpłatnie dostępny jest certyfikat potwierdzający zaawansowany podpis elektroniczny lub zaawansowaną pieczęć elektroniczną, o których mowa w lit. g);

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

j) jeżeli dane służące do wystawiania pieczęci elektronicznej powiązane z danymi służącymi do weryfikacji pieczęci elektronicznej znajdują się w urządzeniu do wystawiania kwalifikowanej pieczęci elektronicznej, odpowiednie wskazanie tego faktu co najmniej w formie pozwalającej na automatyczne przetwarzanie.

ZAŁĄCZNIK IV

Wymagania dotyczące kwalifikowanych certyfikatów uwierzytelniania witryn internetowych

Kwalifikowane certyfikaty uwierzytelniania witryn internetowych zawierają:

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

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

   – w przypadku osoby prawnej: nazwę i numer rejestracyjny zgodne z oficjalnym rejestrem,

   – w przypadku osoby fizycznej: imię i nazwisko;

c) zbiór danych jednoznacznie reprezentujących osobę prawną, której został wydany certyfikat, w tym co najmniej nazwę oraz numer rejestracyjny zgodne z oficjalnym rejestrem;

d) elementy adresu, w tym co najmniej miasto i państwo członkowskie, osoby prawnej, które wystawiono certyfikat, zgodne z oficjalnym rejestrem;

e) nazwę (nazwy) domen, z których korzysta osoba prawna, której wystawiono certyfikat;

f) dane dotyczące początku i końca okresu ważności certyfikatu;

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

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

i) miejsce, w którym nieodpłatnie dostępny jest certyfikat potwierdzający zaawansowany podpis elektroniczny lub zaawansowaną pieczęć elektroniczną, o których mowa w lit. h);

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

OCENA SKUTKÓW FINANSOWYCH REGULACJI

1. STRUKTURA WNIOSKU/INICJATYWY

W niniejszej ocenie skutków finansowych szczegółowo przedstawiono wymagania pod względem wydatków administracyjnych w celu wdrożenia rozporządzenia w sprawie identyfikacji elektronicznej i usług zaufania w odniesieniu do transakcji elektronicznych na rynku wewnętrznym, którego dotyczy wniosek.

Po przeprowadzeniu procedury ustawodawczej i odbyciu dyskusji w celu przyjęcia rozporządzenia, którego dotyczy wniosek, przez Parlament Europejski i Radę, Komisja będzie potrzebowała dwunastu EPC w celu opracowania związanych z wnioskiem aktów delegowanych i wykonawczych, zapewnienia dostępności norm organizacyjnych i technicznych, zarządzania informacjami zgłaszanymi przez państwa członkowskie – w szczególności utrzymywania informacji związanych z zaufanymi listami – a także w celu dopilnowania, aby zainteresowane strony – w szczególności obywatele oraz małe i średnie przedsiębiorstwa – były świadome korzyści płynących ze stosowania identyfikacji elektronicznej, uwierzytelniania elektronicznego i podpisu elektronicznego oraz związanych z nimi usług zaufania (eIAS), oraz w celu prowadzenia rozmów z państwami trzecimi w celu osiągnięcia interoperacyjności eIAS na skalę światową.

1.1. Tytuł wniosku/inicjatywy

Wniosek Komisji w sprawie identyfikacji elektronicznej i usług zaufania w odniesieniu do transakcji elektronicznych na rynku wewnętrznym

1.2. Dziedzina(-y) polityki w strukturze ABM/ABB, których dotyczy wniosek/inicjatywa[25]

09 SPOŁECZEŃSTWO INFORMACYJNE

1.3. Charakter wniosku/inicjatywy

☐ Wniosek/inicjatywa dotyczy **nowego działania**

☐ Wniosek/inicjatywa dotyczy **nowego działania będącego następstwem projektu pilotażowego/działania przygotowawczego**[26]

☐ Wniosek/inicjatywa wiąże się z **przedłużeniem bieżącego działania**

☑ Wniosek/inicjatywa dotyczy **działania, które zostało przekształcone pod kątem nowego działania**

[25] ABM: Activity Based Management: zarządzanie kosztami działań - ABB: Activity Based Budgeting: budżet zadaniowy.

[26] O którym mowa w art. 49 ust. 6 lit. a) lub b) rozporządzenia finansowego.

1.4. Cele

1.4.1. Wieloletni(e) cel(e) strategiczny(-e) Komisji wskazany(-e) we wniosku/inicjatywie

Ogólnymi celami wniosku są cele ogólnych strategii UE, w których osadzony jest wniosek, takich jak strategia „UE 2020”. Celem wniosku jest zagwarantowanie, że gospodarka Europy „stanie się inteligentna i zrównoważona, będzie sprzyjać włączeniu społecznemu, będzie się mogła pochwalić wysokimi wskaźnikami zatrudnienia i wydajności oraz większą spójnością społeczną”.

1.4.2. Cel(e) szczegółowy(-e) i działanie(-a) ABM/ABB, których dotyczy wniosek/inicjatywa

Zwiększenie zaufania do ogólnoeuropejskich transakcji elektronicznych oraz zapewnienie transgranicznego prawnego uznawania identyfikacji elektronicznej, uwierzytelnienia elektronicznego i podpisu elektronicznego oraz związanych z nimi usług zaufania, a także wysokiego poziomu ochrony danych i wzmocnienia pozycji użytkownika na jednolitym rynku (zob. Europejska agenda cyfrowa, główne działania 3 i 16).

Działanie(-a) ABM/ABB, którego(-ych) dotyczy wniosek/inicjatywa

09 02 – Ramy regulacyjne na potrzeby Europejskiej agendy cyfrowej

1.4.3. Oczekiwany(-e) wynik(i) i wpływ

Należy wskazać, jakie efekty przyniesie wniosek/inicjatywa beneficjentom/grupie docelowej.

Ustanowienie wyraźnego otoczenia regulacyjnego w zakresie usług eIAS, dzięki któremu użytkownik będzie się wygodniej poruszał w świecie cyfrowym i będzie go darzył większym zaufaniem.

1.4.4. Wskaźniki wyników i wpływu

Należy określić wskaźniki, które umożliwią monitorowanie realizacji wniosku/inicjatywy.

1. Istnienie dostawców usług eIAS prowadzących działalność w wielu państwach członkowskich UE;

2. Stopień interoperacyjności urządzeń (np. czytników kart elektronicznych) między sektorami i państwami;

3. Wykorzystanie usług eIAS przez wszystkie grupy społeczne;

4. Stopień, w jakim z usług eIAS korzystają użytkownicy końcowi w zakresie transakcji krajowych i międzynarodowych (transgranicznych);

5. Stopień harmonizacji usług eIAS między państwami członkowskimi;

6. Systemy identyfikacji elektronicznej zgłoszone Komisji;

7. Usługi dostępne przy zastosowaniu zgłoszonych środków identyfikacji elektronicznej w sektorze publicznym (administracja elektroniczna, e-zdrowie, e-sprawiedliwość, e-zamówienia);

8. Usługi dostępne przy zastosowaniu zgłoszonych środków identyfikacji elektronicznej w sektorze prywatnym (bankowość internetowa, handel elektroniczny,

hazard internetowy, logowanie się do stron internetowych, usługi w ramach programu „Bezpieczniejszy Internet”).

1.5. Uzasadnienie wniosku/inicjatywy

1.5.1. Potrzeba(-y), która(-e) ma(-ją) zostać zaspokojona(-e) w perspektywie krótko- lub długoterminowej

Zróżnicowane wdrażanie dyrektywy w sprawie podpisów elektronicznych w poszczególnych państwach wynikające z jej różnych interpretacji w poszczególnych państwach członkowskich spowodowało problemy w zakresie transgranicznej interoperacyjności, a przez to doprowadziło do rozdrobnienia w UE i do zakłóceń na rynku wewnętrznym. Towarzyszy temu brak zaufania do systemów elektronicznych utrudniający obywatelom europejskim korzystanie w świecie cyfrowym z tego samego rodzaju usług, co w świecie fizycznym.

1.5.2. Wartość dodana z tytułu zaangażowania Unii Europejskiej

Działania podejmowane na szczeblu UE przyniosłyby wyraźne korzyści w porównaniu z działaniami podejmowanymi na szczeblu państw członkowskich. Jak wynika z dotychczasowych doświadczeń, środki krajowe są nie tylko niewystarczające, aby umożliwić realizowanie transakcji elektronicznych ponad granicami, ale w rzeczywistości tworzą bariery dla ogólnounijnej interoperacyjności podpisów elektronicznych i obecnie mają taki sam wpływ na identyfikację elektroniczną, uwierzytelnianie elektroniczne i powiązane usługi zaufania.

1.5.3. Główne wnioski wyciągnięte z podobnych działań

Wniosek opiera się na doświadczeniach uzyskanych w związku z implementacją dyrektywy w sprawie podpisu elektronicznego oraz na problemach wynikających z rozdrobnienia przepisów transponujących i wykonujących tę dyrektywę, które uniemożliwiły osiągnięcie jej celów.

1.5.4. Spójność z innymi właściwymi instrumentami oraz możliwa synergia

Do dyrektywy w sprawie podpisu elektronicznego nawiązuje szereg innych inicjatyw UE – przygotowanych w celu wyeliminowania problemów związanych z interoperacyjnością oraz problemów w zakresie transgranicznego uznawania i akceptowania dokumentów związanych z określonymi rodzajami kontaktów drogą elektroniczną – takich jak na przykład dyrektywa usługowa, dyrektywy w sprawie zamówień publicznych, zmieniona dyrektywa VAT (fakturowanie elektroniczne) i rozporządzenie w sprawie inicjatywy obywatelskiej.

Ponadto rozporządzenie, którego dotyczy wniosek, będzie stanowić ramy prawne, które pozytywnie wpłyną na szerokie rozpowszechnianie projektów pilotażowych na dużą skalę wdrażanych na szczeblu UE w celu wsparcia opracowania interoperacyjnych i wiarygodnych środków komunikacji elektronicznej (w tym SPOCS, w ramach którego wspiera się realizację dyrektywy usługowej; STORK, w ramach którego wspiera się rozwój i wykorzystanie interoperacyjnych środków identyfikacji elektronicznej; PEPPOL, w ramach którego wspiera się rozwój i wykorzystanie interoperacyjnych rozwiązań w zakresie e-zamówień; epSOS, w

ramach którego wspiera się rozwój i wykorzystanie interoperacyjnych rozwiązań w zakresie e-zdrowia; eCodex, w ramach którego wspiera się rozwój i wykorzystanie interoperacyjnych rozwiązań w zakresie e-sprawiedliwości).

1.6. Czas trwania działania i jego wpływ finansowy

☐ Wniosek/inicjatywa **o określonym czasie trwania**

– ☐ Czas trwania wniosku/inicjatywy: od [DD/MM]RRRR r. do [DD/MM]RRRR r.

– ☐ Czas trwania wpływu finansowego: od RRRR r. do RRRR r.

☑ Wniosek/inicjatywa **o nieokreślonym czasie trwania**

1.7. Przewidywany(-e) tryb(y) zarządzania[27]

☑ **Bezpośrednie zarządzanie scentralizowane** przez Komisję

☐ **Pośrednie zarządzanie scentralizowane** poprzez przekazanie zadań wykonawczych:

– ☐ agencjom wykonawczym

– ☐ organom utworzonym przez Wspólnoty[28]

– ☐ krajowym organom publicznym/organom mającym obowiązek świadczenia usługi publicznej

– ☐ osobom odpowiedzialnym za wykonanie określonych działań na mocy tytułu V Traktatu o Unii Europejskiej, określonym we właściwym prawnym akcie podstawowym w rozumieniu art. 49 rozporządzenia finansowego

☐ **Zarządzanie dzielone** z państwami członkowskimi

☐ **Zarządzanie zdecentralizowane** z państwami trzecimi

☐ **Zarządzanie wspólne** z organizacjami międzynarodowymi **(należy wyszczególnić)**

W przypadku wskazania więcej niż jednego trybu, należy podać dodatkowe informacje w części „Uwagi".

Uwagi

[//]

[27] Wyjaśnienia dotyczące trybów zarządzania oraz odniesienia do rozporządzenia finansowego znajdują się na następującej stronie: http://www.cc.cec/budg/man/budgmanag/budgmanag_en.html

[28] O którym mowa w art. 185 rozporządzenia finansowego.

2. ŚRODKI ZARZĄDZANIA

2.1. Zasady nadzoru i sprawozdawczości

Należy określić częstotliwość i warunki.

Pierwsza ocena zostanie dokonana po upływie czterech lat od wejścia w życie rozporządzenia. W rozporządzeniu przewidziano wyraźną klauzulę dotyczącą sprawozdania, w którym Komisja będzie przekazywać Parlamentowi Europejskiemu i Radzie informacje dotyczące jego stosowania. Następnie kolejne sprawozdania będą przedstawiane co 4 lata. Komisja będzie wykorzystywać wypracowaną przez siebie metodykę oceny. Powyższe oceny będą przeprowadzane za pomocą ukierunkowanych analiz wdrażania instrumentów prawnych, kwestionariuszy skierowanych do organów krajowych, dyskusji ekspertów, warsztatów, ankiet Eurobarometru itp.

2.2. System zarządzania i kontroli

2.2.1. Zidentyfikowane ryzyko

Niniejszemu wnioskowi dotyczącemu rozporządzenia towarzyszy przeprowadzona ocena skutków. Nowy instrument prawny umożliwi wzajemne uznawanie i akceptowanie identyfikacji elektronicznej ponad granicami, usprawni obecne ramy podpisów elektronicznych, zwiększy nadzór krajowy nad dostawcami usług zaufania oraz zapewni skutki prawne i uznawanie powiązanych usług zaufania. W rozporządzeniu wprowadza się również stosowanie aktów delegowanych i wykonawczych jako mechanizmu zapewniającego elastyczność względem zmian technologicznych.

2.2.2. Przewidywane metody kontroli

Istniejące metody kontroli stosowane przez Komisję obejmą środki dodatkowe.

2.3. Środki zapobiegania nadużyciom finansowym i nieprawidłowościom

Określić istniejące lub przewidywane środki zapobiegania i ochrony

Istniejące środki zapobiegania nadużyciom finansowym stosowane przez Komisję obejmą środki dodatkowe.

3. SZACUNKOWY WPŁYW FINANSOWY WNIOSKU/INICJATYWY

3.1. Dział(y) wieloletnich ram finansowych i pozycja(pozycje) wydatków w budżecie, na które wniosek/inicjatywa ma wpływ

- Istniejące pozycje w budżecie

Według działów wieloletnich ram finansowych i pozycji w budżecie

Dział wieloletnich ram finansowych	Pozycja w budżecie	Rodzaj środków	Wkład			
	Numer [Treść……...…….]	Zróżnico-wane /niezróżni-cowane (29)	państw EFTA[30]	krajów kandydujących[31]	państw trzecich	w rozumieniu art. 18 ust. 1 lit. aa) rozporządzenia finansowego
5	09. 01 01 01 Wydatki związane z personelem aktywnie zatrudnionym w DG ds. Społeczeństwa Informacyjnego i Mediów	Zróżnicowane /niezróżni-cowane	NIE	NIE	NIE	NIE
5	09. 01 02 01 Personel zewnętrzny	Zróżnicowane /niezróżni-cowane	NIE	NIE	NIE	NIE

29 Środki zróżnicowane/ środki niezróżnicowane.
30 EFTA: Europejskie Stowarzyszenie Wolnego Handlu.
31 Kraje kandydujące oraz w stosownych przypadkach potencjalne kraje kandydujące Bałkanów Zachodnich.

3.2. Szacunkowy wpływ na wydatki

3.2.1. Synteza szacunkowego wpływu na wydatki

Dział wieloletnich ram finansowych:	**Numer**	[Dział 1. **Inteligentny rozwój sprzyjający włączeniu społecznemu** ……..……]

DG: INFSO			Rok **2014**	Rok **2015**	Rok **2016**	Rok **2017**	Rok 2018	**Rok 2019**	**Rok 2020**	**OGÓŁEM**
• Środki operacyjne										
Numer pozycji w budżecie – nie dotyczy	Środki na zobowiązania	(1)	0.000	0.000	0.000	0.000	0.000	0.000	**0.000**	**0.000**
	Środki na płatności	(2)	0.000	0.000	0.000	0.000	0.000	0.000	**0.000**	**0.000**
Numer pozycji w budżecie – nie dotyczy	Środki na zobowiązania	(1a)	0.000	0.000	0.000	0.000	0.000	0.000	**0.000**	**0.000**
	Środki na płatności	(2a)	0.000	0.000	0.000	0.000	0.000	0.000	**0.000**	**0.000**
Środki administracyjne finansowane ze środków przydzielonych na określone programy operacyjne[32]			0.000	0.000	0.000	0.000	0.000	0.000	**0.000**	**0.000**
Numer pozycji w budżecie		(3)	0.000	0.000	0.000	0.000	0.000	0.000	**0.000**	**0.000**
OGÓŁEM środki dla DG INFSO	Środki na zobowiązania	=1+1a +3	0.000	0.000	0.000	0.000	0.000	0.000	**0.000**	**0.000**
	Środki na płatności	=2+2a	0.000	0.000	0.000	0.000	0.000	0.000	**0.000**	**0.000**

[32] Wsparcie techniczne lub administracyjne oraz wydatki na wsparcie w zakresie wprowadzania w życie programów lub działań UE (dawne pozycje „BA"), pośrednie badania naukowe, bezpośrednie badania naukowe.

		+3								

Dział wieloletnich ram finansowych:	**5**	„Wydatki administracyjne”

w mln EUR (do 3 miejsc po przecinku)

		Rok **2014**	Rok **2015**	Rok **2016**	Rok **2017**	Rok 2018	Rok 2019	Rok 2020	**OGÓŁEM**
		DG: INFSO							
• Zasoby ludzkie		1,344	1,344	1,344	1,344	1,344	1,344	1,344	**9,408**
• Pozostałe wydatki administracyjne									
OGÓŁEM DG INFSO	Środki	1,344	1,344	1,344	1,344	1,344	1,344	1,344	**9,408**

OGÓŁEM środki na DZIAŁ 5 wieloletnich ram finansowych	(Środki na zobowiązania ogółem = środki na płatności ogółem)	1,344	1,344	1,344	1,344	1,344	1,344	1,344	**9,408**

w mln EUR (do 3 miejsc po przecinku)

		Rok **2014**	Rok **2015**	Rok **2016**	Rok **2017**	Rok 2018	Rok 2019	Rok 2020	**OGÓŁEM**
OGÓŁEM środki na DZIAŁY 1 do 5 wieloletnich ram finansowych	Środki na zobowiązania	1,344	1,344	1,344	1,344	1,344	1,344	1,344	**9,408**
	Środki na płatności	1,344	1,344	1,344	1,344	1,344	1,344	1,344	**9,408**

3.2.2. Szacunkowy wpływ na środki operacyjne

– ☑ Wniosek/inicjatywa nie wiąże się z koniecznością wykorzystania środków operacyjnych

– ☐ Wniosek/inicjatywa wiąże się z koniecznością wykorzystania środków operacyjnych, jak określono poniżej:

3.2.3. Szacunkowy wpływ na środki administracyjne

3.2.3.1. Streszczenie

– ☐ Wniosek/inicjatywa nie wiąże się z koniecznością wykorzystania środków administracyjnych

– ☑ Wniosek/inicjatywa wiąże się z koniecznością wykorzystania środków administracyjnych, jak określono poniżej:

w mln EUR (do 3 miejsc po przecinku)

	Rok **N 2014**	Rok **2015**	Rok **2016**	Rok **2017**	Rok **2018**	Rok **2019**	Rok **2020**	**OGÓŁEM**
DZIAŁ 5 wieloletnich ram finansowych								
Zasoby ludzkie	1,344	1,344	1,344	1,344	1,344	1,344	1,344	**9,408**
Pozostałe wydatki administracyjne								
DZIAŁ 5 wieloletnich ram finansowych – suma cząstkowa	1,344	1,344	1,344	1,344	1,344	1,344	1,344	**9,408**

Poza DZIAŁEM 5[33] wieloletnich ram finansowych								
Zasoby ludzkie								
Pozostałe wydatki administracyjne								
Poza DZIAŁEM 5 wieloletnich ram finansowych – suma cząstkowa								

OGÓŁEM	1,344	1,344	1,344	1,344	1,344	1,344	1,344	**9,408**

[33] Wsparcie techniczne lub administracyjne oraz wydatki na wsparcie w zakresie wprowadzania w życie programów lub działań UE (dawne pozycje „BA"), pośrednie badania naukowe, bezpośrednie badania naukowe.

3.2.3.2. Szacowane zapotrzebowanie na zasoby ludzkie

– ☐ Wniosek/inicjatywa nie wiąże się z koniecznością wykorzystania zasobów ludzkich

– ☑ Wniosek/inicjatywa wiąże się z koniecznością wykorzystania zasobów ludzkich, jak określono poniżej:

Wartości szacunkowe należy wyrazić w pełnych kwotach (lub najwyżej z dokładnością do jednego miejsca po przecinku)

	Rok **2014**	Rok **2015**	Rok **2016**	Rok **2017**	Rok **2018**	Rok **2019**	Rok **2020**
• Stanowiska przewidziane w planie zatrudnienia (stanowiska urzędników i pracowników zatrudnionych na czas określony)							
09 01 01 01 (w centrali i w biurach przedstawicielstw Komisji)	9	9	9	9	9	9	9
XX 01 01 02 (w delegaturach)							
XX 01 05 01 (pośrednie badania naukowe)							
10 01 05 01 (bezpośrednie badania naukowe)							
• Personel zewnętrzny (w ekwiwalentach pełnego czasu pracy)[34]							
09 01 02 01 (AC, END, INT z globalnej koperty finansowej)	3	3	3	3	3	3	3
XX 01 02 02 (AC, AL, END, INT i JED w delegaturach)							
XX 01 04 yy[35] - w centrali[36]							
XX 01 04 yy[35] - w delegaturach							
XX 01 05 02 (AC, END, INT - pośrednie badania naukowe)							
10 01 05 02 (AC, END, INT - bezpośrednie badania naukowe)							
Inna pozycja w budżecie (określić)							
OGÓŁEM	**12**	**12**	**12**	**12**	**12**	**12**	**12**

Potrzeby w zakresie zasobów ludzkich zostaną pokryte z zasobów DG już przydzielonych na zarządzanie tym działaniem lub przesuniętych w ramach dyrekcji generalnej, uzupełnionych w razie potrzeby wszelkimi dodatkowymi zasobami, które mogą zostać przydzielone zarządzającej dyrekcji generalnej w ramach procedury rocznego przydziału środków oraz w świetle istniejących ograniczeń budżetowych.

Opis zadań do wykonania:

Urzędnicy i pracownicy zatrudnieni na czas określony	Zarządzenie procedurami ustawodawczymi w celu przyjęcia przez Parlament Europejski i Radę planowanego rozporządzenia oraz związanych z nim aktów delegowanych/wykonawczych.

[34] AC= pracownik kontraktowy; INT= pracownik tymczasowy; JED= młodszy oddelegowany ekspert; AL= członek personelu miejscowego; END= oddelegowany ekspert krajowy.

[35] Poniżej pułapu na personel zewnętrzny ze środków operacyjnych (dawne pozycje „BA").

[36] Przede wszystkim fundusze strukturalne, Europejski Fundusz Rolny na rzecz Rozwoju Obszarów Wiejskich (EFRROW) oraz Europejski Fundusz Rybacki.

	Obszary priorytetowe: 1. Ustanowienie nowych ram prawnych dotyczących elektronicznych usług zaufania 2. Promowanie wykorzystania elektronicznych usług zaufania przez podnoszenie świadomości MŚP i obywateli w zakresie potencjału tych usług 3. Działania następcze względem dyrektywy 1999/93/WE, z uwzględnieniem aspektów międzynarodowych 4. Wykorzystanie potencjału projektów pilotażowych na dużą skalę w celu przyspieszenia konkretnej realizacji celu polegającego na utworzeniu nowych ram prawnych.
Personel zewnętrzny	jw.

3.2.4. Zgodność z obowiązującymi wieloletnimi ramami finansowymi

– ☑ Wniosek/inicjatywa jest zgodny(-a) z obowiązującymi wieloletnimi ramami finansowymi.

– ☐ Wniosek/inicjatywa wymaga przeprogramowania odpowiedniego działu w wieloletnich ramach finansowych.

Należy wyjaśnić, na czym ma polegać przeprogramowanie, określając pozycje w budżecie, których ma ono dotyczyć, oraz podając odpowiednie kwoty.

– ☐ Wniosek/inicjatywa wymaga zastosowania instrumentu elastyczności lub zmiany wieloletnich ram finansowych[37].

Należy wyjaśnić, który wariant jest konieczny, określając pozycje w budżecie, których ma on dotyczyć, oraz podając odpowiednie kwoty.

3.2.5. Udział osób trzecich w finansowaniu

– ☑ Wniosek/inicjatywa nie przewiduje współfinansowania ze strony osób trzecich.

– ☐ Wniosek/inicjatywa przewiduje współfinansowanie szacowane zgodnie z poniższym:

3.3. Szacunkowy wpływ na dochody

– ☑ Wniosek/inicjatywa nie ma wpływu finansowego na dochody.

– ☐ Wniosek/inicjatywa ma wpływ finansowy określony poniżej:

- ☐ wpływ na zasoby własne
- ☐ wpływ na dochody różne

[37] Zob. pkt 19 i 24 porozumienia międzyinstytucjonalnego.