Rada
Unii Europejskiej

Bruksela, 3 czerwca 2021 r.
(OR. en)

9471/21

Międzyinstytucjonalny numer referencyjny:
2021/0136 (COD)

TELECOM 242
COMPET 457
MI 432
DATAPROTECT 156
JAI 670
IA 108
CODEC 826

WNIOSEK

Od:	Sekretarz generalna Komisji Europejskiej (podpisała dyrektor Martine DEPREZ)
Data otrzymania:	3 czerwca 2021 r.
Do:	Jeppe TRANHOLM-MIKKELSEN, sekretarz generalny Rady Unii Europejskiej
Nr dok. Kom.:	COM(2021) 281 final
Dotyczy:	Wniosek dotyczący ROZPORZĄDZENIA PARLAMENTU EUROPEJSKIEGO I RADY zmieniającego rozporządzenie (UE) nr 910/2014 w odniesieniu do ustanowienia europejskich ram tożsamości cyfrowej

Delegacje otrzymują w załączeniu dokument COM(2021) 281 final.

Zał.: COM(2021) 281 final

KOMISJA
EUROPEJSKA

Bruksela, dnia 3.6.2021 r.
COM(2021) 281 final

2021/0136 (COD)

Wniosek

ROZPORZĄDZENIE PARLAMENTU EUROPEJSKIEGO I RADY

zmieniające rozporządzenie (UE) nr 910/2014 w odniesieniu do ustanowienia europejskich ram tożsamości cyfrowej

{SEC(2021) 228 final} - {SWD(2021) 124 final} - {SWD(2021) 125 final}

UZASADNIENIE

1. KONTEKST WNIOSKU

• Przyczyny i cele wniosku

Niniejsze uzasadnienie towarzyszy wnioskowi dotyczącemu rozporządzenia Parlamentu Europejskiego i Rady zmieniającego rozporządzenie Parlamentu Europejskiego i Rady (UE) nr 910/2014 z dnia 23 lipca 2014 r. w sprawie identyfikacji elektronicznej i usług zaufania w odniesieniu do transakcji elektronicznych na rynku wewnętrznym (rozporządzenie eIDAS)[1]. Ten instrument prawny służy zapewnieniu w kontekście korzystania transgranicznego:

– dostępu do wysoce bezpiecznych i wiarygodnych rozwiązań w zakresie tożsamości elektronicznej;

– aby usługi publiczne i prywatne mogły opierać się na zaufanych i bezpiecznych rozwiązaniach w zakresie tożsamości cyfrowej;

– aby osoby fizyczne i prawne były uprawnione do korzystania z rozwiązań w zakresie tożsamości cyfrowej;

– aby rozwiązania te były powiązane z różnymi atrybutami i umożliwiały ukierunkowane udostępnianie danych dotyczących tożsamości ograniczone do potrzeb konkretnej żądanej usługi;

– akceptacji kwalifikowanych usług zaufania w UE i równych warunków ich świadczenia.

Na rynku powstaje nowe środowisko, w którym uwaga nie jest skoncentrowana na świadczeniu i stosowaniu sztywnych tożsamości cyfrowych, ale na zapewnieniu szczególnych atrybutów związanych z takimi tożsamościami i poleganiu na takich atrybutach. Wzrasta zapotrzebowanie na rozwiązania w zakresie tożsamości elektronicznej, w ramach których zapewnia się tego rodzaju zdolności i dzięki którym następuje przyrost wydajności i osiągnięty zostaje wysoki poziom zaufania w całej UE, zarówno w sektorze prywatnym, jak i w sektorze publicznym, w związku z koniecznością identyfikacji i uwierzytelnienia użytkowników przy zapewnieniu wysokiego poziomu bezpieczeństwa.

Ocena rozporządzenia eIDAS[2] wykazała, że w jego obecnym kształcie te nowe potrzeby rynkowe nie są zaspokajane ze względu na jego wewnętrzne ograniczenia do sektora publicznego, ograniczone możliwości i złożoność procesu połączenia z systemem dostawców usług online z sektora prywatnego, niewystarczającą dostępność notyfikowanych rozwiązań z zakresu identyfikacji elektronicznej we wszystkich państwach członkowskich oraz brak elastyczności rozporządzenia umożliwiającej uwzględnienie różnego rodzaju przypadków użycia. Ponadto rozwiązania w zakresie tożsamości wykraczające poza zakres eIDAS, takie jak te, które oferują dostawcy mediów społecznościowych i instytucje finansowe, budzą obawy dotyczące prywatności i ochrony danych. Rozwiązania te nie mogą zapewnić skutecznej reakcji na nowe potrzeby rynkowe i nie mają zasięgu transgranicznego, który pozwalałby zaspokoić szczególne potrzeby sektorowe, w przypadku gdy identyfikacja jest wrażliwa i wymaga wysokiego stopnia pewności.

---

[1] Dz.U. L 257 z 28.8.2014, s. 73.

[2] [po przyjęciu dodać odesłanie]

Od wejścia w życie części rozporządzenia dotyczącej identyfikacji elektronicznej we wrześniu 2018 r. tylko 14 państw członkowskich notyfikowało przynajmniej jeden system identyfikacji elektronicznej. W rezultacie jedynie 59 % mieszkańców UE ma dostęp do zaufanych i bezpiecznych systemów identyfikacji elektronicznej o wymiarze transgranicznym. Tylko siedem systemów to rozwiązania w pełni mobilne, odpowiadające obecnym oczekiwaniom użytkowników. Ponieważ nie wszystkie węzły techniczne mające zapewniać połączenie z ramami interoperacyjności eIDAS w pełni funkcjonują, dostęp transgraniczny jest ograniczony; z bardzo niewielu usług publicznych online dostępnych w kraju można korzystać transgranicznie za pośrednictwem sieci eIDAS.

Dzięki europejskim ramom tożsamości cyfrowej opartym na przeglądzie obecnych ram do 2030 r. co najmniej 80 % obywateli powinno mieć możliwość korzystania z rozwiązań w zakresie tożsamości cyfrowej na potrzeby uzyskiwania dostępu do kluczowych usług publicznych. Ponadto bezpieczeństwo i kontrola, jakie oferują europejskie ramy tożsamości cyfrowej, powinny dawać obywatelom i rezydentom całkowitą pewność, że ramy te zapewnią wszystkim środki pozwalające kontrolować, kto ma dostęp do ich cyfrowego bliźniaka i do jakich konkretnie danych. Będzie to również wymagało wysokiego poziomu bezpieczeństwa w odniesieniu do wszystkich aspektów świadczenia usług w zakresie tożsamości cyfrowej, w tym wydawania europejskiego portfela tożsamości cyfrowej, oraz infrastruktury służącej do gromadzenia, przechowywania i ujawniania danych dotyczących tożsamości cyfrowej.

Ponadto obecne ramy eIDAS nie obejmują dostarczania atrybutów elektronicznych, takich jak orzeczenia lekarskie lub kwalifikacje zawodowe, co utrudnia zapewnienie ogólnoeuropejskiego prawnego uznawania takich danych uwierzytelniających w postaci elektronicznej. Rozporządzenie eIDAS nie daje użytkownikom również możliwości ograniczenia udostępniania danych dotyczących tożsamości do tego, co jest absolutnie niezbędne do świadczenia usługi.

Chociaż z oceny rozporządzenia eIDAS wynika, że ramy świadczenia usług zaufania są raczej skuteczne, gdyż zapewniają wysoki poziom zaufania oraz upowszechnianie i wykorzystywanie większości usług zaufania, potrzebne są dalsze działania, aby osiągnąć pełną harmonizację i akceptację. W przypadku kwalifikowanych certyfikatów uwierzytelniania witryn internetowych obywatele muszą być w stanie na takich certyfikatach polegać i korzystać z bezpiecznych i wiarygodnych informacji o tym, kto stoi za daną witryną internetową, co pozwoli ograniczyć oszustwa.

Ponadto aby zareagować na dynamikę rynków i rozwój technologiczny, w niniejszym wniosku rozszerzono obecny wykaz usług zaufania eIDAS o trzy nowe kwalifikowane usługi zaufania, mianowicie świadczenie usług archiwizacji elektronicznej, rejestry elektroniczne oraz zarządzanie urządzeniami do składania podpisów i pieczęci elektronicznych na odległość.

Niniejszy wniosek przewiduje również zharmonizowane podejście do bezpieczeństwa – dla obywateli, którzy korzystają z europejskiej tożsamości cyfrowej reprezentującej ich online, oraz dla dostawców usług online, którzy będą mogli w pełni polegać na rozwiązaniach w zakresie tożsamości cyfrowej i akceptować je niezależnie od tego, gdzie je wydano. Niniejszy wniosek wiąże się ze zmianami dla wydawców europejskich rozwiązań w zakresie tożsamości cyfrowej, gdyż przewidziano w nim wspólną architekturę techniczną i ramy odniesienia oraz wspólne normy, które mają powstać we współpracy z państwami członkowskimi. Zharmonizowane podejście jest konieczne, by uniknąć sytuacji, w której opracowywanie w państwach członkowskich nowych rozwiązań w zakresie tożsamości

cyfrowej prowadzi do dalszej fragmentacji powodowanej stosowaniem rozbieżnych rozwiązań krajowych. Zharmonizowane podejście wzmocni także jednolity rynek, ponieważ umożliwi obywatelom, innym rezydentom i przedsiębiorstwom identyfikację online w sposób bezpieczny, dogodny i jednolity w całej UE na potrzeby dostępu zarówno do usług publicznych, jak i prywatnych. Użytkownicy będą mogli polegać na ulepszonym ekosystemie tożsamości elektronicznej i usług zaufania uznawanym i akceptowanym w całej Unii.

Aby uniknąć fragmentacji i barier wynikających z rozbieżnych norm, Komisja przyjmie zalecenie w tym samym czasie co niniejszy wniosek. W zaleceniu tym Komisja określi proces wspierania wspólnego podejścia umożliwiającego państwom członkowskim i innym zainteresowanym stronom z sektora publicznego i prywatnego działanie – w ścisłej koordynacji z Komisją – na rzecz opracowania zestawu narzędzi, aby uniknąć rozbieżnych podejść i zagrożenia dla przyszłego wdrożenia europejskich ram tożsamości cyfrowej.

- **Spójność z przepisami obowiązującymi w tej dziedzinie polityki**

Niniejszy wniosek opiera się na rozporządzeniu eIDAS w jego obecnym kształcie, na roli państw członkowskich jako dostawców tożsamości prawnej oraz na ramach świadczenia usług zaufania w Unii Europejskiej. Wniosek uzupełnia inne instrumenty polityki na szczeblu UE, których celem jest przełożenie korzyści płynących z rynku wewnętrznego na świat cyfrowy, w szczególności dzięki zwiększeniu możliwości transgranicznego dostępu obywateli do usług, i jest w pełni spójny z tymi instrumentami. W tym względzie we wniosku realizuje się mandat polityczny, którego udzieliły Rada Europejska[3] i przewodnicząca Komisji Europejskiej[4], dotyczący ustanowienia ogólnounijnych ram publicznej tożsamości elektronicznej zapewniających każdemu obywatelowi lub rezydentowi możliwość dostępu do bezpiecznej europejskiej tożsamości elektronicznej, którą można wykorzystywać w dowolnym miejscu w UE do celów identyfikacji i uwierzytelniania na potrzeby dostępu do usług w sektorze publicznym i prywatnym, oraz umożliwiających obywatelom kontrolowanie, jakie dane są przekazywane i w jaki sposób są one wykorzystywane.

- **Spójność z innymi politykami Unii**

Wniosek jest spójny z priorytetami transformacji cyfrowej określonymi w strategii „Kształtowanie cyfrowej przyszłości Europy”[5] i przyczyni się do osiągnięcia celów wyznaczonych w komunikacie dotyczącym cyfrowej dekady[6]. Wszelkie przetwarzanie danych osobowych na podstawie niniejszego rozporządzenia powinno odbywać się w pełnej zgodności z ogólnym rozporządzeniem o ochronie danych (zwanym dalej „RODO”)[7]. Ponadto w niniejszym rozporządzeniu wprowadza się szczególne zabezpieczenia służące ochronie danych.

---

3 https://www.consilium.europa.eu/media/45927/021020-euco-final-conclusions-pl.pdf

4 Orędzie o stanie Unii wygłoszone w dniu 16 września 2020 r., zob. https://ec.europa.eu/commission/presscorner/detail/pl/SPEECH_20_1655

5 Komunikat Komisji do Parlamentu Europejskiego, Rady, Europejskiego Komitetu Ekonomiczno-Społecznego i Komitetu Regionów „Kształtowanie cyfrowej przyszłości Europy”.

6 Komunikat Komisji do Parlamentu Europejskiego, Rady, Europejskiego Komitetu Ekonomiczno-Społecznego i Komitetu Regionów „Cyfrowy kompas na 2030 r.: europejska droga w cyfrowej dekadzie”.

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

W celu zapewnienia wysokiego poziomu bezpieczeństwa wniosek jest również spójny z polityką Unii w obszarach związanych z cyberbezpieczeństwem[8]. Wniosek opracowano w sposób ograniczający fragmentację, z zastosowaniem ogólnych wymogów cyberbezpieczeństwa do dostawców usług zaufania regulowanych rozporządzeniem eIDAS.

Niniejszy wniosek jest ponadto spójny z innymi politykami sektorowymi opartymi na korzystaniu z tożsamości elektronicznej, elektronicznych poświadczeń atrybutów i innych usług zaufania. Obejmuje to rozporządzenie w sprawie jednolitego portalu cyfrowego[9], wymogi związane z przeciwdziałaniem praniu pieniędzy i finansowaniu terroryzmu, które należy spełnić w sektorze finansowym, inicjatywy na rzecz udostępniania danych uwierzytelniających dotyczących zabezpieczenia społecznego na potrzeby cyfrowego prawa jazdy lub przyszłych cyfrowych dokumentów podróży oraz inne inicjatywy mające na celu zmniejszenie obciążenia administracyjnego obywateli i przedsiębiorstw z wykorzystaniem w pełni możliwości wynikających z transformacji cyfrowej procedur zarówno w sektorze publicznym, jak i prywatnym. Portfel umożliwi ponadto stosowanie kwalifikowanych podpisów elektronicznych, które mogą ułatwić udział w życiu politycznym[10].

2. PODSTAWA PRAWNA, POMOCNICZOŚĆ I PROPORCJONALNOŚĆ

• Podstawa prawna

Celem niniejszej inicjatywy jest wsparcie transformacji Unii w kierunku jednolitego rynku cyfrowego. W kontekście postępującej cyfryzacji transgranicznych usług publicznych i prywatnych, które opierają się na stosowaniu rozwiązań w zakresie tożsamości cyfrowej, istnieje ryzyko, że w obecnych ramach prawnych obywatele nadal będą napotykać przeszkody i nie będą w stanie w pełni korzystać w całej UE z usług online w sposób niezakłócony ani chronić swojej prywatności. Występuje także ryzyko, że niedociągnięcia obecnych ram prawnych dotyczących usług zaufania zwiększyłyby fragmentację i zmniejszyłyby zaufanie, gdyby zaradzenie im pozostawiono wyłącznie w gestii państw członkowskich. W związku z tym jako odpowiednią podstawę prawną niniejszej inicjatywy wskazuje się art. 114 TFUE.

• Pomocniczość (w przypadku kompetencji niewyłącznych)

Obywatele i przedsiębiorstwa powinni móc korzystać z dostępności wysoce bezpiecznych i wiarygodnych rozwiązań w zakresie tożsamości cyfrowej, które mogą być stosowane w całej UE, oraz z możliwości przenoszenia elektronicznych poświadczeń atrybutów powiązanych z tożsamością. Najnowsze osiągnięcia technologiczne, sytuacja na rynku i zapotrzebowanie użytkowników wymagają dostępności bardziej przyjaznych dla użytkownika rozwiązań transgranicznych, które umożliwiają dostęp do usług online w całej UE, czego rozporządzenie eIDAS w swoim obecnym kształcie nie może zaoferować.

Użytkownicy coraz bardziej przyzwyczajają się także do rozwiązań dostępnych na całym świecie, na przykład w kontekście korzystania z rozwiązań takich jak pojedyncze logowanie, które większe platformy mediów społecznościowych zapewniają do celów dostępu do usług online. Państwa członkowskie nie są w stanie samodzielnie sprostać wyzwaniom, jakie stwarza to pod względem władzy rynkowej dużych dostawców usług – potrzebne są interoperacyjność i wiarygodne systemy identyfikacji elektronicznej na szczeblu UE. Ponadto elektroniczne

[8] https://ec.europa.eu/commission/presscorner/detail/pl/IP_20_2391

[9] Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2018/1724 z dnia 2 października 2018 r. w sprawie utworzenia jednolitego portalu cyfrowego w celu zapewnienia dostępu do informacji, procedur oraz usług wsparcia i rozwiązywania problemów, Dz.U. L 295 z 21.11.2018, s. 1.

[10] Europejski plan działania na rzecz demokracji, COM(2020) 790 final.

poświadczenia atrybutów wydawane i akceptowane w jednym państwie członkowskim, takie jak elektroniczne świadectwo zdrowia, często nie są prawnie uznawane i akceptowane w innych państwach członkowskich. Stwarza to ryzyko, że państwa członkowskie będą nadal opracowywać fragmentaryczne rozwiązania krajowe, które nie mogą funkcjonować w kontekście transgranicznym.

Jeżeli chodzi o świadczenie usług zaufania, to mimo że są one w dużej mierze uregulowane i funkcjonują zgodnie z obowiązującymi przepisami, praktyki krajowe również stwarzają ryzyko większej fragmentacji.

Interwencja na szczeblu UE jest ostatecznie najodpowiedniejsza, aby zapewnić obywatelom i przedsiębiorstwom środki umożliwiające identyfikację transgraniczną i wymianę osobistych atrybutów tożsamości i danych uwierzytelniających za pomocą wysoce bezpiecznych i wiarygodnych rozwiązań w zakresie tożsamości cyfrowej zgodnie z unijnymi przepisami o ochronie danych. Wymaga to zaufanej i bezpiecznej identyfikacji elektronicznej oraz ram regulacyjnych łączących tę identyfikację z atrybutami i danymi uwierzytelniającymi na szczeblu UE. Jedynie w drodze interwencji na szczeblu UE można ustanowić zharmonizowane warunki, które zapewniają użytkownikom kontrolę nad transgranicznymi usługami cyfrowymi online i dostęp do nich, oraz ramy interoperacyjności, które ułatwią wykorzystywanie bezpiecznych rozwiązań w zakresie tożsamości cyfrowej w usługach online niezależnie od tego, gdzie w UE wydano dane rozwiązanie lub gdzie mieszka dany obywatel. Jak w dużej mierze wynika z przeglądu stosowania rozporządzenia eIDAS, jest mało prawdopodobne, by interwencja krajowa była równie efektywna i skuteczna.

- **Proporcjonalność**

Niniejsza inicjatywa jest proporcjonalna do zamierzonych celów i stanowi odpowiedni instrument służący ustanowieniu niezbędnej struktury interoperacyjności na potrzeby utworzenia unijnego ekosystemu tożsamości cyfrowej opartego na tożsamościach prawnych wydawanych przez państwa członkowskie oraz na dostarczaniu kwalifikowanych i niekwalifikowanych atrybutów tożsamości cyfrowej. Wnosi ona wyraźny wkład w osiągniecie celu, jakim jest poprawa jednolitego rynku cyfrowego dzięki bardziej zharmonizowanym ramom prawnym. Zharmonizowane europejskie portfele tożsamości cyfrowej, które państwa członkowskie mają wydawać na podstawie wspólnych norm technicznych, również stanowią wspólne podejście unijne przynoszące korzyści użytkownikom i stronom korzystającym z dostępności bezpiecznych rozwiązań transgranicznych w zakresie tożsamości elektronicznej. Niniejsza inicjatywa służy wyeliminowaniu ograniczeń obecnej infrastruktury interoperacyjności identyfikacji elektronicznej opartej na wzajemnym uznawaniu różnych krajowych systemów identyfikacji elektronicznej. Biorąc pod uwagę wyznaczone cele, uznaje się, że inicjatywa ta jest wystarczająco proporcjonalna, a jej koszty będą prawdopodobnie współmierne do potencjalnych korzyści. Proponowane rozporządzenie będzie wiązało się z kosztami finansowymi i administracyjnymi dla państw członkowskich jako wydawców europejskich portfeli tożsamości cyfrowej oraz dla dostawców usług zaufania i usług online. Nad kosztami tymi prawdopodobnie będą jednak przeważały znaczne potencjalne korzyści dla obywateli i użytkowników wynikające bezpośrednio z szerszego transgranicznego uznawania i akceptacji usług w zakresie tożsamości elektronicznej i atrybutów.

Kosztów związanych z tworzeniem nowych norm i dostosowywaniem się do nich dostawców usług zaufania i usług online nie można uniknąć, jeżeli ma zostać osiągnięty cel dotyczący używalności i dostępności. Inicjatywa ta ma na celu wykorzystanie inwestycji, które państwa członkowskie już poczyniły w ramach krajowych systemów tożsamości, i oparcie się na nich. Ponadto koszty dodatkowe wynikające z wniosku mają posłużyć wsparciu harmonizacji i są uzasadnione oczekiwaniem, że w dłuższej perspektywie doprowadzą do spadku obciążenia

administracyjnego i kosztów przestrzegania przepisów. Koszty związane z akceptacją atrybutów uwierzytelniania tożsamości cyfrowej w sektorach regulowanych również można uznać za konieczne i proporcjonalne, o ile przyczyniają się one do osiągnięcia ogólnego celu i stanowią środki, za których pomocą sektory regulowane mogą wypełniać zobowiązania prawne na potrzeby zgodnej z prawem identyfikacji użytkownika.

- **Wybór instrumentu**

Wybór rozporządzenia jako instrumentu prawnego jest uzasadniony potrzebą zapewnienia na rynku wewnętrznym jednolitych warunków stosowania europejskiej tożsamości cyfrowej za pomocą zharmonizowanych ram, których celem jest osiągnięcie niezakłóconej interoperacyjności oraz zapewnienie europejskim obywatelom i przedsiębiorstwom możliwości korzystania z usług publicznych i prywatnych w całej Unii przy użyciu wysoce bezpiecznych i wiarygodnych systemów identyfikacji elektronicznej.

3. WYNIKI OCEN *EX POST*, KONSULTACJI Z ZAINTERESOWANYMI STRONAMI I OCEN SKUTKÓW

- **Oceny *ex post*/oceny adekwatności obowiązującego prawodawstwa**

Ocenę funkcjonowania rozporządzenia eIDAS przeprowadzono w ramach procesu przeglądu wymaganego w art. 49 tego rozporządzenia. Z głównych ustaleń oceny w odniesieniu do tożsamości elektronicznej wynika, że nie wykorzystano pełnego potencjału rozporządzenia eIDAS. Notyfikowano jedynie ograniczoną liczbę systemów identyfikacji elektronicznej, co sprawia, że liczba obywateli Unii objętych notyfikowanymi systemami identyfikacji elektronicznej jest ograniczona do ok. 59 % ludności. Ponadto poziom akceptacji notyfikowanych systemów identyfikacji elektronicznej jest ograniczony zarówno na szczeblu państw członkowskich, jak i dostawców usług. Wydaje się również, że tylko nieliczne usługi dostępne za pośrednictwem krajowego systemu identyfikacji elektronicznej są połączone z krajową infrastrukturą eIDAS. W badaniu oceniającym stwierdzono również, że obecny zakres stosowania rozporządzenia eIDAS i główny jego przedmiot, czyli systemy identyfikacji elektronicznej notyfikowane przez państwa członkowskie UE i umożliwienie dostępu do usług publicznych online, są zbyt ograniczone i niewystarczające. Zdecydowana większość potrzeb w zakresie tożsamości elektronicznej i uwierzytelniania na odległość nadal występuje po stronie sektora prywatnego, w szczególności w obszarach takich jak: bankowość, telekomunikacja i obsługa platform, gdzie operatorzy zgodnie z prawem są zobowiązani do weryfikacji tożsamości klientów. Wartość dodana rozporządzenia eIDAS w odniesieniu do tożsamości elektronicznej jest ograniczona ze względu na jej mały zasięg oraz nieznaczne rozpowszechnienie i wykorzystanie.

Problemy wskazane w niniejszym wniosku są związane z niedociągnięciami obecnych ram eIDAS, a także z zasadniczymi zmianami kontekstowymi dotyczącymi rynków oraz rozwoju społecznego i technologicznego, wskutek których pojawiają się nowe potrzeby użytkowników i rynku.

- **Konsultacje z zainteresowanymi stronami**

Otwarte konsultacje publiczne rozpoczęto w dniu 24 lipca 2020 r., a zamknięto w dniu 2 października 2020 r. Komisja otrzymała łącznie 318 odpowiedzi. Komisja otrzymała również 106 odpowiedzi udzielonych w ukierunkowanym badaniu opinii zainteresowanych stron. Na różnych posiedzeniach dwustronnych i wielostronnych oraz w ramach badań organizowanych od początku 2020 r. zebrano również opinie państw członkowskich. Obejmuje to w szczególności badanie przeprowadzone w okresie lipiec–sierpień 2020 r. wśród

przedstawicieli państw członkowskich w sieci współpracy eIDAS oraz różne specjalne warsztaty. Komisja przeprowadziła również wywiady pogłębione z przedstawicielami branży i zorganizowała spotkania dwustronne z zainteresowanymi przedsiębiorcami z różnych sektorów (np. handlu elektronicznego, opieki zdrowotnej, usług finansowych, telekomunikacji, produkcji sprzętu itp.).

Zdecydowana większość respondentów uczestniczących w otwartych konsultacjach publicznych z zadowoleniem przyjęła utworzenie jednolitej i powszechnie akceptowanej tożsamości cyfrowej opartej na tożsamościach prawnych wydawanych przez państwa członkowskie. Państwa członkowskie w dużej mierze opowiadają się za potrzebą wzmocnienia obecnego rozporządzenia eIDAS w taki sposób, aby zapewnić obywatelom możliwość dostępu zarówno do usług publicznych, jak i prywatnych, oraz uznają potrzebę ustanowienia usługi zaufania umożliwiającej wydawanie elektronicznych poświadczeń atrybutów i transgraniczne korzystanie z nich. Ogólnie rzecz biorąc, państwa członkowskie podkreśliły potrzebę oparcia europejskich ram tożsamości cyfrowej na doświadczeniach wyniesionych z rozwiązań krajowych i na mocnych stronach tych rozwiązań, co ma na celu osiągnięcie synergii i czerpanie korzyści z poczynionych inwestycji. Wiele zainteresowanych stron wspomniało o tym, że pandemia COVID-19 uwidoczniła wartość bezpiecznej identyfikacji na odległość dla wszystkich osób w kontekście dostępu do usług publicznych i prywatnych. W kwestii usług zaufania większość podmiotów zgadza się, że obecne ramy stanowią sukces, jednak konieczne były pewne dodatkowe środki służące dalszej harmonizacji niektórych praktyk związanych z identyfikacją na odległość i nadzorem krajowym. Te zainteresowane strony, których baza klientów jest w dużej mierze krajowa, wyraziły większe wątpliwości co do wartości dodanej europejskich ram tożsamości cyfrowej.

W sektorze publicznym i prywatnym w coraz większym stopniu postrzega się portfele tożsamości cyfrowej jako najwłaściwszy instrument umożliwiający użytkownikom wybór, kiedy i któremu prywatnemu dostawcy usług będą udostępniać różne atrybuty w zależności od przypadku użycia i bezpieczeństwa potrzebnego w odniesieniu do danej transakcji. Za główny atut rozwiązania wytrzymującego próbę czasu uznano tożsamości cyfrowe oparte na cyfrowych portfelach przechowywanych w bezpieczny sposób na urządzeniach przenośnych. Zarówno rynek prywatny (np. Apple, Google, Thales), jak i rządy już zmierzają w tym kierunku.

- **Gromadzenie i wykorzystanie wiedzy eksperckiej**

Niniejszy wniosek opiera się na informacjach zebranych w ramach konsultacji z zainteresowanymi stronami do celów oceny skutków i sprawozdań oceniających na temat rozporządzenia eIDAS w świetle obowiązków w zakresie przeglądu określonych w art. 49 tego rozporządzenia. Zorganizowano liczne spotkania z przedstawicielami państw członkowskich i ekspertami.

- **Ocena skutków**

W odniesieniu do niniejszego wniosku przeprowadzono ocenę skutków. W dniu 19 marca 2021 r. Rada ds. Kontroli Regulacyjnej wydała opinię negatywną z pewnymi uwagami. Po przedłożeniu zmienionego wniosku w dniu 5 maja 2021 r. Rada wydała opinię pozytywną.

Komisja przeanalizowała różne warianty strategiczne mające na celu osiągnięcie ogólnego celu niniejszej inicjatywy, jakim jest zapewnienie należytego funkcjonowania rynku wewnętrznego, w szczególności pod względem dostarczania i stosowania wysoce bezpiecznych i wiarygodnych rozwiązań w zakresie tożsamości elektronicznej.

W ocenie skutków zbadano scenariusz odniesienia, warianty strategiczne oraz ich skutki dla trzech rozważanych wariantów strategicznych. Każdy wariant stanowi wybór do rozważenia z punktu widzenia polityki w zależności od poziomu ambicji. Pierwszy wariant odpowiada niskiemu poziomowi ambicji i obejmuje zestaw środków mających na celu głównie zwiększenie skuteczności i efektywności rozporządzenia eIDAS w jego obecnym kształcie. Pierwszy wariant przewiduje wprowadzenie obowiązku notyfikacji krajowych systemów identyfikacji elektronicznej i usprawnienie istniejących instrumentów dostępnych na potrzeby osiągnięcia wzajemnego uznawania, opiera się zatem na zaspokojeniu potrzeb obywateli w drodze wykorzystania dostępności różnych krajowych systemów identyfikacji elektronicznej, które mają stać się interoperacyjne.

Drugi wariant odzwierciedla średni poziom ambicji i ma na celu głównie rozszerzenie możliwości bezpiecznej wymiany danych związanych z tożsamością, co będzie stanowić uzupełnienie rządowych systemów identyfikacji elektronicznej i przyczyni się do obserwowanego obecnie przechodzenia na usługi w zakresie tożsamości oparte na atrybutach. Celem tego wariantu byłoby zaspokojenie zapotrzebowania użytkowników i utworzenie nowej kwalifikowanej usługi zaufania w celu dostarczania elektronicznych poświadczeń atrybutów powiązanych z zaufanymi źródłami i możliwych do egzekwowania w wymiarze transgranicznym. Rozszerzyłoby to zakres stosowania obecnego rozporządzenia eIDAS i umożliwiłoby uwzględnienie największej możliwej liczby przypadków użycia, które opierają się na weryfikacji atrybutów tożsamości powiązanych z osobą przy zapewnieniu wysokiego poziomu bezpieczeństwa.

Trzeci – preferowany – wariant odpowiada najwyższemu poziomowi ambicji i ma na celu uregulowanie dostarczania wysoce bezpiecznego osobistego portfela tożsamości cyfrowej wydawanego przez państwa członkowskie. Uznano, że preferowany wariant w najbardziej skuteczny sposób przyczyni się do osiągnięcia celów niniejszej inicjatywy. Aby w pełni osiągnąć cele polityki, preferowany wariant oparto na większości środków ocenionych w ramach wariantu pierwszego (korzystanie z tożsamości prawnych poświadczonych przez państwa członkowskie i dostępność wzajemnie uznawanych środków identyfikacji elektronicznej) oraz wariantu drugiego (elektroniczne poświadczenia atrybutów prawnie uznawane transgranicznie).

Jeżeli chodzi o ogólne ramy usług zaufania, poziom ambicji wymaga zestawu środków, które umożliwiają osiągnięcie celów polityki bez konieczności stosowania podejścia etapowego.

Nowa kwalifikowana usługa zaufania na potrzeby zarządzania urządzeniami do składania podpisów i pieczęci elektronicznych na odległość przyniosłaby znaczne korzyści pod względem bezpieczeństwa, jednolitości, pewności prawa i możliwości wyboru oferowanych konsumentom zarówno w związku z certyfikacją kwalifikowanych urządzeń do składania podpisu, jak i w odniesieniu do wymogów, które muszą spełniać kwalifikowani dostawcy usług zaufania zarządzający takimi urządzeniami. Nowe przepisy wzmocniłyby ogólne ramy regulacyjne i nadzorcze na potrzeby świadczenia usług zaufania.

Skutki wariantów strategicznych dla różnych kategorii zainteresowanych stron wyjaśniono szczegółowo w załączniku 3 do oceny skutków uzupełniającej niniejszą inicjatywę. Ocena ta ma zarówno charakter ilościowy, jak i jakościowy. Z badania przeprowadzonego na potrzeby oceny skutków wynika, że minimalne wymierne koszty można oszacować na ponad 3,2 mld EUR, ponieważ niektórych pozycji kosztów nie można określić ilościowo. Łączne wymierne korzyści oszacowano na 3,9–9,6 mld EUR. Jeżeli chodzi o szersze skutki gospodarcze, oczekuje się, że preferowany wariant będzie miał pozytywne skutki dla innowacji, handlu

międzynarodowego i konkurencyjności, przyczyni się do wzrostu gospodarczego oraz doprowadzi do dodatkowych inwestycji w rozwiązania w zakresie tożsamości cyfrowej. Oczekuje się na przykład, że dodatkowe inwestycje w wysokości 500 mln EUR, do których dojdzie w wyniku zmian legislacyjnych w ramach wariantu trzeciego, przyniosą po 10 latach korzyści o wartości 1 268 mln EUR (przy przyjęciu na poziomie 67 %).

Oczekuje się również, że preferowany wariant będzie miał pozytywne skutki dla zatrudnienia – w ciągu pięciu lat od wdrożenia przyczyni się do powstania 5 000–27 000 dodatkowych miejsc pracy. Będzie to efektem dodatkowych inwestycji i mniejszych kosztów dla przedsiębiorstw korzystających z rozwiązań w zakresie identyfikacji elektronicznej.

Oczekuje się, że pozytywne skutki dla środowiska będą największe w przypadku wariantu trzeciego, który ma w jak największym stopniu zwiększyć upowszechnienie i używalność identyfikacji elektronicznej, co będzie miało pozytywne skutki pod względem redukcji emisji związanych ze świadczeniem usług publicznych.

Rejestry elektroniczne zapewniają użytkownikom dowody i niezmienną ścieżkę audytu w odniesieniu do kolejności transakcji i zapisów danych, chroniąc integralność danych. Chociaż tej usługi zaufania nie uwzględniono w ocenie skutków, opiera się ona na istniejących usługach zaufania, ponieważ łączy znaczniki czasu danych i ich kolejność z pewnością w odniesieniu do twórcy danych, co stanowi rozwiązanie podobne do podpisu elektronicznego. Ta usługa zaufania jest niezbędna, by zapobiec fragmentacji rynku wewnętrznego dzięki określeniu jednolitych ogólnoeuropejskich ram umożliwiających transgraniczne uznawanie usług zaufania wykorzystywanych w prowadzeniu kwalifikowanych rejestrów elektronicznych. Integralność danych jest z kolei bardzo ważna dla łączenia danych ze źródeł zdecentralizowanych, dla rozwiązań w zakresie tożsamości opartych na autonomii jednostki, przypisywania własności do aktywów cyfrowych, rejestrowania procesów biznesowych na potrzeby kontroli zgodności z kryteriami zrównoważonego rozwoju oraz dla różnych przypadków użycia na rynkach kapitałowych.

- **Sprawność regulacyjna i uproszczenie**

W niniejszym wniosku ustanawia się środki, które będą miały zastosowanie do organów publicznych, obywateli i dostawców usług online. Zmniejszy to koszty administracyjne i koszty przestrzegania przepisów, które ponosi administracja publiczna, oraz koszty operacyjne i wydatki związane z bezpieczeństwem, które ponoszą dostawcy usług online. Obywatele odniosą korzyści w postaci oszczędności wynikających ze zmniejszenia obciążenia administracyjnego, gdyż będą mogli korzystać w pełni ze środków cyfrowych do celów identyfikacji oraz z możliwości bezpiecznej wymiany atrybutów tożsamości cyfrowej o takiej samej wartości prawnej w wymiarze transgranicznym. Dostawcy tożsamości elektronicznej również skorzystają na niższych kosztach przestrzegania przepisów.

- **Prawa podstawowe**

Ponieważ dane osobowe wchodzą w zakres stosowania niektórych elementów rozporządzenia, środki zaprojektowano w taki sposób, by były w pełni zgodne z przepisami o ochronie danych. We wniosku udoskonalono na przykład możliwości w zakresie udostępniania danych i umożliwiania uznaniowego ujawniania informacji. Za pomocą europejskiego portfela tożsamości cyfrowej użytkownik będzie mógł kontrolować ilość danych przekazywanych stronom ufającym i uzyskiwać informacje o atrybutach wymaganych do świadczenia konkretnej usługi. Dostawcy usług muszą informować państwa członkowskie o zamiarze stosowania europejskiego portfela tożsamości cyfrowej, co umożliwi państwom

członkowskim kontrolowanie, czy dostawcy usług wymagają zbiorów danych wrażliwych, na przykład dotyczących zdrowia, wyłącznie w zakresie zgodnym z prawem krajowym.

4. WPŁYW NA BUDŻET

Aby w optymalny sposób osiągnąć cele niniejszej inicjatywy, trzeba sfinansować szereg działań zarówno na poziomie Komisji, na którym przewiduje się przydział ok. 60 EPC w latach 2022–2027, jak i na poziomie państw członkowskich poprzez ich aktywne uczestnictwo w grupach ekspertów i komitetach powiązanych z pracami w ramach tej inicjatywy i składających się z przedstawicieli państw członkowskich. Łączne zasoby finansowe niezbędne do celów wdrożenia wniosku w latach 2022–2027 wyniosą do 30,825 mln EUR, z której to kwoty 8,825 mln EUR zostanie przeznaczone na koszty administracyjne, a do 22 mln EUR – na wydatki operacyjne objęte programem „Cyfrowa Europa" (do uzgodnienia). Finansowanie będzie przeznaczone na pokrycie kosztów związanych z utrzymaniem, opracowywaniem, hostingiem, obsługą i wspieraniem modułów identyfikacji elektronicznej i usług zaufania. Może być również przeznaczone na dotacje mające na celu łączenie usług z ekosystemem europejskiego portfela tożsamości cyfrowej oraz opracowanie norm i specyfikacji technicznych. Ponadto środki finansowe posłużą również sfinansowaniu corocznych badań i analiz dotyczących skuteczności i efektywności rozporządzenia w osiąganiu jego celów. Szczegółowy przegląd związanych z tym kosztów znajduje się w „ocenie skutków finansowych regulacji" związanej z niniejszą inicjatywą.

5. ELEMENTY FAKULTATYWNE

- **Plany wdrożenia i monitorowanie, ocena i sprawozdania**

Skutki będą monitorowane i oceniane zgodnie z wytycznymi dotyczącymi lepszego stanowienia prawa obejmującymi wdrażanie i stosowanie rozporządzenia, którego dotyczy niniejszy wniosek. Uzgodnienia w zakresie monitorowania stanowią istotną część wniosku, w szczególności w świetle niedociągnięć obecnych ram sprawozdawczości wskazanych w badaniu oceniającym. Oprócz wymogów dotyczących sprawozdawczości wprowadzonych w proponowanym rozporządzeniu, których celem jest zapewnienie lepszej bazy danych i analiz, ramy monitorowania będą obejmować następujące elementy: 1) zakres, w jakim niezbędne zmiany wdrożono zgodnie z przyjętymi środkami; 2) czy wprowadzono niezbędne zmiany w odpowiednich systemach krajowych; 3) czy stosowano się do niezbędnych zmian w zobowiązaniach w zakresie zgodności podmiotów objętych regulacją. Komisja Europejska (1, 2 i 3) oraz właściwe organy krajowe (2 i 3) będą odpowiedzialne za gromadzenie danych na podstawie uprzednio określonych wskaźników.

W kwestii stosowania proponowanego instrumentu Komisja Europejska i właściwe organy krajowe będą oceniać w drodze corocznych badań: 1) dostęp wszystkich obywateli Unii do środków identyfikacji elektronicznej; 2) zwiększone uznawanie i akceptację systemów identyfikacji elektronicznej w wymiarze transgranicznym; 3) środki zachęcające sektor prywatny do przyjęcia proponowanych rozwiązań i pobudzające rozwój nowych usług w zakresie tożsamości cyfrowej.

Komisja Europejska będzie w ramach corocznych badań gromadzić informacje kontekstowe na temat: 1) wielkość rynku tożsamości cyfrowych; 2) wydatków na zamówienia publiczne związanych z tożsamością cyfrową; 3) odsetka przedsiębiorstw świadczących usługi online; 4) odsetka transakcji online wymagających silnego uwierzytelnienia klienta; 5) odsetka obywateli Unii korzystających z usług prywatnych i publicznych online.

- **Szczegółowe objaśnienia poszczególnych przepisów wniosku**

W art. 6a projektu rozporządzenia zobowiązuje się państwa członkowskie do wydania w ramach notyfikowanego systemu identyfikacji elektronicznej europejskiego portfela tożsamości cyfrowej zgodnie ze wspólnymi normami technicznymi po przeprowadzeniu obowiązkowej oceny zgodności i dobrowolnej certyfikacji w europejskich ramach certyfikacji cyberbezpieczeństwa ustanowionych na mocy aktu o cyberbezpieczeństwie. Zawiera on przepisy zapewniające osobom fizycznym i prawnym możliwość bezpiecznego żądania i otrzymywania, przechowywania, łączenia i wykorzystywania danych identyfikujących osobę i elektronicznych poświadczeń atrybutów na potrzeby uwierzytelniania online i offline oraz umożliwienia dostępu do towarów i usług publicznych i prywatnych online pod kontrolą użytkownika. Certyfikacja ta nie narusza przepisów RODO w tym sensie, że operacje przetwarzania danych osobowych związane z europejskim portfelem tożsamości cyfrowej mogą być certyfikowane wyłącznie na podstawie art. 42 i 43 RODO.

Art. 6b wniosku zawiera przepisy szczegółowe dotyczące wymogów mających zastosowanie do stron ufających w celu zapobiegania oszustwom oraz zapewnienia uwierzytelniania danych identyfikujących osobę i elektronicznych poświadczeń atrybutów pochodzących z europejskiego portfela tożsamości cyfrowej.

Aby udostępnić więcej środków identyfikacji elektronicznej do użytku transgranicznego oraz zwiększyć skuteczność procesu wzajemnego uznawania notyfikowanych systemów identyfikacji elektronicznej, w art. 7 nałożono na państwa członkowskie obowiązek zgłoszenia co najmniej jednego systemu identyfikacji elektronicznej. Aby zapewnić niepowtarzalną i trwałą identyfikację osób fizycznych, w art. 11a dodano ponadto przepisy ułatwiające unikalną identyfikację. Dotyczy to przypadków, w których identyfikacja jest wymagana na mocy prawa, np. w obszarze zdrowia, w obszarze finansów, aby wywiązać się z obowiązków w zakresie przeciwdziałania praniu pieniędzy, lub do celów sądowych. W tym celu państwa członkowskie będą zobowiązane do włączenia do minimalnego zbioru danych identyfikujących osobę unikalnego i trwałego identyfikatora. Możliwość korzystania przez państwa członkowskie z certyfikacji w celu zapewnienia zgodności z rozporządzeniem, a tym samym zastąpienie procesu wzajemnej oceny, zwiększa skuteczność wzajemnego uznawania.

W sekcji 3 przedstawiono nowe przepisy dotyczące transgranicznego korzystania z europejskiego portfela tożsamości cyfrowej, aby zapewnić użytkownikom możliwości korzystania z tych portfeli w celu uzyskiwania dostępu do usług online świadczonych przez podmioty sektora publicznego i prywatnych dostawców usług, które to usługi wymagają silnego uwierzytelniania użytkownika.

W rozdziale III dotyczącym usług zaufania zmieniono art. 14 dotyczący aspektów międzynarodowych, aby umożliwić Komisji przyjmowanie decyzji wykonawczych potwierdzających równoważność wymogów mających zastosowanie do dostawców usług zaufania mających siedzibę w państwach trzecich i do świadczonych przez nich usług, poza korzystaniem z umów o wzajemnym uznawaniu zgodnie z art. 218 TFUE.

W odniesieniu do przepisów ogólnych mających zastosowanie do usług zaufania, w tym do kwalifikowanych dostawców usług zaufania, zmieniono art. 17, 18, 20, 21 i 24 w celu dostosowania ich do przepisów mających zastosowanie do bezpieczeństwa sieci i informacji w UE. Jeżeli chodzi o metody, które kwalifikowani dostawcy usług zaufania mają stosować na potrzeby weryfikacji tożsamości osób fizycznych lub prawnych, którym wydawane są kwalifikowane certyfikaty, zharmonizowano i doprecyzowano przepisy dotyczące korzystania ze środków identyfikacji na odległość, aby zapewnić stosowanie tych samych przepisów w całej UE.

W rozdziale III przedstawiono nowy art. 29a w celu określenia wymogów dotyczących kwalifikowanej usługi zarządzania urządzeniami do składania podpisu elektronicznego na odległość. Nowa kwalifikowana usługa zaufania będzie bezpośrednio powiązana ze środkami przywołanymi i ocenionymi w ocenie skutków oraz oparta na nich, w szczególności środkach dotyczących „harmonizacji procesu certyfikacji do celów składania podpisu elektronicznego na odległość" i innych środkach wymagających zharmonizowania przez państwa członkowskie praktyk nadzoru.

W celu zapewnienia użytkownikom możliwości zidentyfikowania, kto stoi za daną witryną internetową, zmieniono art. 45, aby zobowiązać dostawców przeglądarek internetowych do ułatwienia korzystania z kwalifikowanych certyfikatów uwierzytelniania witryn internetowych.

W rozdziale III przedstawiono trzy nowe sekcje.

Nową sekcją 9 wprowadzono przepisy dotyczące skutków prawnych elektronicznych poświadczeń atrybutów, ich stosowania w określonych sektorach oraz wymogów dotyczących kwalifikowanych poświadczeń atrybutów. W celu zapewnienia wysokiego poziomu zaufania w art. 45d dodano przepis dotyczący weryfikacji atrybutów w zestawieniu ze źródłami autentycznymi. Aby zapewnić użytkownikom europejskiego portfela tożsamości cyfrowej możliwość korzystania z dostępności elektronicznych poświadczeń atrybutów i otrzymywania takich poświadczeń w odniesieniu do tego portfela, w art. 45e dodano stosowny wymóg. Art. 45f zawiera natomiast dodatkowe przepisy w odniesieniu do świadczenia usług elektronicznego poświadczania atrybutów, w tym dotyczące ochrony danych osobowych.

Nowa sekcja 10 umożliwia świadczenie kwalifikowanych usług archiwizacji elektronicznej na szczeblu UE. Art. 45g dotyczący kwalifikowanych usług archiwizacji elektronicznej uzupełnia art. 34 i 40, które odnoszą się kwalifikowanych usług konserwacji kwalifikowanych podpisów elektronicznych i kwalifikowanych pieczęci elektronicznych.

W nowej sekcji 11 ustanowiono ramy usług zaufania w odniesieniu do tworzenia i prowadzenia rejestrów elektronicznych i kwalifikowanych rejestrów elektronicznych. Rejestr elektroniczny łączy stosowanie znaczników czasu danych i kolejności danych z pewnością co do twórcy danych, co stanowi rozwiązanie podobne do podpisu elektronicznego, przy czym dodatkową korzyścią wynikającą z rejestru jest umożliwienie bardziej zdecentralizowanego zarządzania, które jest odpowiednie dla współpracy wielostronnej. Jest to ważne w przypadku różnych przypadków użycia, które mogą być oparte na rejestrach elektronicznych.

Rejestry elektroniczne pomagają przedsiębiorstwom osiągnąć oszczędności kosztów dzięki zwiększeniu skuteczności i bezpieczeństwa koordynacji wielostronnej, a także ułatwiają nadzór regulacyjny. Wobec braku europejskich uregulowań istnieje ryzyko, że ustawodawcy krajowi ustanowią rozbieżne normy krajowe. Aby zapobiec fragmentacji, konieczne jest określenie jednolitych ogólnoeuropejskich ram umożliwiających transgraniczne uznawanie usług zaufania wykorzystywanych w prowadzeniu rejestrów elektronicznych. Ta ogólnoeuropejska norma dotycząca operatorów węzłów będzie miała zastosowanie niezależnie od innych przepisów prawa wtórnego UE. W przypadku gdy rejestry elektroniczne wykorzystuje się w obsłudze emisji obligacji lub obrotu nimi, lub na potrzeby kryptoaktywów, przypadki użycia powinny być zgodne z wszystkimi mającymi zastosowanie

przepisami finansowymi, np. z dyrektywą w sprawie rynków instrumentów finansowych[11], dyrektywą w sprawie usług płatniczych[12] i przyszłym rozporządzeniem w sprawie rynków kryptoaktywów[13]. Jeżeli przypadki użycia dotyczą danych osobowych, dostawcy usług będą musieli przestrzegać RODO.

W 2017 r. 75 % wszystkich przypadków użycia rejestrów elektronicznych dotyczyło bankowości i finansów. Przypadki użycia rejestrów elektronicznych są obecnie coraz bardziej zróżnicowane: 17 % dotyczy obszaru komunikacji i mediów; 15 % – produkcji i zasobów naturalnych, 10 % – sektora rządowego, 8 % – ubezpieczeń, 5 % – handlu detalicznego, 6 % – transportu, 5 % – usług użyteczności publicznej[14].

Ponadto w rozdziale VI wprowadzono nowy art. 48b, aby zapewnić gromadzenie danych statystycznych dotyczących korzystania z europejskiego portfela tożsamości cyfrowej na potrzeby monitorowania skuteczności zmienionego rozporządzenia.

---

11 Dyrektywa Parlamentu Europejskiego i Rady 2014/65/UE z dnia 15 maja 2014 r. w sprawie rynków instrumentów finansowych oraz zmieniająca dyrektywę 2002/92/WE i dyrektywę 2011/61/UE (tekst mający znaczenie dla EOG), *Dz.U. L 173 z 12.6.2014, s. 349*.

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

13 Wniosek dotyczący rozporządzenia Parlamentu Europejskiego i Rady w sprawie rynków kryptoaktywów i zmieniającego dyrektywę (UE) 2019/1937, COM(2020) 593 final.

14 Gartner, Blockchain Evolution [Ewolucja łańcucha bloków], 2020 r.

2021/0136 (COD)

Wniosek

ROZPORZĄDZENIE PARLAMENTU EUROPEJSKIEGO I RADY

zmieniające rozporządzenie (UE) nr 910/2014 w odniesieniu do ustanowienia europejskich ram tożsamości cyfrowej

PARLAMENT EUROPEJSKI I RADA UNII EUROPEJSKIEJ,

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

uwzględniając wniosek Komisji Europejskiej,

po przekazaniu projektu aktu ustawodawczego parlamentom narodowym,

uwzględniając opinię Europejskiego Komitetu Ekonomiczno-Społecznego[15],

stanowiąc zgodnie ze zwykłą procedurą ustawodawczą,

a także mając na uwadze, co następuje:

(1) W komunikacie Komisji z dnia 19 lutego 2020 r. pt. „Kształtowanie cyfrowej przyszłości Europy”[16] zapowiedziano przegląd rozporządzenia Parlamentu Europejskiego i Rady (UE) nr 910/2014 w celu zwiększenia jego skuteczności, zwiększenia korzyści dla sektora prywatnego i promowania wiarygodnych tożsamości cyfrowych dla wszystkich Europejczyków.

(2) W konkluzjach z dni 1–2 października 2020 r.[17] Rada Europejska wezwała Komisję do przedstawienia wniosku w sprawie opracowania ogólnounijnych ram bezpiecznej publicznej identyfikacji elektronicznej, w tym interoperacyjnych podpisów cyfrowych, by zapewnić ludziom kontrolę nad ich tożsamością i danymi w internecie, a także by umożliwić dostęp do publicznych, prywatnych i transgranicznych usług cyfrowych.

(3) W komunikacie Komisji z dnia 9 marca 2021 r. pt. „Cyfrowy kompas na 2030 r.: europejska droga w cyfrowej dekadzie”[18] wyznaczono cel ram Unii, zgodnie z którym do 2030 r. powinny one zapewnić wprowadzenie na szeroką skalę zaufanej, kontrolowanej przez użytkownika tożsamości, dzięki której każdy obywatel będzie mógł kontrolować swoje kontakty i obecność online.

(4) Bardziej zharmonizowane podejście do identyfikacji cyfrowej powinno ograniczyć ryzyko i koszty wynikające z obecnej fragmentacji, która spowodowana jest stosowaniem rozbieżnych rozwiązań krajowych, oraz wzmocni jednolity rynek poprzez umożliwienie obywatelom, innym rezydentom określonym w prawie krajowym i przedsiębiorstwom identyfikacji online w dogodny i jednolity sposób w całej Unii. Każdy powinien mieć możliwość bezpiecznego dostępu do usług publicznych i prywatnych za pomocą ulepszonego ekosystemu usług zaufania oraz

---

15 Dz.U. C […] z […], s. […].

16 COM(2020) 67 final.

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

18 COM(2021) 118 final.

zweryfikowanych dowodów potwierdzających tożsamość i poświadczeń atrybutów takich jak dyplom ukończenia studiów wyższych prawnie uznawany i akceptowany w całej Unii. Ramy europejskiej tożsamości cyfrowej mają na celu przejście od polegania wyłącznie na krajowych rozwiązaniach w zakresie tożsamości cyfrowej do dostarczania elektronicznych poświadczeń atrybutów ważnych na szczeblu europejskim. Dostawcy elektronicznych poświadczeń atrybutów powinni odnieść korzyści dzięki jasnemu i jednolitemu zestawowi przepisów, a administracje publiczne powinny mieć możliwość polegania na dokumentach elektronicznych w określonym formacie.

(5) Aby wspierać konkurencyjność europejskich przedsiębiorstw, dostawcy usług online powinni móc polegać na rozwiązaniach w zakresie tożsamości cyfrowej uznawanych w całej Unii, niezależnie od państwa członkowskiego, w którym zostały wydane, a tym samym czerpać korzyści ze zharmonizowanego europejskiego podejścia do zaufania, bezpieczeństwa i interoperacyjności. Zarówno użytkownicy, jak i dostawcy usług powinni mieć możliwość korzystania z przyznania elektronicznym poświadczeniom atrybutów takiej samej wartości prawnej w całej UE.

(6) W ramach wdrażania niniejszego rozporządzenia do przetwarzania danych osobowych ma zastosowanie rozporządzenie (UE) 2016/679[19]. W związku z tym w niniejszym rozporządzeniu należy ustanowić określone zabezpieczenia uniemożliwiające dostawcom środków identyfikacji elektronicznej i elektronicznego poświadczenia atrybutów łączenie danych osobowych pochodzących z innych usług z danymi osobowymi dotyczącymi usług objętych zakresem stosowania niniejszego rozporządzenia.

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

(8) W celu zapewnienia zgodności z prawem Unii lub prawem krajowym zgodnym z prawem Unii dostawcy usług powinni informować państwa członkowskie o zamiarze polegania na europejskich portfelach tożsamości cyfrowej. Pozwoli to państwom członkowskim chronić użytkowników przed oszustwami i zapobiegać nielegalnemu wykorzystywaniu danych dotyczących tożsamości i elektronicznych poświadczeń atrybutów, a także zapewnić, aby przetwarzanie danych wrażliwych, takich jak dane dotyczące zdrowia, mogło być weryfikowane przez strony ufające zgodnie z prawem Unii lub prawem krajowym.

(9) Wszystkie europejskie portfele tożsamości cyfrowej powinny umożliwiać użytkownikom elektroniczną identyfikację i uwierzytelnianie online i offline

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

w kontekście transgranicznym na potrzeby dostępu do szerokiego zakresu usług publicznych i prywatnych. Bez uszczerbku dla prerogatyw państw członkowskich w zakresie identyfikacji ich obywateli i rezydentów, portfele mogą również zaspokajać potrzeby instytucjonalne administracji publicznych, organizacji międzynarodowych oraz instytucji, organów i jednostek organizacyjnych Unii. Korzystanie z portfeli offline byłoby ważne w wielu sektorach, w tym w sektorze opieki zdrowotnej, w którym usługi są często świadczone w ramach kontaktu osobistego, a w przypadku recept elektronicznych powinna istnieć możliwość stosowania kodów QR lub podobnych technologii do weryfikacji autentyczności. W opartych na „wysokim" poziomie bezpieczeństwa europejskich portfelach tożsamości cyfrowej należy wykorzystać potencjał, jaki oferują rozwiązania odporne na ingerencję, takie jak zabezpieczenia, by zapewnić zgodność z wymogami bezpieczeństwa określonymi w niniejszym rozporządzeniu. Europejskie portfele tożsamości cyfrowej powinny również umożliwiać użytkownikom tworzenie i używanie kwalifikowanych podpisów i pieczęci elektronicznych akceptowanych w całej UE. Aby zapewnić obywatelom i przedsiębiorstwom w całej UE korzyści w zakresie uproszczenia przepisów i zmniejszenia kosztów, w tym poprzez umożliwienie korzystania z uprawnień do reprezentowania i zgód elektronicznych, państwa członkowskie powinny wydawać europejskie portfele tożsamości cyfrowej oparte na wspólnych normach, aby zapewnić niezakłóconą interoperacyjność i wysoki poziom bezpieczeństwa. Wyłącznie właściwe organy państw członkowskich mogą zapewnić wysoki stopień pewności przy ustalaniu tożsamości danej osoby, gwarantując tym samym, że osoba podająca daną tożsamość jest faktycznie osobą, za którą się podaje. Europejskie portfele tożsamości cyfrowej muszą być zatem oparte się na tożsamości prawnej obywateli, innych rezydentów lub osób prawnych. Zaufanie do europejskich portfeli tożsamości cyfrowej ulegnie zwiększeniu ze względu na fakt, że podmioty je wydające są zobowiązane do wdrożenia odpowiednich środków technicznych i organizacyjnych w celu zapewnienia poziomu bezpieczeństwa współmiernego do stwarzanego ryzyka dla praw i wolności osób fizycznych zgodnie z rozporządzeniem (UE) 2016/679.

(10) W celu osiągnięcia wysokiego poziomu bezpieczeństwa i wiarygodności w niniejszym rozporządzeniu ustanowiono wymogi dotyczące europejskich portfeli tożsamości cyfrowej. Zgodność europejskich portfeli tożsamości cyfrowej z tymi wymogami powinna być certyfikowana przez akredytowane podmioty sektora publicznego lub prywatnego wyznaczone przez państwa członkowskie. Poleganie na systemie certyfikacji opartym na dostępności norm wspólnie uzgodnionych z państwami członkowskimi powinno zapewnić wysoki poziom zaufania i interoperacyjności. Certyfikacja powinna w szczególności opierać się na odpowiednich europejskich programach certyfikacji cyberbezpieczeństwa ustanowionych na podstawie rozporządzenia (UE) 2019/881[20]. Certyfikacja taka powinna pozostawać bez uszczerbku dla certyfikacji w odniesieniu do przetwarzania danych osobowych na podstawie rozporządzenia (UE) 2016/679.

(11) Europejskie portfele tożsamości cyfrowej powinny zapewniać najwyższy poziom bezpieczeństwa danych osobowych wykorzystywanych do uwierzytelniania

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

niezależnie od tego, czy dane te są przechowywane lokalnie, czy przy użyciu rozwiązań opartych na chmurze, z uwzględnieniem różnych poziomów ryzyka. Wykorzystywanie danych biometrycznych do uwierzytelniania jest jedną z metod identyfikacji zapewniających wysoki poziom pewności, zwłaszcza w połączeniu z innymi elementami uwierzytelniania. Ponieważ dane biometryczne dotyczą unikalnych cech danej osoby, korzystanie z tych danych wymaga środków organizacyjnych i środków bezpieczeństwa współmiernych do ryzyka, jakie takie przetwarzanie może stwarzać dla praw i wolności osób fizycznych, oraz musi być zgodne z rozporządzeniem (UE) 2016/679.

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

(13) Rozporządzenie (UE) 2019/1157[21] zwiększa bezpieczeństwo dowodów osobistych z ulepszonymi zabezpieczeniami do sierpnia 2021 r. Państwa członkowskie powinny rozważyć możliwość notyfikowania tych dowodów w ramach systemów identyfikacji elektronicznej, aby zwiększyć transgraniczną dostępność środków identyfikacji elektronicznej.

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

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

(16) Państwa członkowskie powinny odnieść korzyści dzięki nowym, elastycznym narzędziom służącym do zapewniania zgodności z wymogami niniejszego rozporządzenia i odpowiednich aktów wykonawczych. Niniejsze rozporządzenie powinno umożliwiać państwom członkowskim korzystanie ze sprawozdań i ocen sporządzonych przez akredytowane jednostki oceniające zgodność lub z dobrowolnych programów certyfikacji bezpieczeństwa ICT, takich jak programy

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

certyfikacji, które mają zostać ustanowione na szczeblu Unii na podstawie rozporządzenia (UE) 2019/881, do celów poparcia twierdzeń dotyczących dostosowania programów lub ich części do wymogów rozporządzenia w zakresie interoperacyjności i bezpieczeństwa notyfikowanych systemów identyfikacji elektronicznej.

(17) Dostawcy usług wykorzystują dane dotyczące tożsamości dostarczone przez zbiór danych identyfikujących osobę dostępnych w ramach systemów identyfikacji elektronicznej na podstawie rozporządzenia (UE) nr 910/2014, aby dopasować użytkownika z innego państwa członkowskiego do tożsamości prawnej danego użytkownika. Pomimo korzystania ze zbioru danych eIDAS w wielu przypadkach zapewnienie dokładnego dopasowania wymaga jednak dodatkowych informacji na temat użytkownika oraz określonych procedur unikalnej identyfikacji na szczeblu krajowym. W celu dalszego wspomagania używalności środków identyfikacji elektronicznej w niniejszym rozporządzeniu należy zobowiązać państwa członkowskie do wprowadzenia konkretnych środków służących zapewnieniu prawidłowego dopasowania tożsamości w procesie identyfikacji elektronicznej. W tym samym celu w niniejszym rozporządzeniu należy również rozszerzyć obowiązkowy minimalny zbiór danych i wprowadzić wymóg stosowania unikalnego i trwałego identyfikatora elektronicznego zgodnego z prawem Unii w przypadkach, w których konieczna jest zgodna z prawem unikalna i trwała identyfikacja użytkownika na jego żądanie.

(18) Zgodnie z dyrektywą (UE) 2019/882[22] osoby z niepełnosprawnościami powinny mieć możliwość korzystania z europejskich portfeli tożsamości cyfrowej, usług zaufania i produktów przeznaczonych dla użytkownika końcowego stosowanych do świadczenia tych usług na równi z innymi użytkownikami.

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

(20) Świadczenie usług zaufania i korzystanie z nich staje się coraz ważniejsze dla handlu międzynarodowego i współpracy międzynarodowej. Partnerzy międzynarodowi UE tworzą ramy zaufania oparte na rozporządzeniu (UE) nr 910/2014. Aby w związku z tym ułatwić uznawanie takich usług i ich dostawców, w przepisach wykonawczych można określić warunki, na których ramy zaufania państw trzecich można uznać za równoważne określonym w niniejszym rozporządzeniu ramom zaufania dotyczącym kwalifikowanych usług zaufania i kwalifikowanych dostawców tych usług, jako uzupełnienie możliwości wzajemnego uznawania usług zaufania i dostawców tych usług mających siedzibę w Unii i w państwach trzecich zgodnie z art. 218 Traktatu.

(21) Niniejsze rozporządzenie powinno opierać się na aktach Unii zapewniających kontestowalne i uczciwe rynki w sektorze cyfrowym. Jest ono oparte w szczególności na rozporządzeniu (UE) XXX/XXXX [akt o rynkach cyfrowych], w którym wprowadza się przepisy dotyczące dostawców podstawowych usług platformowych wyznaczonych jako strażnicy dostępu, a także m.in. zakazuje się strażnikom dostępu nakładania na użytkowników biznesowych obowiązku korzystania z usługi

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

identyfikacyjnej świadczonej przez strażnika dostępu w kontekście usług oferowanych przez użytkowników biznesowych za pośrednictwem podstawowych usług platformowych tego strażnika dostępu, jak również obowiązku oferowania takiej usługi identyfikacyjnej lub współdziałania z taką usługą. W art. 6 ust. 1 lit. f) rozporządzenia (UE) XXX/XXXX [akt o rynkach cyfrowych] zobowiązuje się strażników dostępu, aby zapewniali użytkownikom biznesowym i dostawcom usług pomocniczych możliwość uzyskania dostępu do tego samego systemu operacyjnego, sprzętu lub funkcji oprogramowania, które są dostępne dla strażnika dostępu lub wykorzystywane przez niego do świadczenia dowolnych usług pomocniczych, oraz gwarantowali interoperacyjność wspomnianych systemu operacyjnego, sprzętu lub funkcji oprogramowania. Zgodnie z art. 2 pkt 15 [aktu o rynkach cyfrowych] usługi identyfikacyjne stanowią rodzaj usług pomocniczych. Użytkownicy biznesowi i dostawcy usług pomocniczych powinni zatem mieć możliwość dostępu do takiego sprzętu lub oprogramowania, np. zabezpieczeń smartfonów, oraz współdziałać z nimi za pośrednictwem europejskich portfeli tożsamości cyfrowej lub notyfikowanych przez państwa członkowskie środków identyfikacji elektronicznej.

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

(23) Należy zwrócić należytą uwagę na zapewnienie skutecznej współpracy między organami ds. bezpieczeństwa sieci i informacji a organami ds. eIDAS. W przypadkach, w których organ nadzoru na podstawie niniejszego rozporządzenia jest inny niż właściwe organy wyznaczone na podstawie dyrektywy (UE) XXXX/XXXX [dyrektywy NIS 2], organy te powinny ściśle i terminowo współpracować poprzez wymianę odpowiednich informacji, aby zapewnić skuteczny nadzór nad dostawcami usług zaufania i przestrzegania przez tych dostawców wymogów określonych w niniejszym rozporządzeniu i dyrektywie (UE)

XXXX/XXXX [dyrektywie NIS 2]. Organy nadzoru określone w niniejszym rozporządzeniu powinny być w szczególności uprawnione do zwracania się do właściwego organu określonego w dyrektywie (UE) XXXXX/XXXX [dyrektywie NIS 2] o udzielenie odpowiednich informacji potrzebnych do przyznania statusu kwalifikowanego oraz do przeprowadzenia działań nadzorczych w celu zweryfikowania zgodności dostawców usług zaufania z odpowiednimi wymogami określonymi w dyrektywie NIS 2 lub zażądania od tych dostawców, by zaradzili niezgodności.

(24) Istotne jest ustanowienie ram prawnych służących ułatwieniu transgranicznego uznawania między istniejącymi krajowymi systemami prawnymi, związanego z usługami rejestrowanego doręczenia elektronicznego. Ramy te mogłyby stworzyć także nowe możliwości rynkowe dla unijnych dostawców usług zaufania w odniesieniu do oferowania nowych ogólnoeuropejskich usług rejestrowanego doręczenia elektronicznego oraz zapewnić identyfikację odbiorców z wyższym poziomem pewności niż identyfikacja nadawcy.

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

(26) Powinna istnieć możliwość wydawania i obsługi wiarygodnych atrybutów cyfrowych oraz przyczynienia się do zmniejszenia obciążenia administracyjnego dzięki umożliwieniu obywatelom i innym rezydentom korzystania z tych atrybutów w transakcjach prywatnych i publicznych. Obywatele i inni rezydenci powinni móc na przykład wykazać posiadanie ważnego prawa jazdy wydanego przez organ w jednym państwie członkowskim, który to dokument właściwe organy w innych państwach członkowskich mogą zweryfikować i na którym mogą polegać, oraz powinni móc korzystać ze swoich danych uwierzytelniających dotyczących zabezpieczenia społecznego lub z przyszłych cyfrowych dokumentów podróży w kontekście transgranicznym.

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

(28) Do szerokiej dostępności i używalności europejskich portfeli tożsamości cyfrowej wymagana jest ich akceptacja przez prywatnych dostawców usług. Prywatne strony ufające świadczące usługi w obszarach transportu, energetyki, bankowości i usług

finansowych, zabezpieczenia społecznego, zdrowia, wody pitnej, usług pocztowych, infrastruktury cyfrowej, edukacji lub telekomunikacji powinny akceptować korzystanie z europejskich portfeli tożsamości cyfrowej na potrzeby świadczenia usług, w przypadku gdy silne uwierzytelnienie użytkownika do celów identyfikacji w usługach online jest wymagane na mocy prawa krajowego lub unijnego lub na podstawie zobowiązania umownego. W przypadku gdy bardzo duże platformy internetowe zdefiniowane w art. 25 ust. 1 rozporządzenia [odniesienie do rozporządzenia w sprawie aktu o usługach cyfrowych] wymagają uwierzytelniania użytkowników do celów dostępu do usług online, platformy te powinny być zobowiązane do akceptowania wykorzystywania europejskich portfeli tożsamości cyfrowej na podstawie dobrowolnego wniosku użytkownika. Użytkownicy nie powinni być zobowiązani do korzystania z portfela do celów dostępu do usług prywatnych, ale jeżeli sobie tego życzą, duże platformy internetowe powinny akceptować w tym celu europejski portfel tożsamości cyfrowej przy jednoczesnym poszanowaniu zasady minimalizacji danych. Biorąc pod uwagę znaczenie bardzo dużych platform internetowych ze względu na ich zasięg, w szczególności wyrażony liczbą odbiorców usługi i transakcji finansowych, jest to konieczne, aby zwiększyć ochronę użytkowników przed oszustwami i zapewnić wysoki poziom ochrony danych. Aby przyczynić się do zapewnienia szerokiej dostępności i używalności środków identyfikacji elektronicznej, w tym europejskich portfeli tożsamości cyfrowej objętych zakresem niniejszego rozporządzenia, należy opracować samoregulacyjne kodeksy postępowania na szczeblu Unii („kodeksy postępowania”). Kodeksy postępowania powinny ułatwiać szeroką akceptację środków identyfikacji elektronicznej, w tym europejskich portfeli tożsamości cyfrowej, przez tych dostawców usług, którzy nie kwalifikują się jako bardzo duże platformy i którzy do celów uwierzytelniania użytkownika korzystają z usług identyfikacji elektronicznej świadczonych przez strony trzecie. Kodeksy te należy opracować w terminie 12 miesięcy od przyjęcia niniejszego rozporządzenia. Komisja powinna ocenić skuteczność tych postanowień pod względem dostępności i używalności dla użytkowników europejskich portfeli tożsamości cyfrowej po 18 miesiącach od ich wdrożenia oraz dokonać przeglądu postanowień w celu zapewnienia ich akceptacji w drodze aktów delegowanych przyjętych w świetle tej oceny.

(29) Europejski portfel tożsamości cyfrowej powinien pod względem technicznym umożliwiać selektywne ujawnianie atrybutów stronom ufającym. Funkcja ta powinna stać się podstawową cechą projektową, co zwiększy wygodę i ochronę danych osobowych, w tym jeżeli chodzi o minimalizację przetwarzania danych osobowych.

(30) Atrybuty dostarczane przez kwalifikowanych dostawców usług zaufania w ramach kwalifikowanego poświadczania atrybutów powinny być weryfikowane w zestawieniu ze źródłami autentycznymi bezpośrednio przez kwalifikowanego dostawcę usług zaufania albo przez wyznaczonych pośredników uznanych na poziomie krajowym zgodnie z prawem krajowym lub prawem Unii do celów bezpiecznej wymiany poświadczonych atrybutów między dostawcami usług w zakresie tożsamości lub poświadczania atrybutów a stronami ufającymi.

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

odpowiedniego zachowania wynikających z przepisów dotyczących ochrony inwestorów lub do spełnienia wymogów silnego uwierzytelniania klienta w odniesieniu do logowania do rachunku i inicjowania transakcji w dziedzinie usług płatniczych.

(32) Usługi uwierzytelniania witryn internetowych dają użytkownikom pewność, że za daną witryną internetową stoi prawdziwy i prawowity podmiot. Usługi te przyczyniają się do budowy zaufania do prowadzenia działalności gospodarczej online, ponieważ użytkownicy będą mieli zaufanie do witryny internetowej, która została uwierzytelniona. Korzystanie przez witryny internetowe z usług uwierzytelniania witryn internetowych jest dobrowolne. Aby uwierzytelnianie witryny internetowej stało się środkiem zwiększającym zaufanie, zapewniającym użytkownikowi lepsze doświadczenie i wspierającym wzrost na rynku wewnętrznym, niniejsze rozporządzenie określa jednak minimalne obowiązki w zakresie bezpieczeństwa i odpowiedzialności dla dostawców usług uwierzytelniania witryn internetowych i dla tych usług. W tym celu przeglądarki internetowe powinny zapewniać obsługę kwalifikowanych certyfikatów uwierzytelniania witryn internetowych na podstawie rozporządzenia (UE) nr 910/2014 i interoperacyjność z tymi certyfikatami. Przeglądarki powinny uznawać i wyświetlać kwalifikowane certyfikaty uwierzytelniania witryn internetowych, aby zapewnić wysoki poziom bezpieczeństwa, umożliwiając właścicielom witryn internetowych potwierdzenie swojej tożsamości jako właścicieli, a użytkownikom – identyfikację właścicieli witryn internetowych z wysokim stopniem pewności. Aby szerzej propagować korzystanie z kwalifikowanych certyfikatów uwierzytelniania witryn internetowych, organy publiczne w państwach członkowskich powinny rozważyć włączenie tych certyfikatów do swoich witryn internetowych.

(33) Wiele państw członkowskich wprowadziło krajowe wymogi dotyczące usług zapewniających bezpieczną i wiarygodną archiwizację cyfrową, aby umożliwić długoterminową konserwację dokumentów elektronicznych i powiązanych usług zaufania. Do zapewnienia pewności prawa i zaufania konieczne jest ustanowienie ram prawnych ułatwiających transgraniczne uznawanie kwalifikowanych usług archiwizacji elektronicznej. Ramy te mogłyby stworzyć także nowe możliwości rynkowe dla unijnych dostawców usług zaufania.

(34) W kwalifikowanych rejestrach elektronicznych zapisuje się dane w sposób zapewniający unikalność, autentyczność i prawidłową kolejność zapisów danych oraz odporny na ingerencję. Rejestr elektroniczny łączy efekt stosowania znaczników czasu danych z pewnością co do twórcy danych, co stanowi rozwiązanie podobne do podpisu elektronicznego, przy czym dodatkową korzyścią wynikającą z rejestru jest umożliwienie modeli bardziej zdecentralizowanego zarządzania, które są odpowiednie dla współpracy wielostronnej. Rejestr elektroniczny tworzy na przykład wiarygodną ścieżkę audytu w odniesieniu do pochodzenia towarów w handlu transgranicznym, wspiera ochronę praw własności intelektualnej, umożliwia elastyczność rynków energii elektrycznej, stanowi podstawę zaawansowanych rozwiązań w zakresie tożsamości opartych na autonomii jednostki oraz wspomaga skuteczniejsze usługi publiczne w większym stopniu przyczyniające się do transformacji. Aby zapobiec fragmentacji rynku wewnętrznego, należy określić ogólnoeuropejskie ramy prawne umożliwiające transgraniczne uznawanie usług zaufania do celów zapisywania danych w rejestrach elektronicznych.

(35) Certyfikacja w charakterze kwalifikowanych dostawców usług zaufania powinna zapewniać pewność prawa w odniesieniu do przypadków użycia, które opierają się na

rejestrach elektronicznych. Ta usługa zaufania do celów rejestrów elektronicznych i kwalifikowanych rejestrów elektronicznych oraz certyfikacja w charakterze kwalifikowanego dostawcy usług zaufania w odniesieniu do rejestrów elektronicznych powinny obowiązywać niezależnie od wymogu, by przypadki użycia były zgodne z prawem Unii lub prawem krajowym zgodnym z prawem Unii. Przypadki użycia związane z przetwarzaniem danych osobowych muszą być zgodne z rozporządzeniem (UE) 2016/679. Przypadki użycia związane z kryptoaktywami powinny być zgodne ze wszystkimi mającymi zastosowanie przepisami finansowymi, np. z dyrektywą w sprawie rynków instrumentów finansowych[23], dyrektywą w sprawie usług płatniczych[24] i przyszłym rozporządzeniem w sprawie rynków kryptoaktywów[25].

(36) Aby uniknąć fragmentacji i barier wynikających z rozbieżnych norm i ograniczeń technicznych oraz aby zapewnić skoordynowany proces mający na celu wyeliminowanie zagrożeń dla wdrożenia przyszłych europejskich ram tożsamości cyfrowej, potrzebne są ramy bliskiej i zorganizowanej współpracy między Komisją, państwami członkowskimi i sektorem prywatnym. Aby osiągnąć ten cel, państwa członkowskie powinny współpracować w obrębie ram określonych w zaleceniu Komisji (UE) XXX/XXXX [zestaw narzędzi na potrzeby skoordynowanego podejścia do europejskich ram tożsamości cyfrowej][26] nad sformułowaniem zestawu narzędzi na potrzeby europejskich ram tożsamości cyfrowej. Zestaw narzędzi powinien zawierać kompleksową architekturę techniczną i ramy odniesienia, zestaw wspólnych norm i technicznych dokumentów referencyjnych oraz zestaw wytycznych i opisów najlepszych praktyk obejmujące co najmniej wszystkie aspekty funkcji i interoperacyjności europejskich portfeli tożsamości cyfrowej, w tym podpisów elektronicznych, oraz kwalifikowanej usługi zaufania służącej poświadczaniu atrybutów, które to rozwiązania określono w niniejszym rozporządzeniu. W tym kontekście państwa członkowskie powinny również osiągnąć porozumienie w sprawie wspólnych elementów modelu biznesowego i struktury opłat europejskich portfeli tożsamości cyfrowej, aby ułatwić korzystanie z tych portfeli, w szczególności przez małe i średnie przedsiębiorstwa w kontekście transgranicznym. Zawartość zestawu narzędzi powinna ewoluować równolegle z postępami w dialogu i procesie przyjmowania europejskich ram tożsamości cyfrowej oraz powinna odzwierciedlać ich wyniki.

(37) Na podstawie art. 42 ust. 1 rozporządzenia Parlamentu Europejskiego i Rady (UE) 2018/1525 zasięgnięto opinii Europejskiego Inspektora Ochrony Danych[27].

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

---

23 Dyrektywa Parlamentu Europejskiego i Rady 2014/65/UE z dnia 15 maja 2014 r. w sprawie rynków instrumentów finansowych oraz zmieniająca dyrektywę 2002/92/WE i dyrektywę 2011/61/UE (tekst mający znaczenie dla EOG), *Dz.U. L 173 z 12.6.2014, s. 349*.

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

25 Wniosek dotyczący rozporządzenia Parlamentu Europejskiego i Rady w sprawie rynków kryptoaktywów i zmieniającego dyrektywę (UE) 2019/1937, COM(2020) 593 final.

26 [po przyjęciu wstawić odesłanie]

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

PRZYJMUJĄ NINIEJSZE ROZPORZĄDZENIE:

Artykuł 1

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

1) art. 1 otrzymuje brzmienie:

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

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

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

c) ustanawia ramy prawne dla podpisów elektronicznych, pieczęci elektronicznych, elektronicznych znaczników czasu, dokumentów elektronicznych, usług rejestrowanego doręczenia elektronicznego, usług certyfikacyjnych uwierzytelniania witryn internetowych, archiwizacji elektronicznej, elektronicznego poświadczenia atrybutów, zarządzania urządzeniami do składania podpisów i pieczęci elektronicznych na odległość oraz rejestrów elektronicznych;

d) określa warunki wydawania przez państwa członkowskie europejskich portfeli tożsamości cyfrowej.”;

2) w art. 2 wprowadza się następujące zmiany:

a) ust. 1 otrzymuje brzmienie:

„1. Niniejsze rozporządzenie ma zastosowanie do systemów identyfikacji elektronicznej, które zostały notyfikowane przez państwo członkowskie, do europejskich portfeli tożsamości cyfrowej wydanych przez państwa członkowskie oraz do dostawców usług zaufania mających siedzibę w Unii.”;

b) ust. 3 otrzymuje brzmienie:

„3. Niniejsze rozporządzenie nie ma wpływu na prawo krajowe ani unijne związane z zawieraniem i ważnością umów lub innych zobowiązań prawnych lub proceduralnych związanych z wymogami sektorowymi dotyczącymi formy mającymi podstawowe skutki prawne.”;

3) w art. 3 wprowadza się następujące zmiany:

a) pkt 2 otrzymuje brzmienie:

„2) »środek identyfikacji elektronicznej« oznacza materialną lub niematerialną jednostkę, w tym europejskie portfele tożsamości cyfrowej lub dowody osobiste w rozumieniu rozporządzenia (UE) 2019/1157, zawierającą dane identyfikujące osobę i używaną do celów uwierzytelniania dla usługi online lub offline;”;

b) pkt 4 otrzymuje brzmienie:

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

c) pkt 14 otrzymuje brzmienie:

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

d) pkt 16 otrzymuje brzmienie:

„16) »usługa zaufania« oznacza usługę elektroniczną zazwyczaj świadczoną odpłatnie, która obejmuje:

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

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

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

d) archiwizację elektroniczną dokumentów elektronicznych;

e) zarządzanie urządzeniami do składania podpisów i pieczęci elektronicznych na odległość;

f) zapisywanie danych elektronicznych w rejestrze elektronicznym.”;

e) pkt 21 otrzymuje brzmienie:

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

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

„23a) »kwalifikowane urządzenie do składania podpisu na odległość« oznacza kwalifikowane urządzenie do składania podpisu elektronicznego, którym to urządzeniem kwalifikowany dostawca usług zaufania generuje lub kopiuje dane służące do składania podpisu elektronicznego w imieniu podpisującego lub zarządza tymi danymi;

23b) »kwalifikowane urządzenie do składania pieczęci na odległość« oznacza kwalifikowane urządzenie do składania pieczęci elektronicznej, którym to urządzeniem kwalifikowany dostawca usług zaufania generuje lub kopiuje dane służące do składania podpisu elektronicznego w imieniu podmiotu składającego pieczęć lub zarządza tymi danymi;”;

g) pkt 29 otrzymuje brzmienie:

„29) »certyfikat pieczęci elektronicznej« oznacza poświadczenie elektroniczne lub zestaw poświadczeń, które łączą dane służące do walidacji pieczęci elektronicznej z osobą prawną i potwierdzają nazwę tej osoby;”;

h) pkt 41 otrzymuje brzmienie:

„41) »walidacja« oznacza proces weryfikacji i potwierdzenia ważności podpisu elektronicznego, pieczęci elektronicznej, danych identyfikujących osobę lub elektronicznego poświadczenia atrybutów;”;

i) dodaje się pkt 42–55 w brzmieniu:

„42) »europejski portfel tożsamości cyfrowej« jest produktem i usługą, które umożliwiają użytkownikowi przechowywanie danych dotyczących tożsamości, danych uwierzytelniających i atrybutów powiązanych z jego tożsamością, dostarczanie ich na żądanie stronom ufającym oraz wykorzystywanie ich do uwierzytelniania online i offline na potrzeby usługi zgodnie z art. 6a, jak również składanie kwalifikowanych podpisów i pieczęci elektronicznych;

43) »atrybut« jest cechą, właściwością lub przymiotem osoby fizycznej lub prawnej lub podmiotu, wyrażonymi w postaci elektronicznej;

44) »elektroniczne poświadczenie atrybutów« oznacza poświadczenie w postaci elektronicznej, które umożliwia uwierzytelnienie atrybutów;

45) »kwalifikowane elektroniczne poświadczenie atrybutów« oznacza elektroniczne poświadczenie atrybutów, które jest wydawane przez kwalifikowanego dostawcę usług zaufania i spełnia wymogi określone w załączniku V;

46) »źródło autentyczne« oznacza repozytorium lub system, prowadzone w ramach odpowiedzialności podmiotu sektora publicznego lub podmiotu prywatnego, które zawiera atrybuty dotyczące osoby fizycznej lub prawnej i które uważa się za podstawowe źródło tych informacji lub uznaje za autentyczne w prawie krajowym;

47) »archiwizacja elektroniczna« oznacza usługę zapewniającą odbiór, przechowywanie, usuwanie i transmisję danych lub dokumentów elektronicznych w celu zagwarantowania ich integralności, dokładności ich pochodzenia i cech prawnych przez cały okres zachowywania;

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

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

50) »silne uwierzytelnianie użytkownika« oznacza uwierzytelnianie oparte na wykorzystaniu co najmniej dwóch elementów zaklasyfikowanych jako wiedza, posiadanie i cechy użytkownika, które są niezależne, w taki sposób, aby naruszenie jednego z nich nie zagrażało wiarygodności pozostałych, zaprojektowane w taki sposób, aby chronić poufność danych służących do uwierzytelniania;

51) »konto użytkownika« oznacza mechanizm umożliwiający użytkownikowi dostęp do usług publicznych lub prywatnych na warunkach określonych przez dostawcę usług;

52) »dane uwierzytelniające« oznacza dowód zdolności, doświadczenia, prawa lub zgody danej osoby;

53) »rejestr elektroniczny« oznacza odporny na ingerencję zapis elektroniczny danych, zapewniający autentyczność i integralność zawartych w nim danych, dokładność ich daty i godziny oraz ich uporządkowania chronologicznego;

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

55) »unikalna identyfikacja« oznacza proces, w którym dane identyfikujące osobę lub środki identyfikacji osoby są dopasowywane do istniejącego konta należącego do tej samej osoby lub z nim wiązane.";

4) art. 5 otrzymuje brzmienie:

„*Artykuł 5*

Pseudonimy w transakcji elektronicznej

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

5) w rozdziale II nagłówek otrzymuje brzmienie:

„SEKCJA I

IDENTYFIKACJA ELEKTRONICZNA";

6) uchyla się art. 6;

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

„*Artykuł 6a*

Europejskie portfele tożsamości cyfrowej

1. W celu zapewnienia wszystkim osobom fizycznym i prawnym w Unii bezpiecznego, zaufanego i sprawnego dostępu do transgranicznych usług publicznych i prywatnych każde państwo członkowskie wydaje europejski portfel tożsamości cyfrowej w terminie 12 miesięcy od wejścia w życie niniejszego rozporządzenia.

2. Europejskie portfele tożsamości cyfrowej są wydawane:

   a) przez państwo członkowskie;

   b) na mocy upoważnienia od państwa członkowskiego;

   c) niezależnie, lecz są uznawane przez państwo członkowskie.

3. Europejskie portfele tożsamości cyfrowej umożliwiają użytkownikowi:

   a) bezpieczne żądanie i otrzymywanie, przechowywanie, wybieranie, łączenie i udostępnianie – w sposób przejrzysty i identyfikowalny dla użytkownika – niezbędnych danych prawnych identyfikujących osobę i elektronicznego poświadczenia atrybutów na potrzeby uwierzytelniania

online i offline w celu korzystania z usług publicznych i prywatnych online;

b) podpisywanie za pomocą kwalifikowanego podpisu elektronicznego.

4. Portfele tożsamości cyfrowej w szczególności:

a) zapewniają wspólny interfejs:

1) dla kwalifikowanych i niekwalifikowanych dostawców usług zaufania wydających kwalifikowane i niekwalifikowane elektroniczne poświadczenia atrybutów lub inne kwalifikowane i niekwalifikowane certyfikaty do celów wydawania takich poświadczeń i certyfikatów na potrzeby europejskiego portfela tożsamości cyfrowej;

2) dla stron ufających w celu wnioskowania o dane identyfikujące osobę i elektroniczne poświadczenia atrybutów oraz ich walidację;

3) w celu przedstawiania stronom ufającym danych identyfikujących osobę, elektronicznego poświadczenia atrybutów lub innych danych, takich jak dane uwierzytelniające, w trybie lokalnym niewymagającym dostępu internetowego do portfela;

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

b) zapewniają, aby dostawcy usług zaufania w zakresie kwalifikowanych poświadczeń atrybutów nie mogli otrzymywać żadnych informacji o wykorzystaniu tych atrybutów;

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

d) zapewniają mechanizm mający na celu zapewnienie, aby strona ufająca była w stanie uwierzytelnić użytkownika i otrzymywać elektroniczne poświadczenia atrybutów;

e) zapewniają, aby dane identyfikujące osobę, o których mowa w art. 12 ust. 4 lit. d), unikalnie i trwale reprezentowały powiązaną z nimi osobę fizyczną lub prawną.

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

a) zapewnić możliwość weryfikacji ich autentyczności i ważności;

b) umożliwić stronom ufającym weryfikację, czy poświadczenia atrybutów są ważne;

c) umożliwić stronom ufającym i kwalifikowanym dostawcom usług zaufania weryfikację autentyczności i ważności przyporządkowanych danych identyfikujących osobę.

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

bezpieczeństwa. W przypadku osób fizycznych korzystanie z europejskich portfeli tożsamości cyfrowej jest nieodpłatne.

7. Użytkownik ma pełną kontrolę nad europejskim portfelem tożsamości cyfrowej. Wydawca europejskiego portfela tożsamości cyfrowej nie gromadzi informacji na temat korzystania z portfela, które nie są niezbędne do świadczenia usług związanych z portfelem, ani nie łączy danych identyfikujących osobę ani żadnych innych danych osobowych przechowywanych lub związanych z korzystaniem z europejskiego portfela tożsamości cyfrowej z danymi osobowymi pochodzącymi z innych usług oferowanych przez tego wydawcę lub z usług osób trzecich, które nie są niezbędne do świadczenia usług związanych z portfelem, chyba że użytkownik wyraźnie o to wystąpi. Dane osobowe związane z udostępnianiem europejskich portfeli tożsamości cyfrowej muszą być fizycznie i logicznie oddzielone od wszelkich innych przechowywanych danych. Jeśli europejski portfel tożsamości cyfrowej jest udostępniany przez podmioty prywatne zgodnie z ust. 1 lit. b) i c), przepisy art. 45f ust. 4 stosuje się odpowiednio.

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

9. Art. 24 ust. 2 lit. b), e), g) i h) stosuje się odpowiednio do państw członkowskich wydających europejskie portfele tożsamości cyfrowej.

10. Europejski portfel tożsamości cyfrowej jest dostępny dla osób niepełnosprawnych zgodnie z wymogami dostępności określonymi w załączniku I do dyrektywy (UE) 2019/882.

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

Artykuł 6b

Strony ufające europejskich portfeli tożsamości cyfrowej

1. W przypadku gdy strony ufające zamierzają polegać na europejskich portfelach tożsamości cyfrowej wydanych zgodnie z niniejszym rozporządzeniem, informują o tym państwo członkowskie, w którym strona ufająca ma siedzibę, aby zapewnić zgodność z wymogami określonymi w prawie Unii lub prawie krajowym w odniesieniu do świadczenia szczególnych usług. Informując o swoim zamiarze polegania na europejskim portfelu tożsamości cyfrowej, informują również o zamierzonym wykorzystaniu europejskiego portfela tożsamości cyfrowej.

2. Państwa członkowskie wdrażają wspólny mechanizm uwierzytelniania stron ufających.

3. Strony ufające są odpowiedzialne za przeprowadzenie procedury uwierzytelniania danych identyfikujących osobę oraz elektronicznego poświadczenia atrybutów pochodzących z europejskich portfeli tożsamości cyfrowej.

4. W terminie 6 miesięcy od wejścia w życie niniejszego rozporządzenia Komisja ustanawia specyfikacje techniczne i operacyjne dotyczące wymogów, o których mowa w ust. 1 i 2, w drodze aktu wykonawczego dotyczącego wdrożenia europejskich portfeli tożsamości cyfrowej, o których mowa w art. 6a ust. 10.

Artykuł 6c

Certyfikacja europejskich portfeli tożsamości cyfrowej

1. Europejskie portfele tożsamości cyfrowej, które uzyskały certyfikację lub w odniesieniu do których wydano deklarację zgodności w ramach programu certyfikacji cyberbezpieczeństwa zgodnie z rozporządzeniem (UE) 2019/881 i odniesienia do których opublikowano w *Dzienniku Urzędowym Unii Europejskiej*, uznaje się za spełniające odpowiednie wymogi w zakresie cyberbezpieczeństwa ustanowione w art. 6a ust. 3, 4 i 5 w zakresie, w jakim certyfikat cyberbezpieczeństwa lub deklaracja zgodności, lub ich części obejmują te wymogi.

2. Spełnienie wymogów określonych w art. 6a ust. 3, 4 i 5 związanych z operacjami przetwarzania danych osobowych dokonywanymi przez wydawcę europejskich portfeli tożsamości cyfrowej poświadcza się zgodnie z rozporządzeniem (UE) 2016/679.

3. Zgodność europejskich portfeli tożsamości cyfrowej z wymogami określonymi w art. 6a ust. 3, 4 i 5 jest certyfikowana przez akredytowane podmioty publiczne lub prywatne wyznaczone przez państwa członkowskie.

4. W terminie 6 miesięcy od wejścia w życie niniejszego rozporządzenia Komisja ustanawia – w drodze aktów wykonawczych – wykaz norm certyfikacji europejskich portfeli tożsamości cyfrowej, o których mowa w ust. 3.

5. Państwa członkowskie przekazują Komisji nazwy i adresy podmiotów publicznych lub prywatnych, o których mowa w ust. 3. Komisja udostępnia te informacje państwom członkowskim.

6. Komisja jest uprawniona do przyjmowania aktów delegowanych, zgodnie z art. 47, dotyczących ustanowienia specjalnych kryteriów, które muszą spełniać wyznaczone podmioty, o których mowa w ust. 3.

Artykuł 6d

Publikacja wykazu certyfikowanych europejskich portfeli tożsamości cyfrowej

1. Państwa członkowskie bez zbędnej zwłoki informują Komisję o europejskich portfelach tożsamości cyfrowej, które zostały wydane zgodnie z art. 6a i certyfikowane przez organy, o których mowa w art. 6c ust. 3. Bez zbędnej zwłoki informują również Komisję o odwołaniu certyfikacji.

2. Na podstawie otrzymanych informacji Komisja sporządza, publikuje i prowadzi wykaz certyfikowanych europejskich portfeli tożsamości cyfrowej.

3. W terminie 6 miesięcy od wejścia w życie niniejszego rozporządzenia Komisja określa formaty i procedury mające zastosowanie do celów ust. 1 w drodze aktu wykonawczego dotyczącego wdrożenia europejskich portfeli tożsamości cyfrowej, o których mowa w art. 6a ust. 10.”;

8) przed art. 7 dodaje się następujący nagłówek:

„SEKCJA II

SYSTEMY IDENTYFIKACJI ELEKTRONICZNEJ”;

9) w art. 7 formuła wprowadzająca otrzymuje brzmienie:

„Zgodnie z art. 9 ust. 1 państwa członkowskie notyfikują, w terminie 12 miesięcy od wejścia w życie niniejszego rozporządzenia, co najmniej jeden system identyfikacji elektronicznej obejmujący co najmniej jeden środek identyfikacji:”;

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

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

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

11) dodaje się art. 10a w brzmieniu:

„*Artykuł 10a*

Naruszenie bezpieczeństwa europejskich portfeli tożsamości cyfrowej

1. W przypadku gdy nastąpi naruszenie lub częściowa kompromitacja europejskich cyfrowych portfeli wydanych na podstawie art. 6a oraz mechanizmów walidacji, o których mowa w art. 6a ust. 5 lit. a), b) i c), mające wpływ na wiarygodność tych portfeli i mechanizmów lub na wiarygodność pozostałych europejskich portfeli tożsamości cyfrowej, wydające państwo członkowskie bezzwłocznie zawiesza wydawanie lub unieważnia dany europejski portfel tożsamości cyfrowej oraz powiadamia o tym odpowiednio pozostałe państwa członkowskie i Komisję.

2. W przypadku gdy naruszenie lub kompromitacja, o których mowa w ust. 1, zostaną wyeliminowane, wydające państwo członkowskie przywraca wydawanie i wykorzystywanie europejskiego portfela tożsamości cyfrowej i bez zbędnej zwłoki powiadamia o tym pozostałe państwa członkowskie i Komisję.

3. Jeżeli naruszenie lub kompromitacja, o których mowa w ust. 1, nie zostaną wyeliminowane w ciągu trzech miesięcy od zawieszenia lub unieważnienia, zainteresowane państwo członkowskie wycofuje dany europejski cyfrowy portfel oraz odpowiednio powiadamia pozostałe państwa członkowskie i Komisję o jego wycofaniu. W przypadku gdy jest to uzasadnione wagą naruszenia, dany europejski portfel tożsamości cyfrowej wycofuje się bezzwłocznie.

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

5. W terminie 6 miesięcy od wejścia w życie niniejszego rozporządzenia Komisja doprecyzuje środki, o których mowa w ust. 1 i 3, w drodze aktu wykonawczego dotyczącego wdrożenia europejskich portfeli tożsamości cyfrowej, o których mowa w art. 6a ust. 10.”;

12) dodaje się art. 11a w brzmieniu:

„*Artykuł 11a*

Unikalna identyfikacja

1. W przypadku gdy notyfikowane środki identyfikacji elektronicznej i europejskie portfele tożsamości cyfrowej są używane do celów uwierzytelniania, państwa członkowskie zapewniają unikalną identyfikację.

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

3. W terminie 6 miesięcy od wejścia w życie niniejszego rozporządzenia Komisja doprecyzuje środki, o których mowa w ust. 1 i 2, w drodze aktu wykonawczego dotyczącego wdrożenia europejskich portfeli tożsamości cyfrowej, o których mowa w art. 6a ust. 10.";

13) w art. 12 wprowadza się następujące zmiany:

a) w ust. 3 uchyla się lit. c) i d);

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

„d) odniesienie do minimalnego zbioru danych identyfikujących osobę niezbędnych do unikalnego i trwałego reprezentowania osoby fizycznej lub prawnej;";

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

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

14) dodaje się art. 12a w brzmieniu:

„*Artykuł 12a*

Certyfikacja systemów identyfikacji elektronicznej

1. Zgodność notyfikowanych systemów identyfikacji elektronicznej z wymogami określonymi w art. 6a, 8 i 10 może być certyfikowana przez podmioty publiczne lub prywatne wyznaczone przez państwa członkowskie.

2. Wzajemna ocena systemów identyfikacji elektronicznej, o której mowa w art. 12 ust. 6 lit. c), nie ma zastosowania do systemów identyfikacji elektronicznej certyfikowanych zgodnie z ust. 1 ani do części takich systemów. Aby wykazać zgodność takich systemów z wymogami określonymi w art. 8 ust. 2 dotyczącymi poziomów bezpieczeństwa systemów identyfikacji elektronicznej, państwa członkowskie mogą wykorzystać certyfikat lub unijną deklarację zgodności wydane zgodnie z odpowiednim europejskim programem certyfikacji cyberbezpieczeństwa ustanowionym na mocy rozporządzenia (UE) 2019/881.

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

15) po art. 12a dodaje się następujący nagłówek:

„SEKCJA III

TRANSGRANICZNE KORZYSTANIE ZE ŚRODKÓW IDENTYFIKACJI ELEKTRONICZNEJ';

16) dodaje się art. 12b i 12c w brzmieniu:

„Artykuł 12b

Transgraniczne korzystanie z europejskich portfeli tożsamości cyfrowej

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

2. W przypadku gdy prywatne strony ufające świadczące usługi są zobowiązane prawem krajowym lub prawem Unii do stosowania silnego uwierzytelniania użytkownika do celów identyfikacji w usługach online lub w przypadku gdy silne uwierzytelnianie użytkownika jest wymagane na podstawie zobowiązania umownego, w tym w obszarach transportu, energetyki, bankowości i usług finansowych, zabezpieczeń społecznych, zdrowia, wody pitnej, usług pocztowych, infrastruktury cyfrowej, edukacji lub telekomunikacji, prywatne strony ufające akceptują również europejskie portfele tożsamości cyfrowej wydane zgodnie z art. 6a.

3. W przypadku gdy bardzo duże platformy internetowe zdefiniowane w art. 25 ust. 1 rozporządzenia [odniesienie do rozporządzenia w sprawie aktu o usługach cyfrowych] wymagają uwierzytelniania użytkowników do celów dostępu do usług online, akceptują one również wykorzystywanie europejskich portfeli tożsamości cyfrowej wydanych zgodnie z art. 6a, bezwzględnie na podstawie dobrowolnego wniosku użytkownika i z poszanowaniem minimalnych atrybutów konkretnej usługi online, w odniesieniu do której wymaga się uwierzytelnienia, takich jak poświadczenie wieku.

4. Aby przyczynić się do zapewnienia szerokiej dostępności i używalności europejskich portfeli tożsamości cyfrowej objętych zakresem niniejszego rozporządzenia, Komisja wspiera i ułatwia opracowywanie samoregulacyjnych kodeksów postępowania na poziomie Unii („kodeksy postępowania"). Te kodeksy postępowania zapewniają akceptowanie środków identyfikacji elektronicznej, w tym europejskich portfeli tożsamości cyfrowej objętych zakresem niniejszego rozporządzenia, w szczególności przez dostawców usług korzystających z usług identyfikacji elektronicznej świadczonych przez strony trzecie do celów uwierzytelniania użytkownika. Komisja ułatwi opracowanie takich kodeksów postępowania w ścisłej współpracy ze wszystkimi odpowiednimi zainteresowanymi stronami i zachęci dostawców usług do ukończenia prac nad kodeksami postępowania w terminie 12 miesięcy od daty przyjęcia niniejszego rozporządzenia, a także do ich skutecznego wdrożenia w terminie 18 miesięcy od daty przyjęcia niniejszego rozporządzenia.

5. W terminie 18 miesięcy od uruchomienia europejskich portfeli tożsamości cyfrowej Komisja ocenia, czy na podstawie dowodów ukazujących dostępność i używalność europejskich portfeli tożsamości cyfrowej należy zobowiązać dodatkowych prywatnych dostawców usług online do akceptowania

wykorzystywania europejskich portfeli tożsamości cyfrowej bezwzględnie na podstawie dobrowolnego wniosku użytkownika. Kryteria oceny mogą obejmować zakres bazy użytkowników, obecność transgraniczną dostawców usług, rozwój technologiczny, zmiany sposobów użytkowania. Komisja jest uprawniona do przyjęcia aktów delegowanych na podstawie tej oceny w odniesieniu do przeglądu wymogów dotyczących uznawania europejskich portfeli tożsamości cyfrowej na podstawie ust. 1–4 niniejszego artykułu.

6. Do celów niniejszego artykułu europejskie portfele tożsamości cyfrowej nie podlegają wymogom, o którym mowa w art. 7 i 9.

Artykuł 12c

Wzajemne uznawanie innych środków identyfikacji elektronicznej

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

   a) środek identyfikacji elektronicznej jest wydany w ramach systemu identyfikacji elektronicznej wymienionego w wykazie, o którym mowa w art. 9;

   b) poziom bezpieczeństwa środka identyfikacji elektronicznej odpowiada poziomowi bezpieczeństwa równemu poziomowi bezpieczeństwa wymaganego przez odpowiedni podmiot sektora publicznego na potrzeby dostępu do tej usługi online w zainteresowanym państwie członkowskim lub wyższemu od tego poziomu, a w każdym razie nie niższemu od średniego poziomu bezpieczeństwa;

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

   Takiego uznania dokonuje się nie później niż 6 miesięcy po opublikowaniu przez Komisję wykazu, o którym mowa w akapicie pierwszym lit. a).

2. Środek identyfikacji elektronicznej wydawany w ramach systemu identyfikacji elektronicznej wymienionego w wykazie, o którym mowa w art. 9, i odpowiadający niskiemu poziomowi bezpieczeństwa, może być uznany przez podmioty sektora publicznego na potrzeby transgranicznego uwierzytelniania dla usługi online świadczonej przez te podmioty.”;

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

„1. Niezależnie od ust. 2 niniejszego artykułu, dostawcy usług zaufania są odpowiedzialni za szkody wyrządzone w sposób zamierzony lub z powodu zaniedbania osobie fizycznej lub prawnej w związku z niewypełnieniem obowiązków określonych w niniejszym rozporządzeniu, a także obowiązków w zakresie zarządzania ryzykiem w cyberprzestrzeni określonych w art. 18 dyrektywy (UE) XXXX/XXXX [dyrektywy NIS 2].”;

18) art.nbsp14 otrzymuje brzmienie:

„*Artykuł 14*

Aspekty międzynarodowe

1. Komisja może przyjąć zgodnie z art. 48 ust. 2 akty wykonawcze ustanawiające warunki, na których wymogi państwa trzeciego mające zastosowanie do dostawców usług zaufania mających siedzibę na jego terytorium i do świadczonych przez nich usług zaufania można uznać za równoważne wymogom mającym zastosowanie do kwalifikowanych dostawców usług zaufania mających siedzibę w Unii oraz do świadczonych przez nich kwalifikowanych usług zaufania.

2. W przypadku przyjęcia przez Komisję aktu wykonawczego na podstawie ust. 1 lub zawarcia przez nią umowy międzynarodowej w sprawie wzajemnego uznawania usług zaufania zgodnie z art. 218 Traktatu usługi zaufania świadczone przez dostawców mających siedzibę w zainteresowanym państwie trzecim są uznawane za równoważne kwalifikowanym usługom zaufania świadczonym przez kwalifikowanych dostawców usług zaufania mających siedzibę w Unii.”;

19) art. 15 otrzymuje brzmienie:

„*Artykuł 15*

Dostępność dla osób niepełnosprawnych

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

20) w art. 17 wprowadza się następujące zmiany:

a) w ust. 4 wprowadza się następujące zmiany:

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

„c) informowanie odpowiednich właściwych organów krajowych zainteresowanego państwa członkowskiego wyznaczonych zgodnie z dyrektywą (UE) XXXX/XXXX [dyrektywą NIS 2] o wszelkich istotnych naruszeniach bezpieczeństwa lub utracie integralności, o których poweźmie wiadomość w ramach wykonywania swoich obowiązków. W przypadku gdy naruszenie bezpieczeństwa lub utrata integralności dotyczy innych państw członkowskich, organ nadzoru powiadamia pojedynczy punkt kontaktowy zainteresowanego państwa członkowskiego wyznaczony zgodnie z dyrektywą (UE) XXXX/XXXX [dyrektywą NIS 2];”;

2) lit. f) otrzymuje brzmienie:

„f) współpracę z organami nadzorczymi ustanowionymi na mocy rozporządzenia (UE) 2016/679, w szczególności przez informowanie ich, bez zbędnej zwłoki, o wynikach audytów kwalifikowanych dostawców usług zaufania, w przypadku gdy doszło do naruszenia przepisów dotyczących ochrony danych

osobowych, a także o naruszeniach bezpieczeństwa stanowiących naruszenie ochrony danych osobowych;";

b) ust. 6 otrzymuje brzmienie:

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

c) ust. 8 otrzymuje brzmienie:

„8. W terminie 12 miesięcy od wejścia w życie niniejszego rozporządzenia Komisja w drodze aktów wykonawczych doprecyzowuje zadania organów nadzoru, o których mowa w ust. 4, oraz określa formaty i procedury dotyczące sprawozdania, o którym mowa w ust. 6. Te akty wykonawcze przyjmuje się zgodnie z procedurą sprawdzającą, o której mowa w art. 48 ust. 2.";

21) w art. 18 wprowadza się następujące zmiany:

a) tytuł art. 18 otrzymuje brzmienie:

„**Wzajemna pomoc i współpraca**";

b) ust. 1 otrzymuje brzmienie:

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

c) dodaje się ust. 4 i 5 w brzmieniu:

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

5. W terminie 12 miesięcy od wejścia w życie niniejszego rozporządzenia Komisja w drodze aktów wykonawczych ustanawia niezbędne proceduralne warunki ułatwiania współpracy między organami nadzoru, o których mowa w ust. 1.";

22) w art. 20 wprowadza się następujące zmiany:

a) ust. 1 otrzymuje brzmienie:

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

b) w ust. 2 ostatnie zdanie otrzymuje brzmienie:

„W przypadku gdy wydaje się, że zostały naruszone przepisy dotyczące ochrony danych, organ nadzoru informuje o wynikach swoich audytów organy nadzorcze na podstawie rozporządzenia (UE) 2016/679.”;

c) ust. 3 i 4 otrzymują brzmienie:

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

Jeżeli dostawca ten nie wyeliminuje przypadków niespełnienia wymogów w stosownych przypadkach w terminie ustalonym przez organ nadzoru, organ nadzoru, biorąc pod uwagę w szczególności zakres, czas trwania i skutki tego niespełnienia wymogów, może odebrać status kwalifikowany temu dostawcy lub danej świadczonej przez niego usłudze i żąda od niego, w stosownych przypadkach w ustalonym terminie, spełnienia wymogów określonych w dyrektywie (UE) XXXX/XXXX [dyrektywie NIS 2]. Organ nadzoru informuje organ, o którym mowa w art. 22 ust. 3, do celów zaktualizowania zaufanych list, o których mowa w art. 22 ust. 1.

Organ nadzoru informuje kwalifikowanego dostawcę usług zaufania o odebraniu jego statusu kwalifikowanego lub statusu kwalifikowanego danej usługi.

4. W terminie 12 miesięcy od wejścia w życie niniejszego rozporządzenia Komisja w drodze aktów wykonawczych podaje numery referencyjne następujących norm:

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

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

c) norm dotyczących programów oceny zgodności w zakresie przeprowadzania oceny zgodności kwalifikowanych dostawców usług zaufania przez jednostki oceniające zgodność i w zakresie

przekazywania raportu z oceny zgodności, o którym mowa w ust. 1.

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

23) w art. 21 wprowadza się następujące zmiany:

a) ust. 2 otrzymuje brzmienie:

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

W celu zweryfikowania zgodności dostawcy usług zaufania z wymogami określonymi w art. 18 dyrektywy (UE) XXXX/XXXX [dyrektywy NIS 2] organ nadzoru zwraca się do właściwych organów, o których mowa w dyrektywie (UE) XXXX/XXXX [dyrektywie NIS 2], o przeprowadzenie działań nadzorczych w tym zakresie oraz o udzielenie informacji na temat wyniku tych działań w terminie trzech dni od ich ukończenia.

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

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

b) ust. 4 otrzymuje brzmienie:

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

24) w art. 23 dodaje się ust. 2a w brzmieniu:

„2a. Ustępy 1 i 2 mają również zastosowanie do dostawców usług zaufania mających siedzibę w państwach trzecich i do świadczonych przez nich usług, pod warunkiem że zostali oni uznani w Unii zgodnie z art. 14.";

25) w art. 24 wprowadza się następujące zmiany:

a) ust. 1 otrzymuje brzmienie:

„1. Wydając kwalifikowany certyfikat lub kwalifikowane elektroniczne poświadczenie atrybutów dla usługi zaufania, kwalifikowany dostawca

usług zaufania weryfikuje tożsamość i, w stosownym przypadku, wszelkie specjalne atrybuty osoby fizycznej lub prawnej, której wydaje kwalifikowany certyfikat lub kwalifikowane elektroniczne poświadczenie atrybutów.

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

a) przy użyciu notyfikowanego środka identyfikacji elektronicznej, który spełnia wymogi określone w art. 8 w odniesieniu do średniego lub wysokiego poziomu bezpieczeństwa;

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

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

d) przez fizyczną obecność osoby fizycznej lub upoważnionego przedstawiciela osoby prawnej, za pomocą odpowiednich procedur oraz zgodnie z prawem krajowym, jeżeli inne środki nie są dostępne.";

b) dodaje się ust. 1a w brzmieniu:

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

c) w ust. 2 wprowadza się następujące zmiany:

1) lit. d) otrzymuje brzmienie:

„d) przed wejściem w stosunek umowny informuje, w jasny, zrozumiały i przystępny sposób w przestrzeni publicznej oraz indywidualnie wszystkie osoby pragnące skorzystać z kwalifikowanej usługi zaufania o dokładnych warunkach korzystania z tej usługi, w tym o wszelkich ograniczeniach korzystania z niej;";

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

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

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

(ii) środki związane z kontrolami proceduralnymi lub administracyjnymi;

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

fb) zawiadamia organ nadzoru i, w stosownych przypadkach, inne właściwe podmioty o wszelkich powiązanych przypadkach naruszenia bezpieczeństwa lub zakłóceniach we wdrażaniu środków, o których mowa w lit. fa) ppkt (i), (ii) i (iii), które to naruszenia lub zakłócenia mają znaczący wpływ na świadczoną usługę zaufania lub przetwarzane w jej ramach dane osobowe.";

3) lit. g) i h) otrzymują brzmienie:

„g) podejmuje odpowiednie środki zapobiegające fałszowaniu, kradzieży lub niewłaściwemu wykorzystaniu danych, lub nieupoważnionemu usuwaniu, zmianie lub uniemożliwianiu dostępu do danych;

h) rejestruje i udostępnia tak długo, jak jest to konieczne po zaprzestaniu działalności przez kwalifikowanego dostawcę usług zaufania, wszelkie odpowiednie informacje dotyczące danych wydanych i otrzymanych przez kwalifikowanego dostawcę usług zaufania, do celów przedstawienia dowodów w postępowaniach sądowych i do celów zapewnienia ciągłości usług. Informacje mogą być przechowywane w formie elektronicznej;";

4) uchyla się lit. j);

d) dodaje się ust. 4a w brzmieniu:

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

e) ust. 5 otrzymuje brzmienie:

„5. W terminie 12 miesięcy od wejścia w życie niniejszego rozporządzenia Komisja w drodze aktów wykonawczych podaje numery referencyjne norm dotyczących wymogów, o których mowa w ust. 2. W przypadku gdy wiarygodne systemy i produkty spełniają te normy, domniemywa się zgodność z wymogami określonymi w niniejszym artykule. Te akty wykonawcze przyjmuje się zgodnie z procedurą sprawdzającą, o której mowa w art. 48 ust. 2.";

f) dodaje się ust. 6 w brzmieniu:

„6. Komisja jest uprawniona do przyjęcia aktów delegowanych dotyczących dodatkowych środków, o których mowa w ust. 2 lit. fa).";

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

„6. W terminie 12 miesięcy od wejścia w życie niniejszego rozporządzenia Komisja w drodze aktów wykonawczych podaje numery referencyjne norm dotyczących kwalifikowanych certyfikatów podpisów elektronicznych.

W przypadku gdy kwalifikowany certyfikat podpisu elektronicznego spełnia te normy, domniemywa się zgodność z wymogami określonymi w załączniku I. Te akty wykonawcze przyjmuje się zgodnie z procedurą sprawdzającą, o której mowa w art. 48 ust. 2.";

27) W art. 29 dodaje się nowy ust. 1a w brzmieniu:

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

28) dodaje się art. 29a w brzmieniu:

„*Artykuł 29a*

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

1. Zarządzaniem kwalifikowanymi urządzeniami do składania podpisu elektronicznego na odległość jako usługą kwalifikowaną może zajmować się wyłącznie kwalifikowany dostawca usług zaufania, który:

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

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

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

      liczba skopiowanych zbiorów danych nie przekracza minimum niezbędnego do zapewnienia ciągłości usługi;

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

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

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

„3a. Certyfikacja, o której mowa w ust. 1, jest ważna przez 5 lat, pod warunkiem, że regularnie, co dwa lata, przeprowadza się ocenę podatności na zagrożenia. W przypadku stwierdzenia podatności, które nie zostały naprawione, certyfikacja zostaje cofnięta.";

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

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

31) w art. 32 wprowadza się następujące zmiany:

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

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

b) ust. 3 otrzymuje brzmienie:

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

32) art. 34 otrzymuje brzmienie:

„*Artykuł 34*

Kwalifikowana usługa konserwacji kwalifikowanych podpisów elektronicznych

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

2. W przypadku gdy ustalenia w zakresie kwalifikowanej usługi konserwacji kwalifikowanych podpisów elektronicznych spełniają normy, o których mowa w ust. 3, domniemywa się zgodność z wymogami określonymi w ust. 1.

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

33) w art.37 wprowadza się następujące zmiany:

a) dodaje się ust. 2a w brzmieniu:

„2a. W przypadku gdy zaawansowana pieczęć elektroniczna spełnia normy, o których mowa w ust. 4, domniemywa się zgodność z wymogami dotyczącymi zaawansowanych pieczęci elektronicznych, o których mowa w art. 36 i ust. 5 niniejszego artykułu.”;

b) ust. 4 otrzymuje brzmienie:

„4. W terminie 12 miesięcy od wejścia w życie niniejszego rozporządzenia Komisja w drodze aktów wykonawczych podaje numery referencyjne norm dotyczących zaawansowanych pieczęci elektronicznych. Te akty wykonawcze przyjmuje się zgodnie z procedurą sprawdzającą, o której mowa w art. 48 ust. 2.”;

34) w art. 38 wprowadza się następujące zmiany:

a) ust. 1 otrzymuje brzmienie:

„1. Kwalifikowane certyfikaty pieczęci elektronicznych spełniają wymogi określone w załączniku III. W przypadku gdy kwalifikowany certyfikat pieczęci elektronicznej spełnia normy, o których mowa w ust. 6,

domniemywa się zgodność z wymogami określonymi w załączniku III.”;

b) ust. 6 otrzymuje brzmienie:

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

35) dodaje się art. 39a w brzmieniu:

„*Artykuł 39a*

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

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

36) w art. 42 wprowadza się następujące zmiany:

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

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

b) ust. 2 otrzymuje brzmienie:

„2. W terminie 12 miesięcy od wejścia w życie niniejszego rozporządzenia Komisja w drodze aktów wykonawczych podaje numery referencyjne norm dotyczących powiązania daty i czasu z danymi oraz precyzyjnych źródeł czasu. Te akty wykonawcze przyjmuje się zgodnie z procedurą sprawdzającą, o której mowa w art. 48 ust. 2.”;

37) w art. 44 wprowadza się następujące zmiany:

a) dodaje się ust. 1a w brzmieniu:

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

b) ust. 2 otrzymuje brzmienie:

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

38) art. 45 otrzymuje brzmienie:

„*Artykuł 45*

Wymogi dotyczące kwalifikowanych certyfikatów uwierzytelniania witryn internetowych

1. Kwalifikowane certyfikaty uwierzytelniania witryn internetowych muszą spełniać wymogi określone w załączniku IV. W przypadku gdy spełniają one

normy, o których mowa w ust. 3, domniemywa się zgodność kwalifikowanych certyfikatów uwierzytelniania witryn internetowych z wymogami określonymi w załączniku IV.

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

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

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

„SEKCJA 9

ELEKTRONICZNE POŚWIADCZENIE ATRYBUTÓW

Artykuł 45a

Skutki prawne elektronicznego poświadczenia atrybutów

1. Nie kwestionuje się skutku prawnego elektronicznego poświadczenia atrybutów ani jego dopuszczalności jako dowodu w postępowaniu sądowym wyłącznie z tego powodu, że poświadczenie to ma postać elektroniczną.

2. Kwalifikowane elektroniczne poświadczenie atrybutów ma taki sam skutek prawny jak legalnie wystawione poświadczenia w formie papierowej.

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

Artykuł 45b

Elektroniczne poświadczenie atrybutów w usługach publicznych

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

Artykuł 45c

Wymogi dotyczące kwalifikowanego poświadczenia atrybutów

1. Kwalifikowane elektroniczne poświadczenie atrybutów musi spełniać wymogi określone w załączniku V. W przypadku gdy spełnia ono normy, o których mowa w ust. 4, domniemywa się zgodność kwalifikowanego elektronicznego poświadczenia atrybutów z wymogami określonymi w załączniku V.
2. Kwalifikowane elektroniczne poświadczenia atrybutów nie podlegają żadnym obowiązkowym wymogom wykraczającym poza wymogi określone w załączniku V.
3. Jeżeli kwalifikowane elektroniczne poświadczenie atrybutów zostało unieważnione po początkowym wydaniu, traci ono ważność z chwilą jego unieważnienia i w żadnym przypadku nie można przywrócić jego poprzedniego statusu.
4. W terminie 6 miesięcy od wejścia w życie niniejszego rozporządzenia Komisja określa numery referencyjne norm dotyczących kwalifikowanych elektronicznych poświadczeń atrybutów w drodze aktu wykonawczego dotyczącego wdrożenia europejskich portfeli tożsamości cyfrowej, o których mowa w art. 6a ust. 10.

Artykuł 45d

Weryfikacja atrybutów na podstawie źródeł autentycznych

1. Państwa członkowskie zapewniają, aby przynajmniej w odniesieniu do atrybutów wymienionych w załączniku VI, jeżeli atrybuty te opierają się na źródłach autentycznych w sektorze publicznym, podjęto działania umożliwiające kwalifikowanym dostawcom elektronicznych poświadczeń atrybutów weryfikację drogą elektroniczną, na żądanie użytkownika, autentyczności atrybutu bezpośrednio w zestawieniu z odpowiednim źródłem autentycznym na poziomie krajowym lub poprzez wyznaczonych pośredników uznanych na poziomie krajowym zgodnie z prawem krajowym lub prawem Unii.
2. W terminie 6 miesięcy od wejścia w życie niniejszego rozporządzenia, uwzględniając mające zastosowanie normy międzynarodowe, Komisja określa minimalne specyfikacje techniczne, normy i procedury dotyczące katalogu atrybutów i systemów poświadczania atrybutów i procedur weryfikacji kwalifikowanych elektronicznych poświadczeń atrybutów w drodze aktu wykonawczego dotyczącego wdrożenia europejskich portfeli tożsamości cyfrowej, o których mowa w art. 6a ust. 10.

Artykuł 45e

Wydawanie elektronicznych poświadczeń atrybutów do europejskich portfeli tożsamości cyfrowej

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

Artykuł 45f

Dodatkowe przepisy w odniesieniu do świadczenia usług elektronicznego poświadczania atrybutów

1. Dostawcy kwalifikowanych i niekwalifikowanych usług elektronicznego poświadczania atrybutów nie łączą danych osobowych związanych ze świadczeniem tych usług z danymi osobowymi pochodzącymi z jakichkolwiek innych oferowanych przez nich usług.

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

3. Dane osobowe związane ze świadczeniem usług kwalifikowanego elektronicznego poświadczania atrybutów muszą być fizycznie i logicznie oddzielone od wszelkich innych przechowywanych danych.

4. Dostawcy usług kwalifikowanego elektronicznego poświadczania atrybutów świadczą takie usługi w ramach odrębnego podmiotu prawnego.

SEKCJA 10

KWALIFIKOWANE USŁUGI ARCHIWIZACJI ELEKTRONICZNEJ

Artykuł 45g

Kwalifikowane usługi archiwizacji elektronicznej

Kwalifikowaną usługę archiwizacji elektronicznej dokumentów elektronicznych może świadczyć wyłącznie kwalifikowany dostawca usług zaufania, który stosuje procedury i technologie umożliwiające przedłużenie wiarygodności dokumentu elektronicznego poza techniczny okres ważności.

W terminie 12 miesięcy od wejścia w życie niniejszego rozporządzenia Komisja w drodze aktów wykonawczych podaje numery referencyjne norm dotyczących usług archiwizacji elektronicznej. Te akty wykonawcze przyjmuje się zgodnie z procedurą sprawdzającą, o której mowa w art. 48 ust. 2.

SEKCJA 11

REJESTRY ELEKTRONICZNE

Artykuł 45h

Skutki prawne rejestrów elektronicznych

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

2. Kwalifikowany rejestr elektroniczny korzysta z domniemania unikalności i autentyczności zawartych w nim danych, dokładności ich daty i czasu oraz ich sekwencyjnego, chronologicznego uporządkowania w ramach rejestru.

Artykuł 45i

Wymogi dotyczące kwalifikowanych rejestrów elektronicznych

1. Kwalifikowane rejestry elektroniczne muszą spełniać następujące wymogi:

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

   b) zapewniają unikalność, autentyczność i prawidłową kolejność zapisów danych w rejestrze;

c) zapewniają prawidłowe, sekwencyjne, chronologiczne uporządkowanie danych w rejestrze oraz dokładność daty i godziny wprowadzenia danych;

d) dane zapisuje się w nich w taki sposób, że każda późniejsza zmiana danych jest bezpośrednio wykrywalna.

2. W przypadku gdy rejestr elektroniczny spełnia normy, o których mowa w ust. 3, domniemywa się zgodność z wymogami określonymi w ust. 1.

3. Komisja może w drodze aktów wykonawczych podać numery referencyjne norm dotyczących procesów wykonania i rejestracji zbioru danych w kwalifikowanym rejestrze elektronicznym oraz jego tworzenia. Te akty wykonawcze przyjmuje się zgodnie z procedurą sprawdzającą, o której mowa w art. 48 ust. 2.";

40) dodaje się art. 48a w brzmieniu:

„*Artykuł 48a*

Wymogi dotyczące sprawozdawczości

1. Państwa członkowskie gwarantują gromadzenie danych statystycznych dotyczących działania europejskich portfeli tożsamości cyfrowej i kwalifikowanych usług zaufania.

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

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

b) rodzaj i liczba usług akceptujących korzystanie z europejskiego cyfrowego portfela;

c) incydenty i przestoje w infrastrukturze na poziomie krajowym uniemożliwiające korzystanie z aplikacji portfela tożsamości cyfrowej.

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

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

41) art. 49 otrzymuje brzmienie:

„*Artykuł 49*

Przegląd

1. Komisja dokona przeglądu stosowania niniejszego rozporządzenia i przekaże sprawozdanie Parlamentowi Europejskiemu i Radzie w terminie 24 miesięcy od jego wejścia w życie. Komisja oceni w szczególności, czy należy zmienić zakres stosowania niniejszego rozporządzenia lub jego poszczególnych przepisów, biorąc pod uwagę doświadczenia zdobyte przy stosowaniu niniejszego rozporządzenia, a także rozwój technologiczny, sytuację rynkową i prawną. W stosownych przypadkach do sprawozdania dołącza się propozycje zmian niniejszego rozporządzenia.

2. Sprawozdanie oceniające obejmuje ocenę dostępności i używalności środków identyfikacji, w tym europejskich portfeli tożsamości cyfrowej, objętych zakresem niniejszego rozporządzenia, oraz ocenę, czy wszyscy prywatni dostawcy usług online korzystający z usług identyfikacji elektronicznej świadczonych przez strony trzecie do celów uwierzytelniania użytkowników zostaną zobowiązani do akceptowania wykorzystywania notyfikowanych środków identyfikacji elektronicznej i europejskiego portfela tożsamości cyfrowej.

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

42) art. 51 otrzymuje brzmienie:

„*Artykuł 51*

Środki przejściowe

1. Bezpieczne urządzenia do składania podpisu, których zgodność ustalono zgodnie z art. 3 ust. 4 dyrektywy 1999/93/WE, w dalszym ciągu uznaje się za kwalifikowane urządzenia do składania podpisu elektronicznego na mocy niniejszego rozporządzenia do [data – Urząd Publikacji: proszę wstawić okres czterech lat od wejścia w życie niniejszego rozporządzenia].

2. Kwalifikowane certyfikaty wydane osobom fizycznym na mocy dyrektywy 1999/93/WE w dalszym ciągu uznaje się za kwalifikowane certyfikaty podpisów elektronicznych na mocy niniejszego rozporządzenia do [data – Urząd Publikacji: proszę wstawić okres czterech lat od wejścia w życie niniejszego rozporządzenia].”.

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

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

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

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

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

48) do niniejszego rozporządzenia dodaje się nowy załącznik VI.

Artykuł 2

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*

OCENA SKUTKÓW FINANSOWYCH REGULACJI

1. STRUKTURA WNIOSKU/INICJATYWY

1.1. Tytuł wniosku/inicjatywy

Rozporządzenie Parlamentu Europejskiego i Rady w sprawie ram europejskiej tożsamości cyfrowej, zmieniające rozporządzenie eIDAS

1.2. Obszary polityki, których dotyczy wniosek/inicjatywa

Dziedzina polityki: Rynek wewnętrzny

Europa na miarę ery cyfrowej

1.3. Wniosek/inicjatywa dotyczy:

☐ **nowego działania**

☐ **nowego działania, będącego następstwem projektu pilotażowego/działania przygotowawczego**[28]

☑**przedłużenia bieżącego działania**

☐ **połączenia lub przekształcenia co najmniej jednego działania pod kątem innego/nowego działania**

1.4. Cel(e)

1.4.1. Cel(e) ogólny(e)

Ogólnym celem niniejszej inicjatywy jest zapewnienie prawidłowego funkcjonowania rynku wewnętrznego, w szczególności pod względem świadczenia i korzystania z transgranicznych i międzysektorowych usług publicznych i prywatnych opierających się na dostępności i korzystaniu z wysoce bezpiecznych i wiarygodnych rozwiązań w zakresie tożsamości elektronicznej. Cel ten wpisuje się w cele strategiczne określone w komunikacie zatytułowanym „Kształtowanie cyfrowej przyszłości Europy".

1.4.2. Cel(e) szczegółowy(e)

Cel szczegółowy nr 1

Zapewnienie dostępu do zaufanych i bezpiecznych rozwiązań w zakresie tożsamości cyfrowej, z których można korzystać w wymiarze transgranicznym, spełniających oczekiwania użytkowników i zapotrzebowanie rynku;

Cel szczegółowy nr 2

Zapewnienie, aby usługi publiczne i prywatne mogły opierać się na zaufanych i bezpiecznych rozwiązaniach w zakresie tożsamości cyfrowej;

Cel szczegółowy nr 3

Zapewnienie obywatelom pełnej kontroli nad ich danymi osobowymi i zagwarantowanie im bezpieczeństwa podczas korzystania z rozwiązań w zakresie tożsamości cyfrowej;

[28] O którym mowa w art. 58 ust. 2 lit. a) lub b) rozporządzenia finansowego.

Cel szczegółowy nr 4 Zapewnienie równych warunków świadczenia kwalifikowanych usług zaufania w UE oraz ich akceptacji.

1.4.3. Oczekiwane wyniki i wpływ

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

Ogólnie rzecz biorąc, największymi oczekiwanymi beneficjentami inicjatywy są użytkownicy końcowi/obywatele, dostawcy usług online, dostawcy aplikacji portfela oraz publiczni i prywatni dostawcy usług w zakresie tożsamości cyfrowej. Oczekuje się, że w ramach inicjatywy zapewniony zostanie dostęp do zaufanych i bezpiecznych rozwiązań w zakresie tożsamości cyfrowej, z których można korzystać w wymiarze transgranicznym, spełniających oczekiwania użytkowników i zapotrzebowanie rynku; zapewnienie, aby usługi publiczne i prywatne mogły opierać się na zaufanych i bezpiecznych rozwiązaniach w zakresie tożsamości cyfrowej w wymiarze transgranicznym; zapewnienie obywatelom pełnej kontroli nad ich danymi osobowymi i zagwarantowanie im bezpieczeństwo podczas korzystania z rozwiązań w zakresie tożsamości cyfrowej; zapewnienie równych warunków świadczenia kwalifikowanych usług zaufania w UE oraz ich akceptacji. Oprócz łatwości w dostępie do usług publicznych i prywatnych, obywatele i przedsiębiorstwa odniosą bezpośrednie korzyści z faktu, że interfejs służący do uwierzytelniania portfela będzie wygodny i łatwy w obsłudze, i będą w stanie przeprowadzać transakcje wymagające dowolnego poziomu bezpieczeństwa (np. od logowania w mediach społecznościowych po zastosowania związane z e-zdrowiem). Zastosowanie zaawansowanego podejścia uwzględniającego ochronę prywatności już w fazie projektowania przyniesie dodatkowe korzyści, ponieważ portfel nie będzie wymagał pośredników w procesie poświadczania atrybutów, dzięki czemu obywatele będą mogli się łączyć bezpośrednio z dostawcami usług i podmiotami wydającymi dane uwierzytelniające. Zwiększenie bezpieczeństwa danych w portfelu będzie zapobiegało kradzieży tożsamości, a tym samym stratom finansowym obywateli Unii i unijnych przedsiębiorstw. Jeżeli chodzi o wzrost gospodarczy, oczekuje się, że wprowadzenie systemu opartego na normach zmniejszy niepewność uczestników rynku i będzie miało pozytywny wpływ na innowacyjność. Co istotne, oczekuje się, że system ten zapewni bardziej inkluzywny dostęp do usług publicznych i prywatnych związanych z dobrami publicznymi, takimi jak edukacja i ochrona zdrowia, w których przypadku niektóre grupy społeczne napotykają obecnie pewne bariery. Niektórzy obywatele z niepełnosprawnościami, a przede wszystkim osoby o ograniczonej sprawności ruchowej lub mieszkające na obszarach wiejskich, mogą mieć na przykład mniejszy dostęp do usług, które zazwyczaj wymagają fizycznej obecności, jeśli w pobliżu nie ma odpowiedniej placówki.

1.4.4. Wskaźniki dotyczące realizacji celów

Należy wskazać wskaźniki stosowane do monitorowania postępów i osiągnięć.

Aspekt monitorowania i oceny oraz odpowiednie cele	Wskaźnik	Podmioty odpowiedzialne za gromadzenie informacji	Źródła

Stosowanie			
Zapewnienie dostępu do środków identyfikacji elektronicznej wszystkim obywatelom Unii	Liczba obywateli Unii i przedsiębiorstw unijnych, którym przyznano identyfikację elektroniczną w ramach notyfikowanych systemów/europejskie portfele tożsamości cyfrowej, oraz liczba wydanych poświadczeń tożsamości (poświadczeń atrybutów)	Komisja Europejska i właściwe organy krajowe	Ankieta roczna/dane dotyczące monitorowania i oceny gromadzone przez właściwe organy krajowe
Zapewnienie dostępu do środków identyfikacji elektronicznej wszystkim obywatelom Unii	Liczba obywateli Unii i przedsiębiorstw unijnych, którzy aktywnie korzystają z identyfikacji elektronicznej w ramach notyfikowanych systemów/europejskich portfeli tożsamości cyfrowej oraz poświadczeń tożsamości (poświadczeń atrybutów)	Komisja Europejska i właściwe organy krajowe	Ankieta roczna/dane dotyczące monitorowania i oceny gromadzone przez właściwe organy krajowe
Zwiększenie uznawania i akceptacji systemów identyfikacji elektronicznej w wymiarze transgranicznym, z myślą o doprowadzeniu do powszechnej akceptacji	Liczba dostawców usług online, którzy uznają identyfikację elektroniczną w ramach notyfikowanych systemów/europejskie portfele tożsamości cyfrowej oraz poświadczenia tożsamości (poświadczenia atrybutów)	Komisja Europejska	Ankieta roczna
Zwiększenie uznawania i akceptacji systemów identyfikacji elektronicznej w wymiarze transgranicznym, z myślą o doprowadzeniu do powszechnej akceptacji	Liczba transakcji online dokonywanych za pomocą identyfikacji elektronicznej w ramach notyfikowanych systemów/europejskich portfeli tożsamości cyfrowej oraz poświadczeń tożsamości (poświadczeń atrybutów) (łącznie oraz w wymiarze transgranicznym)	Komisja Europejska	Ankieta roczna
Zachęcanie sektora prywatnego do przyjęcia proponowanych rozwiązań i pobudzanie rozwoju nowych usług w zakresie tożsamości cyfrowej	Liczba nowych prywatnych usług poświadczania atrybutów spełniających normy wymagane do integracji z europejskim portfelem tożsamości cyfrowej	Komisja Europejska i właściwe organy krajowe	Ankieta roczna

Informacje kontekstowe			
Zachęcanie sektora prywatnego do przyjęcia proponowanych rozwiązań i pobudzanie rozwoju nowych usług w zakresie tożsamości cyfrowej	Wielkość rynku tożsamości cyfrowej	Komisja Europejska	Ankieta roczna
Zachęcanie sektora prywatnego do przyjęcia proponowanych rozwiązań i pobudzanie rozwoju nowych usług w zakresie tożsamości cyfrowej	Wydatki na zamówienia publiczne związane z tożsamością cyfrową	Komisja Europejska i właściwe organy krajowe	Ankieta roczna
Zwiększenie uznawania i akceptacji systemów identyfikacji elektronicznej w wymiarze transgranicznym, z myślą o doprowadzeniu do powszechnej akceptacji	Odsetek przedsiębiorstw prowadzących sprzedaż towarów lub usług za pośrednictwem handlu elektronicznego	Komisja Europejska	Eurostat
Zwiększenie uznawania i akceptacji systemów identyfikacji elektronicznej w wymiarze transgranicznym, z myślą o doprowadzeniu do powszechnej akceptacji	Udział transakcji internetowych wymagających silnego uwierzytelnienia klienta (ogółem)	Komisja Europejska	Ankieta roczna
Zapewnienie dostępu do środków identyfikacji elektronicznej wszystkim obywatelom Unii	Odsetek osób korzystających z handlu elektronicznego Odsetek osób korzystających z usług publicznych online	Komisja Europejska	Eurostat

1.5. Uzasadnienie wniosku/inicjatywy

1.5.1. Potrzeby, które należy zaspokoić w perspektywie krótko- lub długoterminowej, w tym szczegółowy terminarz przebiegu realizacji inicjatywy

Niniejsze rozporządzenie wiąże w całości i jest bezpośrednio stosowane we wszystkich państwach członkowskich. Państwa członkowskie będą zobowiązane do wprowadzenia europejskiego portfela tożsamości cyfrowej w terminie ok. 24–48 miesięcy od przyjęcia rozporządzenia. Komisja będzie uprawniona do przyjęcia aktów wykonawczych określających specyfikacje techniczne i normy referencyjne dotyczące architektury technicznej europejskich ram tożsamości cyfrowej w terminie ok. 12–24 miesięcy od przyjęcia rozporządzenia.

1.5.2. Wartość dodana z tytułu zaangażowania Unii Europejskiej (może wynikać z różnych czynników, na przykład korzyści koordynacyjnych, pewności prawa, większej efektywności lub komplementarności). Na potrzeby tego punktu „wartość dodaną z tytułu zaangażowania Unii" należy rozumieć jako wartość wynikającą z unijnej interwencji, wykraczającą poza wartość, która zostałaby wytworzona przez same państwa członkowskie.

Przyczyny działania na poziomie europejskim (*ex ante*)

Biorąc pod uwagę rosnące zapotrzebowanie ze strony obywateli, przedsiębiorstw i dostawców usług online na łatwe w obsłudze, bezpieczne i chroniące prywatność rozwiązania w zakresie tożsamości cyfrowej, które można stosować w wymiarze transgranicznym, dalsze działania na poziomie UE mogą przynieść większe korzyści niż działania podejmowane przez poszczególne państwa członkowskie, jak wykazano w ocenie rozporządzenia eIDAS.

Oczekiwana wygenerowana unijna wartość dodana (*ex post*)

Bardziej zharmonizowane podejście na poziomie UE, oparte na fundamentalnej zmianie polegającej na przejściu od polegania wyłącznie na rozwiązaniach w zakresie tożsamości cyfrowej do dostarczania elektronicznych poświadczeń atrybutów, zapewni obywatelom i przedsiębiorstwom dostęp do usług publicznych i prywatnych w dowolnym miejscu w UE za pomocą zweryfikowanych dowodów potwierdzających tożsamość i atrybutów. Dostawcy usług online będą mogli akceptować rozwiązania w zakresie tożsamości cyfrowej niezależnie od miejsca ich wystawienia, opierając się na wspólnym europejskim podejściu do kwestii zaufania, bezpieczeństwa i interoperacyjności. Zarówno użytkownicy, jak i dostawcy usług skorzystają również z przyznania elektronicznym poświadczeniom atrybutów takiej samej wartości prawnej w całej UE. co jest szczególnie istotne, gdy zachodzi konieczność prowadzenia działań w sposób skoordynowany, jak ma to na przykład miejsce w przypadku elektronicznych świadectw zdrowia. Również dostawcy usług zaufania zapewniające elektroniczne poświadczenia atrybutów skorzystają dzięki możliwości świadczenia usług na rynku europejskim. Na przykład koszty związane z zapewnieniem wysoce wiarygodnego i bezpiecznego środowiska świadczenia kwalifikowanych usług zaufania łatwiej zrównoważyć na szczeblu UE ze względu na korzyści skali. Tylko ramy unijne mogą w pełni zapewnić możliwość przenoszenia w wymiarze transgranicznym tożsamości prawnej i elektronicznego poświadczania atrybutów z nią związanych, uwiarygadniając poświadczenia tożsamości przedstawiane przez inne państwa członkowskie.

1.5.3. Główne wnioski wyciągnięte z podobnych działań

Rozporządzenie eIDAS (rozporządzenie (UE) nr 910/2014) stanowi jedyne transgraniczne ramy zaufanej identyfikacji elektronicznej osób fizycznych i prawnych oraz usług zaufania. Chociaż eIDAS odgrywa niekwestionowaną rolę na rynku wewnętrznym, od czasu przyjęcia rozporządzenia wiele się zmieniło. Przyjęte w 2014 r. rozporządzenie eIDAS opiera się na krajowych systemach identyfikacji elektronicznej, w których uwzględnia się różne normy i które koncentrują się na stosunkowo nieznacznej części potrzeb obywateli i przedsiębiorstw w zakresie identyfikacji elektronicznej: na bezpiecznym transgranicznym dostępie do usług publicznych. Przedmiotowe usługi dotyczą głównie 3 % ludności UE, która mieszka w państwie członkowskim innym niż państwo, w którym takie osoby się urodziły.

Od tamtego czasu transformacja cyfrowa gwałtownie przyspieszyła w zakresie wszystkich funkcji społeczeństwa. W szczególności do przyspieszenia procesu transformacji cyfrowej w bardzo dużej mierze przyczyniała się pandemia COVID-19. W rezultacie świadczenie usług publicznych i prywatnych w coraz większym stopniu odbywa się w przestrzeni cyfrowej. Obywatele i przedsiębiorstwa oczekują zapewnienia wysokiego poziomu bezpieczeństwa i wygody podczas dokonywania wszelkich czynności przeprowadzanych za pośrednictwem internetu, takich jak między innymi składanie deklaracji podatkowych, zapisywanie się na studia za granicą, zdalne otwieranie rachunku bankowego lub ubieganie się o pożyczkę, wynajem samochodu, zakładanie działalności gospodarczej w innym państwie członkowskim, uwierzytelnianie płatności online czy też składanie ofert w odpowiedzi na zaproszenie do składania ofert online.

W rezultacie drastycznie wzrosło zapotrzebowanie na środki identyfikacji i uwierzytelniania online, a także środki cyfrowej wymiany informacji związanych z tożsamością, atrybutami lub kwalifikacjami (tożsamość, adresy, wiek, ale również kwalifikacje zawodowe, prawa jazdy i inne zezwolenia i systemy płatności) w sposób bezpieczny i z zapewnieniem wysokiego stopnia ochrony danych.

Spowodowało to zmianę modelu działania w kierunku zaawansowanych i wygodnych rozwiązań, które umożliwiają integrację różnych możliwych do sprawdzenia danych i certyfikatów użytkownika. Użytkownicy oczekują środowiska, nad którym będą mieli kontrolę i za którego pomocą będzie można przesyłać i udostępniać różne rodzaje danych uwierzytelniających i atrybutów, takie jak np. krajowa identyfikacja elektroniczna, certyfikaty kompetencji zawodowych, bilety uprawniające do korzystania z transportu publicznego lub, w niektórych przypadkach, również elektroniczne bilety na koncerty. Są to tzw. portfele oparte na autonomii jednostki i oparte na aplikacjach, którymi użytkownik zarządza za pomocą urządzenia mobilnego i które umożliwiają mu bezpieczny i łatwy dostęp do różnych usług, zarówno publicznych, jak i prywatnych, oraz pełną kontrolę nad tym procesem.

1.5.4. Spójność z wieloletnimi ramami finansowymi oraz możliwa synergia z innymi właściwymi instrumentami

Inicjatywa wspiera europejskie działania na rzecz odbudowy, zapewniając obywatelom i przedsiębiorstwom niezbędne narzędzia – np. wygodną identyfikację elektroniczną i usługi zaufania – aby mogli wykonywać codzienne czynności w internecie przy użyciu zaufanych i bezpiecznych metod. W związku z tym inicjatywa jest w pełni zgodna z celami wieloletnich ram finansowych.

Wydatki operacyjne zostaną sfinansowane w ramach celu szczegółowego nr 5 programu „Cyfrowa Europa”. Szacuje się, że zamówienia publiczne związane z opracowaniem norm i specyfikacji technicznych, jak również koszty utrzymania modułów systemu identyfikacji elektronicznej i usług zaufania, wyniosą maksymalnie 3–4 mln EUR rocznie. Dokładny podział budżetowy w tym zakresie zostanie ustalony podczas przygotowywania przyszłych programów prac. Dotacje udzielane na potrzeby przyłączania usług publicznych i prywatnych do ekosystemu identyfikacji elektronicznej mogłyby bardzo pomóc w osiągnięciu celów wniosku. Koszt zintegrowania przez dostawcę usług niezbędnego interfejsu programowania aplikacji portfela identyfikacji elektronicznej szacuje się na około 25 000 EUR jednorazowego kosztu na dostawcę usług. Jeżeli będzie taka możliwość po rozpoczęciu rozmów na temat podziału budżetu w odniesieniu do kolejnego programu prac, budżet na dotacje w wysokości do 0,5 mln EUR na państwo członkowskie pomógłby w podłączeniu masy krytycznej usług.

Posiedzenia grupy ekspertów związane z opracowywaniem aktów wykonawczych obciążą część administracyjną programu „Cyfrowa Europa” na łączną kwotę do 0,5 mln EUR.

Synergie z innymi instrumentami

Inicjatywa stworzy ramy poświadczania tożsamości elektronicznej i świadczenia usług w zakresie tożsamości elektronicznej w UE, na których określone sektory będą mogły polegać w celu spełnienia określonych sektorowych wymogów prawnych, np. związanych z cyfrowymi dokumentami podróży, cyfrowymi prawami jazdy itp. Wniosek jest również zgodny z celami rozporządzenia (UE) 2019/1157, które jest poświęcone poprawie zabezpieczeń dowodów osobistych i dokumentów pobytu. Zgodnie z tym rozporządzeniem państwa członkowskie są zobowiązane do wprowadzenia do sierpnia 2021 r. nowych dowodów tożsamości ze zaktualizowanymi zabezpieczeniami. Po opracowaniu nowych dowodów tożsamości państwa członkowskie będą mogły je ulepszyć, aby można je było notyfikować jako systemy identyfikacji elektronicznej zgodnie z rozporządzeniem eIDAS.

W kontekście inicjatywy na rzecz stworzenia środowiska unijnego punktu kompleksowej obsługi na potrzeby celne niniejsza inicjatywa przyczyni się również do transformacji obszaru celnego w środowisko elektroniczne, w którym nie korzysta się z dokumentów w formie papierowej. Należy również zauważyć, że wniosek pomoże w realizacji europejskiej polityki mobilności, ponieważ ułatwi agentom morskim spełnienie wymogów prawnych w zakresie sprawozdawczości określonych w kontekście europejskiego systemu morskich pojedynczych punktów kontaktowych, który zacznie obowiązywać od dnia 15 sierpnia 2025 r. To samo dotyczy powiązania z rozporządzeniem w sprawie elektronicznych informacji dotyczących transportu towarowego, w którym zobowiązano organy państw członkowskich do przyjmowania elektronicznych informacji dotyczących transportu towarowego. Aplikacja europejskiego portfela tożsamości cyfrowej będzie również w stanie obsługiwać dane uwierzytelniające związane z kierowcami, pojazdami i operacjami wymagane w unijnych ramach prawnych w dziedzinie transportu drogowego (np. cyfrowe prawa jazdy / dyrektywa 2006/126/WE). Specyfikacje będą dalej rozwijane w kontekście tych ram. Inicjatywa może również pomóc w kształtowaniu przyszłych inicjatyw dotyczących koordynacji systemów zabezpieczenia społecznego, np. w ewentualnych pracach nad europejskim dowodem zabezpieczenia społecznego, który można by oprzeć na kotwicach zaufania

oferowanych przez systemy tożsamości notyfikowane zgodnie z rozporządzeniem eIDAS.

Inicjatywa wspiera wdrażanie RODO (2016/679), ponieważ daje użytkownikowi kontrolę nad sposobem wykorzystywania jego danych osobowych. Inicjatywa zapewnia wysoki poziom komplementarności z nowym aktem o cyberbezpieczeństwie i z określonymi w nim wspólnymi programami certyfikacji cyberbezpieczeństwa. Konieczność posiadania przez przedmioty należące do internetu rzeczy niepowtarzalnej tożsamości w ramach eIDAS zapewnia również spójność z aktem o cyberbezpieczeństwie oraz z potrzebą uwzględnienia szerszego zakresu podmiotów, niż osoby fizyczne i przedsiębiorstwa, np. maszyn, przedmiotów, dostawców i urządzeń internetu rzeczy.

Również rozporządzenie w sprawie jednolitego portalu cyfrowego posiada istotne elementy wspólne z niniejszą inicjatywą. Celem rozporządzenia w sprawie jednolitego portalu cyfrowego jest pełne unowocześnienie usług administracji publicznej oraz ułatwienie dostępu online do informacji, procedur administracyjnych i usług wsparcia, których potrzebują obywatele i przedsiębiorstwa mieszkający lub prowadzący działalność w innym państwie UE. Niniejsza inicjatywa zapewnia podstawowe elementy, które pomogą w realizacji celów dotyczących wprowadzenia zasady jednorazowości w ramach jednolitego portalu cyfrowego.

Inicjatywa jest również spójna z europejską strategią w zakresie danych i proponowanym rozporządzeniem w sprawie europejskiego zarządzania danymi, ponieważ zapewnia ramy sprzyjające wykorzystywaniu rozwiązań opartych na danych w przypadkach, gdy powstaje konieczność przekazania danych osobowych dotyczących tożsamości, dzięki czemu użytkownicy mają kontrolę i mogą działać przy zachowaniu pełnej anonimizacji.

1.5.5. Ocena różnych dostępnych możliwości finansowania, w tym zakresu przegrupowania środków

Inicjatywa będzie się opierać na modułach identyfikacji elektronicznej i usług zaufania, które opracowano w ramach instrumentu „Łącząc Europę” i które są włączane do programu „Cyfrowa Europa”.

Państwa członkowskie mogą ponadto wystąpić się o finansowanie na przygotowanie/modernizację niezbędnej infrastruktury w ramach Instrumentu na rzecz Odbudowy i Zwiększania Odporności.

1.6. Czas trwania i wpływ finansowy wniosku/inicjatywy

☐ **Ograniczony czas trwania**

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

☐ Okres trwania wpływu finansowego: od RRRR r. do RRRR r. w odniesieniu do środków na zobowiązania oraz od RRRR r. do RRRR r. w odniesieniu do środków na płatności.

☑ **Nieograniczony czas trwania**

Wprowadzenie w życie z okresem rozruchu od RRRR r. do RRRR r.,

po którym następuje faza operacyjna.

1.7. Planowane tryby zarządzania[29]

☑ **Bezpośrednie zarządzanie** przez Komisję

☑ w ramach jej służb, w tym za pośrednictwem jej pracowników w delegaturach Unii;

☐ przez agencje wykonawcze;

☐ **Zarządzanie dzielone** z państwami członkowskimi

☐ **Zarządzanie pośrednie** poprzez przekazanie zadań związanych z wykonaniem budżetu:

☐ państwom trzecim lub organom przez nie wyznaczonym;

☐ organizacjom międzynarodowym i ich agencjom (należy wyszczególnić);

☐ EBI oraz Europejskiemu Funduszowi Inwestycyjnemu;

☐ organom, o których mowa w art. 70 i 71 rozporządzenia finansowego;

☐ organom prawa publicznego;

☐ podmiotom podlegającym prawu prywatnemu, które świadczą usługi użyteczności publicznej, o ile zapewniają one odpowiednie gwarancje finansowe;

☐ podmiotom podlegającym prawu prywatnemu państwa członkowskiego, którym powierzono realizację partnerstwa publiczno-prywatnego oraz które zapewniają odpowiednie gwarancje finansowe;

☐ osobom odpowiedzialnym za wykonanie określonych działań w dziedzinie wspólnej polityki zagranicznej i bezpieczeństwa na mocy tytułu V Traktatu o Unii Europejskiej oraz określonym we właściwym podstawowym akcie prawnym.

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

Uwagi

[…]
[…]

[29] Wyjaśnienia dotyczące trybów zarządzania oraz odniesienia do rozporządzenia finansowego znajdują się na następującej stronie: https://myintracomm.ec.europa.eu/budgweb/EN/man/budgmanag/Pages/budgmanag.aspx

2. ŚRODKI ZARZĄDZANIA

2.1. Zasady nadzoru i sprawozdawczości

Określić częstotliwość i warunki

Pierwszy przegląd rozporządzenia odbędzie się dwa lata po rozpoczęciu pełnego stosowania, a następnie będzie się odbywać co cztery lata. Komisja musi przedstawić sprawozdanie z wyników Parlamentowi Europejskiemu i Radzie.

W kontekście stosowania środków państwa członkowskie gromadzą ponadto dane statystyczne dotyczące wykorzystywania i działania europejskich portfeli tożsamości cyfrowej i kwalifikowanych usług zaufania. Dane statystyczne zostają zebrane w sprawozdaniu, które jest corocznie przedkładane Komisji.

2.2. System zarządzania i kontroli

2.2.1. Uzasadnienie dla systemu zarządzania, mechanizmów finansowania wykonania, warunków płatności i proponowanej strategii kontroli

W rozporządzeniu ustanawia się bardziej zharmonizowane przepisy dotyczące poświadczania identyfikacji elektronicznej i świadczenia usług zaufania na rynku wewnętrznym przy jednoczesnym należytym uwzględnieniu zaufania i z poszanowaniem praw użytkowników dotyczących kontroli nad własnymi danymi. Te nowe przepisy wymagają opracowania specyfikacji i norm technicznych oraz nadzoru ze strony organów krajowych i koordynacji ich działań. Ponadto do zapewnienia odpowiednich modułów identyfikacji elektronicznej, podpisu elektronicznego itp. oraz zarządzania nimi zostanie wykorzystany program „Cyfrowa Europa". Należy również uwzględnić zasoby potrzebne do komunikacji z państwami trzecimi na temat wzajemnego uznawania usług zaufania i wynegocjowania z nimi porozumienia w tej sprawie.

Aby służby Komisji mogły sprostać tym zadaniom, należy im zapewnić odpowiednie zasoby. Szacuje się, że egzekwowanie nowego rozporządzenia będzie wymagało 11 EPC; 4–5 EPC na potrzeby prac dotyczących kwestii prawnych, 4–5 EPC na potrzeby prac technicznych oraz 2 EPC na potrzeby koordynacji, kontaktów międzynarodowych i wsparcia administracyjnego.

2.2.2. Informacje dotyczące zidentyfikowanego ryzyka i systemów kontroli wewnętrznej ustanowionych w celu jego ograniczenia

Jednym z głównych problemów leżących u źródła niedoskonałości obowiązujących ram legislacyjnych jest brak harmonizacji systemów krajowych. Aby przezwyciężyć ten problem w odniesieniu do przedmiotowej inicjatywy, działania będą w znacznym stopniu polegać na normach referencyjnych i specyfikacjach technicznych, które zostaną określone w aktach wykonawczych.

W opracowywaniu tych aktów wykonawczych Komisję będzie wspierać grupa ekspertów. Ponadto Komisja natychmiast rozpocznie wraz z państwami członkowskimi prace w celu uzgodnienia technicznego charakteru przyszłego systemu, aby zapobiec powstawaniu kolejnych rozbieżności podczas negocjacji na temat wniosku.

2.2.3. Oszacowanie i uzasadnienie efektywności kosztowej kontroli (relacja kosztów kontroli do wartości zarządzanych funduszy powiązanych) oraz ocena prawdopodobnego ryzyka błędu (przy płatności i przy zamykaniu)

Jeżeli chodzi o wydatki na posiedzenia grupy ekspertów, biorąc pod uwagę niską wartość pojedynczej transakcji (np. zwrot kosztów podróży dla delegata uczestniczącego w posiedzeniu, jeżeli jest to posiedzenie fizyczne), standardowe procedury kontroli wewnętrznej wydają się wystarczające.

Również w przypadku projektów pilotażowych, które mają być realizowane w ramach programu „Cyfrowa Europa", zwykłe standardowe procedury DG ds. Sieci Komunikacyjnych, Treści i Technologii powinny wystarczyć.

2.3. Środki zapobiegania nadużyciom finansowym i nieprawidłowościom

Określić istniejące lub przewidywane środki zapobiegania i ochrony, np. ze strategii zwalczania nadużyć finansowych.

Dodatkowe potrzeby w zakresie środków niezbędnych do celów niniejszego rozporządzenia zostaną zaspokojone w ramach istniejących środków zapobiegania nadużyciom finansowym mających zastosowanie do Komisji.

3. SZACUNKOWY WPŁYW FINANSOWY WNIOSKU/INICJATYWY

3.1. Działy wieloletnich ram finansowych i linie budżetowe po stronie wydatków, na które wniosek/inicjatywa ma wpływ

Istniejące linie budżetowe

Według działów wieloletnich ram finansowych i linii budżetowych

Dział wieloletnich ram finansowych	Linia budżetowa	Rodzaj środków	Wkład			
	Numer	Zróżn./ niezróżn.[30]	państw EFTA[31]	krajów kandydujących[32]	państw trzecich	w rozumieniu art. 21 ust. 2 lit. b) rozporządzenia finansowego
2	02 04 05 01 (w delegaturach)	Zróżn.	TAK	NIE	NIE	NIE
2	02 01 30 01 Wydatki na wsparcie dotyczące programu „Cyfrowa Europa”	Niezróżn.				
7	20 02 06 Wydatki administracyjne	Niezróżn.	NIE			

Proponowane nowe linie budżetowe

Według działów wieloletnich ram finansowych i linii budżetowych

Dział wieloletnich ram finansowych	Linia budżetowa	Rodzaj środków	Wkład			
	Numer	Zróżn./ niezróżn.	państw EFTA	krajów kandydujących	państw trzecich	w rozumieniu art. 21 ust. 2 lit. b) rozporządzenia finansowego
	[XX.YY.YY.YY]		TAK/ NIE	TAK/ NIE	TAK/ NIE	TAK/ NIE

30 Środki zróżnicowane/środki niezróżnicowane

31 EFTA: Europejskie Stowarzyszenie Wolnego Handlu.

32 Kraje kandydujące oraz w stosownych przypadkach potencjalne kraje kandydujące Bałkanów Zachodnich.

3.2. Szacunkowy wpływ finansowy wniosku na środki

3.2.1. Podsumowanie szacunkowego wpływu 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:

w mln EUR (do trzech miejsc po przecinku)

Dział wieloletnich ram finansowych	Numer	2

Dyrekcja Generalna: CNECT			Rok **2022**	Rok **2023**	Rok **2024**	Rok **2025**	Rok **2026**	Rok **2027**		**OGÓŁEM**
○ Środki operacyjne				Podział środków budżetowych zostanie określony podczas opracowywania programów prac. Podane liczby oznaczają minimalną kwotę potrzebną do utrzymania i modernizacji[33].						
Linia budżetowa[34] 02 04 05	Środki na zobowiązania	(1a)	2,000	4,000	4,000	4,000	4,000	4,000		**22,000**
	Środki na płatności	(2a)	1,000	3,000	4,000	4,000	4,000	4,000	2,000	**22,000**
Linia budżetowa	Środki na zobowiązania	(1b)								
	Środki na płatności	(2b)								
Środki administracyjne finansowane ze środków przydzielonych na określone programy[35]										
Linia budżetowa 02 01 03 01		(3)	**0,048**	**0,144**	**0,144**	**0,072**	**0,072**	**0,072**		**0,552**

33 Jeżeli faktyczne koszty przekroczą podane kwoty, zostaną one pokryte w ramach 02 04 05 01.

34 Zgodnie z oficjalną nomenklaturą budżetową.

35 Wsparcie techniczne lub administracyjne oraz wydatki na wsparcie realizacji programów lub działań UE (dawne linie „BA"), pośrednie badania naukowe, bezpośrednie badania naukowe.

OGÓŁEM środki na rzecz DG CNECT	Środki na zobowiązania	=1a+1b +3	2,048	4,144	4,144	4,072	4,072	**4,072**		**22,552**
	Środki na płatności	=2a+2b +3	1,048	3,144	4,144	4,072	4,072	**4,072**	**2,000**	**22,552**

○ OGÓŁEM środki operacyjne	Środki na zobowiązania	(4)	2,000	4,000	4,000	4,000	4,000	4,000		**22,000**
	Środki na płatności	(5)	1,000	3,000	4,000	4,000	4,000	4,000	2,000	**22,000**
○ OGÓŁEM środki administracyjne finansowane ze środków przydzielonych na określone programy		(6)	**0,048**	**0,144**	**0,144**	**0,072**	**0,072**	**0,072**		**0,552**
OGÓŁEM środki na DZIAŁ 2 wieloletnich ram finansowych	Środki na zobowiązania	=4 + 6	2,048	4,144	4,144	4,072	4,072	**4,072**		**22,552**
	Środki na płatności	=5 + 6	0,048	4,144	4,144	4,072	4,072	**4,072**	**2,000**	**22,552**

Dział wieloletnich ram finansowych	**7**	„Wydatki administracyjne”

Niniejszą część uzupełnia się przy użyciu „danych budżetowych o charakterze administracyjnym”, które należy najpierw wprowadzić do załącznika do oceny skutków finansowych regulacji (załącznika V do zasad wewnętrznych), przesyłanego do DECIDE w celu konsultacji między służbami.

w mln EUR (do trzech miejsc po przecinku)

		Rok **2022**	Rok **2023**	Rok **2024**	Rok **2025**	Rok **2026**	Rok **2027**	**OGÓŁEM**
Dyrekcja Generalna: CNECT								
○ Zasoby ludzkie		0,776	1,470	1,470	1,470	1,470	1,318	**7,974**
○ Pozostałe wydatki administracyjne		0,006	0,087	0,087	0,087	0,016	0,016	**0,299**
OGÓŁEM Dyrekcja Generalna CNECT	Środki	0,782	1,557	1,557	1,557	1,486	1,334	**8,273**

OGÓŁEM środki na DZIAŁ 7 wieloletnich ram finansowych	(Środki na zobowiązania ogółem = środki na płatności ogółem)	0,782	1,557	1,557	1,557	1,486	1,334	**8,273**

w mln EUR (do trzech miejsc po przecinku)

		Rok **2022**	Rok **2023**	Rok **2024**	Rok **2025**	Rok **2026**	Rok **2027**		**OGÓŁEM**
OGÓŁEM środki na DZIAŁY od 1 do 7 wieloletnich ram finansowych	Środki na zobowiązania	2,830	5,701	5,701	5,629	5,558	5,408		**30,825**
	Środki na płatności	1,830	4,701	5,701	5,629	5,558	5,406	2,000	**30,825**

3.2.2. Przewidywany produkt finansowany ze środków operacyjnych

Środki na zobowiązania w mln EUR (do trzech miejsc po przecinku)

Określić cele i produkty ⇩			Rok **2022**		Rok **2023**		Rok **2024**		Rok **2025**		Rok **2026**		Rok **2027**		**OGÓŁEM**	
	Rodzaj[36]	Średni koszt	Liczba	Koszt	Liczba	Koszt	Liczba	Koszt	Liczba	Koszt	Liczba	Koszt	Liczba	Koszt	Liczba ogółem	Koszt całkowity
CEL SZCZEGÓŁOWY nr 1[37]	Zapewnienie dostępu do zaufanych i bezpiecznych rozwiązań w zakresie tożsamości cyfrowej, z których można korzystać w wymiarze transgranicznym, spełniających oczekiwania użytkowników i zapotrzebowanie rynku															
Ankiety/badania roczne			1	0,050	1	0,050	1	0,050	1	0,050	1	0,050	1	0,050	6	0,300
Cel szczegółowy nr 1 – suma cząstkowa			1	0,050	1	0,050	1	0,050	1	0,050	1	0,050	1	0,050	6	0,300
CEL SZCZEGÓŁOWY nr 2	Zapewnienie, aby usługi publiczne i prywatne mogły opierać się na zaufanych i bezpiecznych rozwiązaniach w zakresie tożsamości cyfrowej															
Ankiety/badania			1	0,050	1	0,050	1	0,050	1	0,050	1	0,050	1	0,050	6	0,300
Cel szczegółowy nr 2 – suma cząstkowa			1	0,050	1	0,050	1	0,050	1	0,050	1	0,050	1	0,050	6	0,300
CEL SZCZEGÓŁOWY nr 3	Zapewnienie obywatelom pełnej kontroli nad ich danymi osobowymi i zagwarantowanie im bezpieczeństwa podczas korzystania z rozwiązań w zakresie tożsamości cyfrowej															
Ankiety/badania			1	0,050	1	0,050	1	0,050	1	0,050	1	0,050	1	0,050	6	0,300
Cel szczegółowy nr 3 – suma cząstkowa			1	0,050	1	0,050	1	0,050	1	0,050	1	0,050	1	0,050	6	0,300

[36] Produkty odnoszą się do produktów i usług, które zostaną zapewnione (np. liczba sfinansowanych wymian studentów, liczba kilometrów zbudowanych dróg itp.).

[37] Zgodnie z opisem w pkt 1.4.2. „Cel(e) szczegółowy(e) …”.

CEL SZCZEGÓŁOWY nr 4			Zapewnienie równych warunków świadczenia kwalifikowanych usług zaufania w UE oraz ich akceptacji.													
Ankiety/badania			1	0,050	1	0,050	1	0,050	1	0,050	1	0,050	1	0,050	6	0,300
Cel szczegółowy nr 4 – suma cząstkowa			1	0,050	1	0,050	1	0,050	1	0,050	1	0,050	1	0,050	6	0,300
OGÓŁEM			4	0,200	4	0,200	4	0,200	4	0,200	4	0,200	4	0,200	24	1,200

3.2.3. Podsumowanie szacunkowego wpływu na środki administracyjne

☐ 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 trzech miejsc po przecinku)

	Rok **2022**	Rok **2023**	Rok **2024**	Rok **2025**	Rok **2026**	Rok **2027**	**OGÓŁEM**
DZIAŁ 7 wieloletnich ram finansowych							
Zasoby ludzkie	0,776	1,470	1,470	1,470	1,470	1,318	**7,974**
Pozostałe wydatki administracyjne	0,006	0,087	0,087	0,087	0,0162	0,0162	**0,299**
Suma cząstkowa DZIAŁU 7 wieloletnich ram finansowych	0,782	1,557	1,557	1,557	1,486	1,334	**8,273**

Poza DZIAŁEM 7[38] **wieloletnich ram finansowych**							
Zasoby ludzkie							
Pozostałe wydatki o charakterze administracyjnym Koszty administracyjne należy pokryć w ramach programu „Cyfrowa Europa”	0,048	0,144	0,144	0,072	0,072	**0,072**	**0,552**
Suma cząstkowa poza DZIAŁEM 7 wieloletnich ram finansowych	0,048	0,144	0,144	0,072	0,072	**0,072**	**0,552**

OGÓŁEM	**0,830**	**1,701**	**1,701**	**1,629**	**1,558**	**1,406**	**8,825**

Potrzeby w zakresie środków na zasoby ludzkie i inne wydatki o charakterze administracyjnym zostaną pokryte z zasobów dyrekcji generalnej 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.

[38] Wsparcie techniczne lub administracyjne oraz wydatki na wsparcie realizacji programów lub działań UE (dawne linie „BA”), pośrednie badania naukowe, bezpośrednie badania naukowe.

3.2.4. 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 ekwiwalentach pełnego czasu pracy

		Rok **2022**	Rok **2023**	Rok **2024**	Rok **2025**	Rok **2026**	Rok **2027**
20 01 02 01 (w centrali i w biurach przedstawicielstw Komisji)		4	8	8	8	8	7
20 01 02 03 (w delegaturach)							
01 01 01 01 (pośrednie badania naukowe)							
01 01 01 11 (bezpośrednie badania naukowe)							
Inna linia budżetowa (określić)							
20 02 01 (CA, SNE, INT z globalnej koperty finansowej)		2	3	3	3	3	3
20 02 03 (CA, LA, SNE, INT i JPD w delegaturach)							
XX 01 xx **yy** zz[39]	– w centrali						
	– w delegaturach						
01 01 01 02 (CA, SNE, INT – pośrednie badania naukowe)							
01 01 01 12 (CA, INT, SNE – bezpośrednie badania naukowe)							
Inna linia budżetowa (określić)							
OGÓŁEM		**6**	**11**	**11**	**11**	**11**	**10**

XX oznacza odpowiedni obszar polityki lub odpowiedni tytuł w budżecie.

Potrzeby w zakresie zasobów ludzkich zostaną pokryte z zasobów dyrekcji generalnej 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	Urzędnicy będą głównie prowadzić prace dotyczące kwestii prawnych, działania koordynacyjne oraz negocjacje z państwami trzecimi i podmiotami związanymi z wzajemnym uznawaniem usług zaufania.
Personel zewnętrzny	Eksperci krajowi powinni udzielić wsparcia w technicznym i funkcjonalnym przygotowaniu systemu. W realizacji zadań technicznych powinien pomóc również personel kontraktowy, w tym w zarządzaniu modułami.

[39] W ramach podpułapu na personel zewnętrzny ze środków operacyjnych (dawne linie „BA").

3.2.5. Zgodność z obowiązującymi wieloletnimi ramami finansowymi

Wniosek/inicjatywa:

☑ może zostać w pełni sfinansowany(a) przez przegrupowanie środków w ramach odpowiedniego działu wieloletnich ram finansowych (WRF).

Należy wyjaśnić, na czym ma polegać przeprogramowanie, określając linie budżetowe, których ma ono dotyczyć, oraz podając odpowiednie kwoty. W przypadku znacznego przeprogramowania należy załączyć arkusz kalkulacyjny.

☐ wymaga zastosowania nieprzydzielonego marginesu środków w ramach odpowiedniego działu WRF lub zastosowania specjalnych instrumentów zdefiniowanych w rozporządzeniu w sprawie WRF.

Należy wyjaśnić, który wariant jest konieczny, określając działy i linie budżetowe, których ma dotyczyć, odpowiadające im kwoty oraz proponowane instrumenty, które należy zastosować.

☐ wymaga rewizji WRF.

Należy wyjaśnić, który wariant jest konieczny, określając linie budżetowe, których ma on dotyczyć, oraz podając odpowiednie kwoty.

3.2.6. Udział osób trzecich w finansowaniu

Wniosek/inicjatywa:

☑ nie przewiduje współfinansowania ze strony osób trzecich

☐ przewiduje współfinansowanie ze strony osób trzecich szacowane zgodnie z poniższymi szacunkami:

środki w mln EUR (do trzech miejsc po przecinku)

	Rok **N**[40]	Rok **N+1**	Rok **N+2**	Rok **N+3**	Wprowadzić taką liczbę kolumn dla poszczególnych lat, jaka jest niezbędna, by odzwierciedlić cały okres wpływu (por. pkt 1.6)			Ogółem
Określić organ współfinansujący								
OGÓŁEM środki objęte współfinansowaniem								

[40] Rok N jest rokiem, w którym rozpoczyna się realizację wniosku/inicjatywy. „N" należy zastąpić oczekiwanym pierwszym rokiem realizacji (np.: 2021). Tak samo należy postąpić dla kolejnych lat.

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 inne

Wskazać, czy dochody są przypisane do linii budżetowej po stronie wydatków☐

w mln EUR (do trzech miejsc po przecinku)

Linia budżetowa po stronie dochodów	Środki zapisane w budżecie na bieżący rok budżetowy	Wpływ wniosku/inicjatywy[41]						
		Rok **N**	Rok **N+1**	Rok **N+2**	Rok **N+3**	Wprowadzić taką liczbę kolumn dla poszczególnych lat, jaka jest niezbędna, by odzwierciedlić cały okres wpływu (por. pkt 1.6)		
Artykuł …								

W przypadku wpływu na dochody przeznaczone na określony cel należy wskazać linie budżetowe po stronie wydatków, które ten wpływ obejmie.

[…]

Pozostałe uwagi (np. metoda/wzór użyte do obliczenia wpływu na dochody albo inne informacje).

[…]

[41] W przypadku tradycyjnych zasobów własnych (opłaty celne, opłaty wyrównawcze od cukru) należy wskazać kwoty netto, tzn. kwoty brutto po odliczeniu 20 % na poczet kosztów poboru.

ZAŁĄCZNIK
do OCENY SKUTKÓW FINANSOWYCH REGULACJI

Tytuł wniosku/inicjatywy:

Wniosek dotyczący rozporządzenia w sprawie ram europejskiej tożsamości cyfrowej, zmieniającego rozporządzenie eIDAS

1. LICZBA I KOSZT ZASOBÓW LUDZKICH UZNANYCH ZA NIEZBĘDNE

2. KOSZT POZOSTAŁYCH WYDATKÓW ADMINISTRACYJNYCH

3. ŁĄCZNE KOSZTY ADMINISTRACYJNE

4. METODY OBLICZANIA SZACUNKOWYCH KOSZTÓW

4.1. Zasoby ludzkie

4.2. Pozostałe wydatki administracyjne

Niniejszy załącznik musi towarzyszyć ocenie skutków finansowych regulacji podczas konsultacji między służbami.

Tabele danych są wykorzystywane jako materiał wyjściowy dla tabel zawartych w ocenie skutków finansowych regulacji. Służą one wyłącznie do użytku wewnętrznego w Komisji.

1) Koszt zasobów ludzkich uznanych za niezbędne

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

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

w mln EUR (do trzech miejsc po przecinku)

HEADING 7 of the multiannual financial framework		Year 2022		Year 2023		Year 2024		Year 2025		Year 2026		Year 2027		TOTAL	
		FTE	Appropriations	FTE	Appropriations	FTE	Appropriations	FTE	Appropriations	FTE	Appropriations	FTE	Appropriations	FTE	Appropriations
• Establishment plan posts (officials and temporary staff)															
20 01 02 01 - Headquarters and Representation offices	AD	4	608	7	1.064	7	1.064	7	1.064	7	1.064	6	912	38	5.776
	AST	0	-	1	152	1	152	1	152	1	152	1	152	5	760
20 01 02 03 - Union Delegations	AD														
	AST														
External staff [1]															
20 02 01 and 20 02 02 – External personnel – Headquarters and Representation offices	AC	1	82	1	82	1	82	1	82	1	82	1	82	6	492
	END	1	86	2	172	2	172	2	172	2	172	2	172	11	946
	INT														
20 02 03 – External personnel - Union Delegations	AC														
	AL														
	END														
	INT														
	JPD														
Other HR related budget lines (*specify*)															
Subtotal HR – HEADING 7		6	776	11	1.470	11	1.470	11	1.470	11	1.470	10	1.318	60	7.974

4.3. Potrzeby w zakresie zasobów ludzkich zostaną pokryte z zasobów dyrekcji generalnej 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.

4.4.

4.5.

Poza DZIAŁEM 7 wieloletnich ram finansowych		**Rok 2022**		**Rok 2023**		**Rok 2024**		**Rok 2025**		**Rok 2026**		**Rok 2027**		**OGÓŁEM**	
		EPC	Środki	EPC	Środki	EPC	Środki	EPC	Środki	EPC	Środki	EPC	Środki	EPC	Środki
01 01 01 01 Pośrednie badania naukowe[42] 01 01 01 11 Bezpośrednie badania naukowe Inne (proszę określić)	AD														
	AST														
Personel zewnętrzny w ramach środków operacyjnych (dawne linie „BA”).	– w centrali	CA													
		SNE													
		INT													
	– w delegaturach Unii	CA													
		LA													
		SNE													
		INT													
		JPD													
01 01 01 02 Pośrednie badania naukowe 01 01 01 12 Bezpośrednie badania naukowe Inne (proszę określić)[43]	CA														
	SNE														
	INT														
Inne linie budżetowe związane z HR (*proszę określić*)															

[42] Należy wybrać odpowiednią linię budżetową lub w razie potrzeby wskazać inną; jeżeli sprawa dotyczy większej liczby linii budżetowych, należy podzielić personel według odpowiednich linii budżetowych.

[43] Należy wybrać odpowiednią linię budżetową lub w razie potrzeby wskazać inną; jeżeli sprawa dotyczy większej liczby linii budżetowych, należy podzielić personel według odpowiednich linii budżetowych.

Suma cząstkowa dotycząca HR – Poza DZIAŁEM 7															
HR ogółem (wszystkie działy WRF)		6	0,776	11	1,470	11	1,470	11	1,470	11	1,470	10	1,318	60	7,974

Potrzeby w zakresie zasobów ludzkich zostaną pokryte z zasobów dyrekcji generalnej 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.

4.6. Koszt pozostałych wydatków administracyjnych

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

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

w mln EUR (do trzech miejsc po przecinku)

DZIAŁ 7 wieloletnich ram finansowych	Rok 2022	Rok 2023	Rok 2024	Rok 2025	Rok 2026	Rok 2027	Ogółem
W centrali lub na terytorium UE:							
20 02 06 01 – Wydatki na podróże służbowe i cele reprezentacyjne	0,006	0,015	0,015	0,015	0,015	0,015	**0,081**
20 02 06 02 – Koszty konferencji i spotkań							
20 02 06 03 – Komitety[44]		0,072	0,072	0,072	0,0012	0,012	**0,218**
20 02 06 04 Badania i konsultacje							
20 04 – Wydatki na IT (zarządzane przez Komisję)[45]							
Inne linie budżetowe niezwiązane z HR (*określić w stosownych przypadkach*)							
W delegaturach Unii							
20 02 07 01 – Wydatki na podróże służbowe, konferencje i cele reprezentacyjne							
20 02 07 02 – Szkolenia specjalistyczne personelu							
20 03 05 – Infrastruktura i logistyka							
Inne linie budżetowe niezwiązane z HR (*określić w stosownych przypadkach*)							
Suma cząstkowa, Inne – DZIAŁ 7 wieloletnich ram finansowych	0,006	0,087	0,087	0,087	0,016	0,016	**0,299**

[44] Należy określić rodzaj komitetu i grupę, do której należy.

[45] Należy zasięgnąć opinii zespołu ds. inwestycji informatycznych DG DIGIT (zob. wytyczne w sprawie finansowania technologii informatycznych, C(2020) 6126 final z 10.9.2020, s. 7).

w mln EUR (do trzech miejsc po przecinku)

Poza DZIAŁEM 7 wieloletnich ram finansowych	**Rok 2022**	**Rok 2023**	**Rok 2024**	**Rok 2025**	**Rok 2026**	**Rok 2027**	**Ogółem**
Wydatki na pomoc techniczną i administracyjną (oprócz personelu zewnętrznego) ze środków operacyjnych (dawne linie „BA"):	0,048	0,144	0,144	0,072	0,072	0,072	**0,552**
– w centrali							
– w delegaturach Unii							
Inne wydatki na zarządzanie programami w zakresie badań naukowych							
Wydatki na IT wynikające z realizacji polityki tytułem programów operacyjnych[46]							
Wydatki na IT zarządzane przez Komisję tytułem programów operacyjnych[47]							
Inne linie budżetowe niezwiązane z HR (*określić w stosownych przypadkach*)							
Suma cząstkowa, Inne – Poza DZIAŁEM 7 wieloletnich ram finansowych	0,048	0,144	0,144	0,072	0,072	0,072	**0,552**
Inne wydatki administracyjne ogółem (wszystkie działy WRF)	0,054	0,231	0,231	0,159	0,088	0,088	0,851

[46] Należy zasięgnąć opinii zespołu ds. inwestycji informatycznych DG DIGIT (zob. wytyczne w sprawie finansowania technologii informatycznych, C(2020) 6126 final z 10.9.2020, s. 7).

[47] Pozycja ta obejmuje lokalne systemy administracyjne i wkłady na rzecz współfinansowania systemów informatycznych zarządzanych przez Komisję (zob. wytyczne w sprawie finansowania technologii informatycznych, C(2020) 6126 final z 10.9.2020).

5. KOSZTY ADMINISTRACYJNE OGÓŁEM (WSZYSTKIE DZIAŁY WRF)

w mln EUR (do trzech miejsc po przecinku)

Streszczenie	Rok 2022	Rok 2023	Rok 2024	Rok 2025	Rok 2026	Rok 2027	Ogółem
Dział 7 – Zasoby ludzkie	0,776	1,470	1,470	1,470	1,470	1,318	**7,974**
Dział 7 – Inne wydatki administracyjne	0,006	0,087	0,087	0,087	0,016	0,016	**0,218**
Suma cząstkowa działu 7							
Poza działem 7 – Zasoby ludzkie							
Poza działem 7 – Inne wydatki administracyjne	0,048	0,144	0,144	0,072	0,072	0,072	**0,552**
Suma cząstkowa innych działów							
1. OGÓŁEM **2. DZIAŁ 7 i poza DZIAŁEM 7**	0,830	1,701	1,701	1,629	1,558	1,406	**8,825**

1) Potrzeby w zakresie środków administracyjnych zostaną pokryte ze środków już przydzielonych na zarządzanie tym działaniem lub przesuniętych, 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.

6. METODY OBLICZANIA SZACUNKOWYCH KOSZTÓW

a) Zasoby ludzkie

W niniejszej części określono metodę obliczania szacunkowych kosztów zasobów ludzkich uznanych za niezbędne (założenia co do obciążenia pracą, w tym konkretne stanowiska pracy (profile zawodowe wg Sysper 2), kategorie personelu i odpowiadające im średnie koszty)

1. DZIAŁ 7 wieloletnich ram finansowych
2. Uwaga: średnie koszty dla poszczególnych kategorii pracowników w centrali są dostępne na stronie BudgWeb: 3. https://myintracomm.ec.europa.eu/budgweb/EN/pre/legalbasis/Pages/pre-040-020_preparation.aspx
4. O Urzędnicy i pracownicy zatrudnieni na czas określony 5. 7 urzędników z grupy funkcyjnej AD (w tym 1 z CNECT/F.3 w latach 2023–2024) x 152 000 EUR/rok w latach 2023–2027 (w 2022 r. połowa, ponieważ spodziewany termin przyjęcia to połowa 2022 r.) 6. 1 urzędnik z grupy funkcyjnej AST x 152 000 EUR/rok w latach 2023–2027 (w 2022 r. połowa, ponieważ spodziewany termin przyjęcia to połowa 2022 r.) 7.
8. O Personel zewnętrzny 9. CA: 1 x 82 000 EUR/rok w latach 2023–2027 (w 2022 r. połowa, ponieważ spodziewany termin przyjęcia to połowa 2022 r.) (zastosowano współczynnik indeksacji) 10. SNE 2 x 86 000 EUR/rok w latach 2023–2027 (w 2022 r. połowa, ponieważ spodziewany termin przyjęcia to połowa 2022 r.) (zastosowano współczynnik indeksacji) 11.

12. Poza DZIAŁEM 7 wieloletnich ram finansowych
13. O Jedynie stanowiska finansowane z budżetu na badania naukowe 14.
15. O Personel zewnętrzny 16.

7. POZOSTAŁE WYDATKI ADMINISTRACYJNE

Należy wskazać metodę obliczeń zastosowaną w odniesieniu do poszczególnych linii budżetowych, a w szczególności założenia będące podstawą obliczeń (np. liczba posiedzeń rocznie, średnie koszty itp.)

17. DZIAŁ 7 wieloletnich ram finansowych
18. Posiedzenia komitetu co dwa miesiące x 12 000 EUR/posiedzenie w latach 2022–2024 na potrzeby przyjęcia aktów wykonawczych. Następnie coroczne posiedzenia komitetu na potrzeby przyjęcia zaktualizowanych aktów wykonawczych. 19. Podróże służbowe obejmują głównie podróże na trasie Luksemburg–Bruksela, ale także udział w konferencjach, spotkaniach z przedstawicielami państw członkowskich i z innymi zainteresowanymi stronami. 20.

21. **Poza DZIAŁEM 7** wieloletnich ram finansowych
22. Posiedzenia grupy ekspertów zostaną sfinansowane z linii administracyjnej programu „Cyfrowa Europa”.
23. Według założeń podczas przygotowywania aktu wykonawczego (od połowy 2022 r. do 2024 r.) posiedzenia grupy będą się odbywać co miesiąc (12 000 EUR), a poza tym okresem przewiduje się posiedzenia co dwa miesiące, aby zapewnić ogólnounijną koordynację działań związanych z wdrożeniem technicznym.
24.