KOMISJA
EUROPEJSKA

Bruksela, dnia 3.6.2021 r.
COM(2021) 290 final

SPRAWOZDANIE KOMISJI DLA PARLAMENTU EUROPEJSKIEGO I RADY

w sprawie oceny rozporządzenia (UE) nr 910/2014 w sprawie identyfikacji elektronicznej i usług zaufania w odniesieniu do transakcji elektronicznych na rynku wewnętrznym (rozporządzenie eIDAS)

{SEC(2021) 229 final} - {SWD(2021) 130 final}

1. WPROWADZENIE

W niniejszym sprawozdaniu przedstawiono wyniki oceny rozporządzenia (UE) nr 910/2014 w sprawie identyfikacji elektronicznej i usług zaufania w odniesieniu do transakcji elektronicznych na rynku wewnętrznym („rozporządzenie eIDAS")[1]. Zgodnie z art. 49 rozporządzenia Komisja musi dokonać przeglądu stosowania tego rozporządzenia i ocenić w szczególności, czy należy zmienić zakres jego stosowania lub zakres stosowania jego poszczególnych przepisów, biorąc pod uwagę doświadczenia zdobyte przy stosowaniu tego rozporządzenia, a także rozwój technologiczny, sytuację rynkową i prawną[2], a ponadto do sprawozdania należy załączyć w stosownych przypadkach wnioski ustawodawcze.

Towarzyszący niniejszemu sprawozdaniu dokument roboczy służb Komisji zawiera bardziej szczegółowe dane i analizę na poparcie tych ustaleń.

1.1. Ramy eIDAS

Przyjmując w 2014 r. rozporządzenie eIDAS, UE otworzyła nowe możliwości, ponieważ wprowadziła pierwsze transgraniczne ramy dla wiarygodnej tożsamości cyfrowej i usług zaufania, które to ramy obecnie są uznane i przestrzegane na całym świecie. Rozporządzenie eIDAS miało umożliwić wszystkim obywatelom Unii uzyskanie dostępu do usług publicznych w całej UE przy użyciu środków identyfikacji elektronicznej wydawanych w kraju pochodzenia. Celem tego rozporządzenia było zwiększenie zaufania do transakcji elektronicznych na rynku wewnętrznym poprzez zapewnienie wspólnej podstawy bezpiecznej i ciągłej interakcji elektronicznej między obywatelami, przedsiębiorstwami i organami publicznymi, co pozwoli podnieść efektywność publicznych i prywatnych usług online, e-biznesu i e-handlu w Unii. Rozporządzeniem tym uchylono dyrektywę 1999/93/WE w sprawie wspólnotowych ram w zakresie podpisów elektronicznych, która zasadniczo dotyczyła wyłącznie podpisów elektronicznych.

Jak wynika z podstawy prawnej tego rozporządzenia, czyli art. 114 TFUE, służyło ono zniesieniu istniejących barier w funkcjonowaniu rynku wewnętrznego poprzez promowanie zbliżenia przepisów państw członkowskich, w szczególności w zakresie wzajemnego uznawania i akceptacji identyfikacji elektronicznej, uwierzytelnienia, podpisów i powiązanych usług zaufania ponad granicami, gdy są to elementy niezbędne do uzyskania dostępu do procedur lub transakcji elektronicznych oraz do ich przeprowadzenia.

Zanim rozporządzenie to weszło w życie, nie istniały żadne kompleksowe unijne ramy transgraniczne i międzysektorowe, które pozwoliłyby na bezpieczne, wiarygodne i łatwe w użyciu transakcje elektroniczne i obejmowałyby identyfikację elektroniczną,

---

[1] Rozporządzenie Parlamentu Europejskiego i Rady (UE) 910/2014 z dnia 23 lipca 2014 r. w sprawie identyfikacji elektronicznej i usług zaufania w odniesieniu do transakcji elektronicznych na rynku wewnętrznym oraz uchylające dyrektywę 1999/93/WE, *Dz.U. L 257*, http://eur-lex.europa.eu/legal-content/PL/TXT/PDF/?uri=CELEX:32014R0910&from=EN

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

uwierzytelnienie i usługi zaufania. We wniosku Komisji (COM(2012) 238 final) z dnia 4 czerwca 2012 r., któremu towarzyszyła ocena skutków (SWD(2012) 135 final), określono następujące cztery cele ogólne:

- zapewnienie rozwoju jednolitego rynku cyfrowego;
- promowanie rozwoju kluczowych transgranicznych usług publicznych;
- pobudzanie i wzmacnianie konkurencji na jednolitym rynku;
- tworzenie środowiska przyjaznego użytkownikowi (obywatelom i przedsiębiorstwom).

Pomimo że rozporządzenie to spełnia wiele swoich celów i stało się podstawowym elementem ułatwiającym funkcjonowanie jednolitego rynku w wielu sektorach (np. jeżeli chodzi o usługi finansowe oraz umożliwienie udostępniania i ponownego użycia danych w procedurach administracyjnych), wiąże się z nim jednak szereg ograniczeń: brak obowiązku notyfikowania krajowych systemów identyfikacji elektronicznej, ograniczone atrybuty (elementy danych osobowych), które można wiarygodnie ujawnić osobom trzecim, fakt, że akt ten koncentruje się na sektorze publicznym, oraz brak wyraźnych zachęt do korzystania z krajowych systemów identyfikacji elektronicznej przez podmioty prywatne. Ponadto europejski ekosystem tożsamości elektronicznej jest rozproszony między różne krajowe otoczenia regulacyjne, poziomy administracji cyfrowej, kultury cyfrowej oraz zróżnicowane poziomy zaufania do instytucji publicznych.

1.2. Kontekst

Sposób, w jaki zapewnia się tożsamość cyfrową, podlega fundamentalnym zmianom. Podmioty takie jak banki, dostawcy usług łączności elektronicznej lub zakłady użyteczności publicznej, z których niektóre są prawnie zobowiązane do gromadzenia atrybutów umożliwiających identyfikację, wykorzystują potencjał swoich procedur, aby występować w charakterze zweryfikowanych dostawców tożsamości. Pośrednicy internetowi, w tym duże platformy mediów społecznościowych i przeglądarki internetowe[3], występują w charakterze faktycznych strażników dostępu do tożsamości cyfrowej i oferują rozwiązania umożliwiające przenoszenie tożsamości (ang. bring your own identity, BYOI), dzięki którym ich użytkownicy mogą dokonywać uwierzytelnienia na stronach zewnętrznych i w ramach usług zewnętrznych za pomocą swoich profili użytkowników. Takie wygodne rozwiązanie zapewnia się kosztem utraty kontroli nad ujawnianymi danymi osobowymi, gdyż takie środki identyfikacji elektronicznej nie są połączone z fizycznym środkiem identyfikacji, przez co trudniej jest ograniczać zagrożenia w formie oszustw i zagrożenia dla cyberbezpieczeństwa. Znaczna większość obywateli Unii chciałaby mieć dostęp do bezpiecznej tożsamości cyfrowej, za pomocą której mogliby uzyskać dostęp do usług online[4]. Ponadto, mimo że istnieje wiele różnych poglądów dotyczących przyszłości tożsamości cyfrowej, konieczne jest należyte rozważenie kluczowej roli rządów krajowych w rozwoju każdego daleko idącego ekosystemu tożsamości cyfrowej.

Obecnie użytkownicy oczekują płynnego działania internetu, aplikacji mobilnych i rozwiązań umożliwiających pojedyncze logowanie, które stosuje się do korzystania z usług online w sektorze publicznym i prywatnym, obejmujących wszystkie przypadki użycia do celów

[3] Na przykład użytkownicy portalu Facebook lub użytkownicy Google przez swoje konta mogą logować się do portalu Booking.com lub łączyć się z bazą EU Login https://developers.facebook.com/docs/facebook-login/overview https://developers.google.com/identity/

[4] Badanie Eurobarometr 503: Postawy wobec wpływu cyfryzacji na życie codzienne, grudzień 2019 r., zob.: https://ec.europa.eu/commfrontoffice/publicopinion/index.cfm/Survey/getSurveyDetail/instruments/SPECIAL/surveyKy/2228

identyfikacji, począwszy od logowania do platformy internetowej z użyciem danych pseudonimicznych aż po bezpieczną identyfikację do celów korzystania z usług cyfrowych w dziedzinie e-zdrowia lub elektronicznych usług bankowych. Bezpieczna identyfikacja elektroniczna i wymiana danych uwierzytelniających opartych na atrybutach zyskują na znaczeniu wraz ze wzrostem liczby usług wymagających potwierdzenia tożsamości i usług indywidualnych. Zdolność do dokonania cyfrowej identyfikacji stanie się ważnym czynnikiem włączenia społecznego, a możliwość zapewnienia tożsamości cyfrowej będzie stanowić istotny atut strategiczny.

W orędziu o stanie Unii z dnia 16 września 2020 r. przewodnicząca Komisji Europejskiej ogłosiła, że celem Komisji jest zapewnienie bezpiecznej i wiarygodnej tożsamości cyfrowej wszystkim obywatelom UE: „Chcemy zestawu przepisów, które będą ukierunkowane na ludzi.(...)Obejmuje to także kontrolę nad naszymi danymi osobowymi, której dziś wciąż brakuje.Za każdym razem, gdy aplikacja lub strona internetowa prosi nas o stworzenie nowej tożsamości cyfrowej lub o łatwe zalogowanie się na dużej platformie, nie mamy pojęcia, co w rzeczywistości dzieje się z naszymi danymi.Dlatego też Komisja wkrótce zaproponuje bezpieczną europejską tożsamość elektroniczną.Taką, której będziemy mogli zaufać i z której każdy obywatel będzie mógł skorzystać z każdego miejsca w Europie, aby na przykład zapłacić podatki czy wynająć rower.Mówimy o technologii, w ramach której sami możemy kontrolować, jakie dane są wykorzystywane i w jaki sposób.

Rada Europejska poparła ambicję Komisji i w konkluzjach z dni 1–2 października 2020 r. zwróciła się do Komisji, by do połowy 2021 r. przedstawiła wniosek dotyczący inicjatywy na rzecz europejskiej identyfikacji cyfrowej:

W konkluzjach Rada Europejska apeluje o „opracowanie ogólnounijnych ram bezpiecznej publicznej identyfikacji elektronicznej (e-ID), w tym interoperacyjnych podpisów cyfrowych, by zapewnić obywatelom kontrolę nad ich tożsamością i danymi w internecie, a także by umożliwić dostęp do publicznych, prywatnych i transgranicznych usług cyfrowych.Zwraca się do Komisji, by do połowy 2021 r. przedstawiła wniosek dotyczący inicjatywy na rzecz europejskiej identyfikacji cyfrowej”.

Dzięki identyfikacji elektronicznej obywatele i przedsiębiorstwa mogą potwierdzić swoją tożsamość przy uzyskiwaniu dostępu do usług online. Usługi zaufania, takie jak podpisy elektroniczne, sprawiają, że transakcje online stają się bezpieczniejsze i skuteczniejsze, a korzystanie z nich jest wygodniejsze. Rozporządzenie eIDAS stanowi jedyne transgraniczne ramy dotyczące wiarygodnej identyfikacji elektronicznej osób fizycznych i prawnych oraz usług zaufania. Rozporządzenie eIDAS umożliwia transgraniczne uznawanie rządowych systemów identyfikacji elektronicznych zapewniających dostęp do usług publicznych, pod warunkiem że dany system identyfikacji elektronicznej notyfikowano na podstawie rozporządzenia eIDAS. Rozporządzeniem eIDAS ustanowiono również unijny rynek usług zaufania uznawanych ponad granicami i mających ten sam status prawny co tradycyjne równoważne procesy oparte na dokumentacji papierowej.

2. GŁÓWNE USTALENIA OCENY

Zgodnie z kryteriami oceny jej główne ustalenia można podsumować w poniższych punktach.

2.1. Skuteczność

W wyniku stosowania przepisów dotyczących tożsamości elektronicznej utworzono sieć eIDAS, która ma umożliwić posiadaczom systemu identyfikacji elektronicznej uzyskanie

transgranicznego dostępu do usług publicznych online. Na szczeblu unijnym osiągnięto interoperacyjność jedynie ograniczonej liczby systemów identyfikacji elektronicznej[5].
Za sprawą rozporządzenia eIDAS z powodzeniem osiągnięto pewność prawa w zakresie odpowiedzialności i ciężaru dowodu w związku z usługami zaufania oraz skutków prawnych i międzynarodowych aspektów usług zaufania, przy czym nadal pewne kwestie pozostają jednak do rozwiązania. Od czasu wprowadzenia rozporządzenia eIDAS odnotowano wzrost dostępności i wykorzystania usług zaufania w UE, choć występują różnice w tym zakresie między państwami członkowskimi i między poszczególnymi usługami zaufania.

Pomimo pewnych osiągnięć nie wykorzystano pełnego potencjału rozporządzenia pod względem skuteczności. Notyfikowano jedynie ograniczoną liczbę systemów identyfikacji elektronicznej, co sprawia, że liczba obywateli Unii objętych notyfikowanymi systemami identyfikacji elektronicznej jest ograniczona (59 % ludności). Ograniczony jest również poziom akceptacji notyfikowanych systemów identyfikacji elektronicznej, co wynika z faktu, że nie wszystkie węzły eIDAS zostały uruchomione, ograniczona liczba usług publicznych obejmuje możliwość notyfikacji eIDAS lub jest połączona z infrastrukturą, a błędy techniczne uniemożliwiają użytkownikom skuteczne uwierzytelnienie.

Jeżeli chodzi o usługi zaufania, przyjęcie celu, zgodnie z którym rozporządzenie to powinno być neutralne pod względem technologicznym, skutkowało różnicami w zakresie interpretacji wymogów występującymi między poszczególnymi państwami członkowskimi, co wynika również z braku przyjęcia dodatkowych aktów wykonawczych. Nie można stwierdzić, że w pełni osiągnięto równe warunki działania na szczeblu UE. W drodze rozporządzenia eIDAS ustanowiono jednak solidne ramy, które można uzupełnić o niezbędne normy i wymogi w celu ograniczenia obecnie obserwowanej fragmentacji rynku i zróżnicowanej interpretacji przyjmowanej przez organy nadzoru i jednostki oceniające zgodność oraz w celu osiągnięcia ściślejszej współpracy między organami nadzoru.

2.2. Efektywność

Z oceny wyjściowej wynika, że dotychczas wymierne koszty przekraczają korzyści. Jeżeli chodzi o identyfikację elektroniczną, wynika to z braku urzeczywistnienia korzyści w związku z niskim poziomem wykorzystania.

Kluczowymi grupami zainteresowanych stron, które odnotowały koszty i korzyści w związku z częścią rozporządzenia eIDAS dotyczącą identyfikacji elektronicznej, są organy krajowe, operatorzy węzłów eIDAS, dostawcy środków identyfikacji elektronicznej i dostawcy usług. Jeżeli chodzi o usługi zaufania, kluczowymi grupami zainteresowanych stron, które poniosły największe koszty i uzyskały największe korzyści, są jednostki akredytujące, jednostki oceniające zgodność, organy nadzoru oraz kwalifikowani i niekwalifikowani dostawcy usług zaufania.

W przypadku poszczególnych zainteresowanych stron znaczną część korzyści stanowią korzyści oczekiwane (pomijane jako przyszłe korzyści), które trudno jest oszacować. Stałe koszty zarządzania w obszarze usług zaufania są ograniczone i głównie wiążą się z zapewnieniem przestrzegania przepisów. W przypadku poszczególnych zainteresowanych

[5] Od wejścia w życie części rozporządzenia dotyczącej identyfikacji elektronicznej we wrześniu 2017 r. 14 państw członkowskich notyfikowało przynajmniej jeden system identyfikacji elektronicznej, a cztery państwa członkowskie notyfikowało już kilka systemów. Łącznie do tej pory notyfikowano 19 systemów identyfikacji elektronicznej: https://ec.europa.eu/cefdigital/wiki/display/CEFDIGITAL/Country+overview

stron znaczna część korzyści na tym etapie ma wyłącznie charakter hipotetyczny (korzyści te są pomijane jako przyszłe korzyści) i jest trudna do oszacowania. Dostawcy usług zaufania zgłaszają korzyści w formie przychodów z tytułu świadczenia usług zaufania w innych państwach UE i zwiększenia rynku podstawowego.

2.3. Znaczenie

Od czasu wprowadzenia rozporządzenia eIDAS ekosystem identyfikacji elektronicznej przeszedł diametralna zmianę wraz z rosnącym znaczeniem prywatnych dostawców tożsamości. Biorąc pod uwagę wzrost liczby transakcji cyfrowych, wszyscy obywatele Unii powinni mieć dostęp do bezpiecznej i interoperacyjnej tożsamości cyfrowej, co obecnie nie ma miejsca. Cele ram prawnych eIDAS pozostają istotne w kontekście rozwiązania początkowo zidentyfikowanych kwestii, w szczególności w związku z koniecznością zmniejszenia fragmentacji rynku poprzez zapewnienie transgranicznej i międzysektorowej interoperacyjności usług zaufania dzięki przyjęciu wspólnych norm. Wydaje się, 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.

Określone kluczowe przeszkody w zakresie rozpowszechniania proponowanych rozwiązań wśród użytkowników i dostawców usług z sektora prywatnego uniemożliwiają wykorzystanie pełnego potencjału tych ram regulacyjnych. Pomimo wprowadzenia odniesień do rozwiązań eIDAS w szeregu sektorowych przepisów UE w rozporządzeniu eIDAS nie zapewniono jeszcze rozwiązań dostosowanych do potrzeb występujących w konkretnych sektorach (np. w sektorze kształcenia, bankowości, podróżowania, lotnictwa). Jednym z czynników powodujących ograniczenie obecnie obowiązujących ram pod względem tego rodzaju potrzeb sektorowych jest brak szczególnych atrybutów w podziale na dziedziny.

Główny problem stanowi zdolność do zapewnienia ciągłej zgodności rozporządzenia eIDAS z najnowszym rozwojem technologii w dziedzinie usług zaufania. Dzięki rozszerzeniu listy usług zaufania, w szczególności poprzez wprowadzenie usługi zaufania na potrzeby e-archiwizacji, usługi zaufania obsługującej przenośne poświadczenia tożsamości oraz usługi zaufania w zakresie rejestrów elektronicznych, uwzględniono by szereg przypadków użycia oraz umożliwiono by obywatelom i przedsiębiorstwom cyfrowe poświadczenie swojej tożsamości lub swoich atrybutów/cech charakterystycznych bez konieczności przedstawienia dokumentów w formie fizycznej.

2.4. Spójność

Z oceny wynika, że część rozporządzenia dotycząca identyfikacji elektronicznej jest poparta ogólnie spójnym systemem wzajemnego uznawania środków identyfikacji elektronicznej na podstawie notyfikowania i wzajemnej oceny. W ramach dotyczących usług zaufania przewidziano spójny system nadzoru w zakresie usług zaufania. Zidentyfikowano jednak określone problemy mające wpływ na wewnętrzną spójność tego rozporządzenia.

W przypadku identyfikacji elektronicznej system notyfikacji i wzajemnej oceny jest określony w ramach eIDAS, które mają na celu osiągnięcie wspólnego porozumienia w sprawie poziomu bezpieczeństwa zapewnianego w ramach danego systemu identyfikacji elektronicznej, ale z oceny praktycznego wdrożenia wynika, że nie zawsze tak się dzieje. Chociaż rozporządzenie sprzyja elastyczności i neutralności pod względem technologicznym, nadal brakuje wspólnego porozumienia w kwestii, co można uznać za średni i wysoki poziom

bezpieczeństwa. Nacisk na usługi publiczne kontrastuje z możliwością ograniczenia przez użytkownika przesyłanych danych do minimum niezbędnego do uwierzytelnienia na potrzeby danej usługi, jako że do celów umożliwienia identyfikacji danej osoby zawsze przesyła się minimalny zestaw danych. W ramach wdrażania obecnie obowiązującego systemu eIDAS użytkownik nie ma możliwości wyegzekwowania przewidzianych w RODO zasad minimalizacji danych i domyślnej ochrony prywatności w drodze kontroli, które dane są udostępniane i komu są one udostępniane.

Jeżeli chodzi o przepisy dotyczące oceny dostawców usług zaufania pod kątem wymagań funkcjonalnych określonych w rozporządzeniu w zakresie uzyskania statusu kwalifikowanego, stwierdzono niedociągnięcia związane z niewystarczającym doprecyzowaniem roli jednostek oceniających zgodność w zakresie ich obowiązków, odpowiedzialności lub poziomu kompetencji. W niektórych przepisach przewidziano, że państwa członkowskie odpowiadają za uznawanie określonych metod identyfikacji (takich jak weryfikacja biometryczna) na szczeblu krajowym, co utrudnia zapewnienie takich samych warunków prawnych i stanowi źródło niepewności.

2.5. Europejska wartość dodana

Mimo że w ramach rozporządzenia eIDAS stwarza się zachęty dla państw członkowskich do wdrażania krajowych rozwiązań z zakresu identyfikacji elektronicznej, to jednak stwierdzono znaczne ograniczenia pod względem wartości dodanej ram identyfikacji elektronicznej ze względu na ich mały zasięg oraz nieznaczne rozpowszechnienie i wykorzystanie. W rozporządzeniu przewidziano wspólne ramy prawne dotyczące korzystania z usług zaufania, ograniczające fragmentację rynku i zwiększające rozpowszechnienie takich usług. Za pomocą usług zaufania administracje publiczne mogą unowocześnić usługi i świadczyć je w formie cyfrowej oraz wydawać dowody w formie cyfrowej, co skutkuje ograniczeniem obciążenia administracyjnego.

W przypadku części dotyczącej identyfikacji elektronicznej początkowo określone potrzeby przemawiające za przyjęciem rozporządzenia nadal są ważne, a uchylenie rozporządzenia skutkowałoby fragmentacją i miałoby niekorzystny wpływ na inne obszary prawa uzależnione od rozporządzenia eIDAS. Wprowadzając określone dostosowania ram regulacyjnych, można by zwiększyć ich europejską wartość dodaną (dotyczy to między innymi ułatwienia korzystania z wiarygodnych rządowych systemów identyfikacji elektronicznej przez sektor prywatny oraz definicji ram dotyczących wymiany szczególnych atrybutów i danych uwierzytelniających zapewnianych przez sektor publiczny i sektor prywatny). W przypadku usług zaufania nadal występują niektóre przeszkody wynikające z wykładni krajowej lub sprzecznych przepisów krajowych, które to przeszkody skutkują ograniczeniem rozpowszechnienia usług zaufania.

3. PRZEGLĄD RAM EIDAS

Rozporządzenie eIDAS jest podstawowym elementem ułatwiającym funkcjonowanie jednolitego rynku w wielu sektorach (np. w sektorze bankowym umożliwia przekazywanie niektórych wymaganych danych dotyczących tożsamości w celu ułatwienia zapewnienia zgodności z przepisami dotyczącymi przeciwdziałania praniu pieniędzy[6], druga dyrektywa

[6] Dyrektywa Parlamentu Europejskiego i Rady (UE) 2015/849 z dnia 20 maja 2015 r. w sprawie zapobiegania wykorzystywaniu systemu finansowego do prania pieniędzy lub finansowania terroryzmu, zmieniająca rozporządzenie Parlamentu Europejskiego i Rady (UE) nr 648/2012 i uchylająca dyrektywę Parlamentu Europejskiego i Rady 2005/60/WE oraz dyrektywę Komisji 2006/70/WE.

w sprawie usług płatniczych[7] bazuje na usługach zaufania przewidzianych w rozporządzeniu eIDAS, takich jak pieczęci elektroniczne i kwalifikowane certyfikaty uwierzytelniania witryn internetowych, w celu ustalenia autentyczności witryn internetowych dostarczanych przez zewnętrznych dostawców usług płatniczych, systemy identyfikacji elektronicznej oparte na rozporządzeniu eIDAS stanowią wymóg transgranicznej wymiany certyfikatów administracyjnych, rozporządzenie ma także podstawowe znaczenie dla skutecznego wdrożenia i funkcjonowania zasady jednorazowości, która będzie stosowana od 2023 r.[8]). Ramy dotyczące usług zaufania zostały uznane na forum międzynarodowym i stanowią podstawę projektu przepisów[9], które mają stać się wzorcowymi przepisami dotyczącymi usług zaufania w handlu elektronicznym w ramach ONZ w 2021 r., a także podstawę trwających negocjacji dotyczących handlu elektronicznego na forum WTO[10].

Odkąd przyjęto rozporządzenie eIDAS w 2014 r., nastąpiło jednak wiele zmian. Ramy te opierają 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: tj. na bezpiecznym transgranicznym dostępie do usług publicznych. Przedmiotowe usługi dotyczą głównie 3 % ludności UE[11], która mieszka w państwie członkowskim innym niż państwo urodzenia.

Od tamtego czasu nastąpił gwałtowny rozwój transformacji cyfrowej w zakresie wszystkich funkcji społeczeństwa. W szczególności do przyspieszenia procesu transformacji cyfrowej w bardzo dużej mierze przyczyniała się pandemia COVID-19. W rezultacie coraz więcej usług publicznych i usług prywatnych jest świadczonych w przestrzeni cyfrowej. Obywatele i przedsiębiorstwa oczekują osiągnięcia wysokiego poziomu bezpieczeństwa i wygody w zakresie 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 w sposób bezpieczny i z zapewnieniem wysokiego stopnia ochrony danych[12]. Spowodowało to zmianę paradygmatu w kierunku zaawansowanych i wygodnych rozwiązań, które umożliwiają integrację różnych możliwych do sprawdzenia danych i certyfikatów użytkownika. Obecnie takiego zapotrzebowania nie da się zaspokoić w ramach środków identyfikacji elektronicznej i usług zaufania uregulowanych w rozporządzeniu

---

7 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.

8 Od 2023 r. dzięki obowiązywaniu zasady jednorazowości administracje publiczne będą mogły w przejrzysty i bezpieczny sposób ponownie wykorzystywać oraz udostępniać dane i dokumenty już dostarczone przez obywateli. (Art. 14 rozporządzenia 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).

9 https://undocs.org/en/A/CN.9/WG.IV/WP.167

10 Zob. np. dokumenty z posiedzeń grupy roboczej IV UNCITRAL / Handel elektroniczny, posiedzenie w dniach 6–9 kwietnia 2021 r.: https://uncitral.un.org/en/working_groups/4/electronic_commerce

11. https://ec.europa.eu/eurostat/statistics-explained/index.php/EU_citizens_living_in_another_Member_State_-_statistical_overview

12 Na przykład we Włoszech system SPID (uruchomiony w 2016 r.) na koniec 2019 r. liczył około 5 milionów użytkowników. Obecnie liczba aktywnych użytkowników wynosi ponad 18 milionów (zob. https://avanzamentodigitale.italia.it/it/progetto/spid), przy czym liczba ta stale rośnie o około 1 milion użytkowników na miesiąc. W całym roku 2019 r. z systemu SPID skorzystało około 55 mln użytkowników, podczas gdy tylko w lutym 2021 r. liczba ta wyniosła około 32,4 mln.

eIDAS, mając na uwadze jego obecne ograniczenia. Środki identyfikacji i uwierzytelniania opracowane przez sektor prywatny nieobjęty ramami eIDAS stanowią jedynie częściowe rozwiązanie tego problemu. O ile obejmują one łatwe w obsłudze zewnętrzne usługi uwierzytelniania (czego przykładem jest logowanie się do różnych usług za pomocą konta na portalu Facebook lub konta Google), to jednak w ich ramach powszechnie uzyskuje się dostęp do nieregulowanych prywatnych usług online, które nie wymagają wysokiego poziomu bezpieczeństwa. Za pomocą takich środków nie można zapewnić takiego samego poziomu pewności prawa, ochrony danych i prywatności, czego głównym powodem jest fakt, że są one określane samodzielnie i nie mogą zostać połączone z wiarygodnym i bezpiecznym rządowym systemem identyfikacji elektronicznej.

W lutym 2020 r. w ramach strategii dotyczącej kształtowania cyfrowej przyszłości Europy[13] Komisja zobowiązała się do dokonania przeglądu rozporządzenia eIDAS w celu zwiększenia jego skuteczności, rozszerzenia zakresu jego stosowania na sektor prywatny i promowania wiarygodnych tożsamości cyfrowych dla wszystkich obywateli i przedsiębiorstw Unii. Wraz z wybuchem pandemii COVID-19 oczywiste stało się, że istnieje pilna potrzeba dokonania tego przeglądu. W związku z zakłóceniami usług publicznych i prywatnych świadczonych poza internetem oraz nagłym zapotrzebowaniem na dostęp do wszelkiego rodzaju usług publicznych i prywatnych online oraz na korzystanie z takich usług widoczne stały się ograniczenia rozporządzenia eIDAS, jeżeli chodzi o zapewnienie oczekiwanych korzyści obywatelom, przedsiębiorstwom i rządom po upływie sześciu lat od przyjęcia tego rozporządzenia. W ramach zmienionego i udoskonalonego rozporządzenia eIDAS można będzie reagować na nowe potrzeby rynkowe i społeczne dzięki zaspokojeniu zapotrzebowania na powiązane rozwiązania w zakresie wiarygodnych rządowych systemów identyfikacji elektronicznej, ale również na atrybuty i dane uwierzytelniające zapewniane przez sektor publiczny i sektor prywatny, przy czym wszystkie te elementy byłyby w pełni zarządzane przez użytkownika i uznawane w całej UE na potrzeby uzyskania dostępu zarówno do usług publicznych, jak i do usług prywatnych. W ten sposób zapewniono by wsparcie dużej liczby już obowiązujących lub proponowanych ram regulacyjnych, umacniając unijny jednolity rynek.

4. WNIOSKI

W ogólnym rozliczeniu rozporządzenie eIDAS przyczyniło się do dalszego rozwoju jednolitego rynku. Rozporządzenie to stanowi podstawę rozwoju rynku w zakresie poświadczania tożsamości i usług zaufania w UE i tym samym przyczynia się do zaspokojenia stale rosnącego zapotrzebowania na bezpieczne transakcje cyfrowe. Mając jednak na uwadze długoterminowe podejście perspektywiczne, które zmieniło się pod względem celów i oczekiwań użytkowników, rozporządzenie eIDAS należy udoskonalić pod kątem skuteczności, efektywności, spójności i znaczenia, aby przyczyniało się ono do osiągnięcia nowych celów polityki, odpowiadało oczekiwaniom użytkowników i popytowi na rynku, z uwzględnieniem również najnowszych zmian w zakresie transformacji cyfrowej.

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 do usług, zarówno w sektorze

[13] Komisja Europejska. (2020 r.). Strategia „Kształtowanie cyfrowej przyszłości Europy”.

prywatnym, jak i w sektorze publicznym, w związku z koniecznością identyfikacji i uwierzytelnienia użytkowników przy zapewnieniu wysokiego poziomu bezpieczeństwa.

W ramach rozporządzenia eIDAS w jego obecnym kształcie nie można zaspokoić tych nowych potrzeb rynkowych ze względu na jego wewnętrzne ograniczenia do sektora publicznego, złożoność procesu połączenia z systemem dostawców usług online z sektora prywatnego, niewystarczającą dostępność systemu we wszystkich państwach członkowskich oraz brak elastyczności rozporządzenia umożliwiającej uwzględnienie różnego rodzaju przypadków.