Opinia Europejskiego Komitetu Ekonomiczno-Społecznego „Wniosek dotyczący rozporządzenia Parlamentu Europejskiego i Rady zmieniającego rozporządzenie (UE) nr 910/2014 w odniesieniu do ustanowienia europejskich ram tożsamości cyfrowej”

[COM(2021) 281 final – 2021/0136 (COD)]

(2022/C 105/12)

Sprawozdawca: **Tymoteusz Adam ZYCH**

Wniosek	Parlament Europejski, 8.7.2021
	Rada, 15.7.2021
Podstawa prawna	Art. 114 Traktatu o funkcjonowaniu Unii Europejskiej
Sekcja odpowiedzialna	Sekcja Jednolitego Rynku, Produkcji i Konsumpcji
Data przyjęcia przez sekcję	30.9.2021
Data przyjęcia na sesji plenarnej	20.10.2021
Sesja plenarna nr	564
Wynik głosowania	
(za/przeciw/wstrzymało się)	229/2/5

1. **Wnioski i zalecenia**

1.1. Europejski Komitet Ekonomiczno-Społeczny (EKES) z zadowoleniem przyjmuje wniosek Komisji Europejskiej dotyczący instrumentu zmieniającego rozporządzenie eIDAS odnośnie do ustanowienia europejskich ram tożsamości cyfrowej i dostosowującego go do bieżących potrzeb rynku. Ocena obowiązującego rozporządzenia pokazała, że niezbędne jest zapewnienie lepszych rozwiązań w zakresie usług cyfrowych, które to rozwiązania rozszerzyłyby dostęp zarówno na sektor prywatny, jak i publiczny i zostałyby udostępnione przeważającej większości europejskich obywatelek i obywateli oraz mieszkańców.

1.2. EKES odnotowuje jednak, że proponowana cyfryzacja usług może prowadzić do wykluczenia części społeczeństwa europejskiego, w szczególności osób starszych, osób o niskim poziomie umiejętności cyfrowych i osób z niepełnosprawnościami. W związku z tym zwraca się do Komisji Europejskiej (KE) i państw członkowskich o ustanowienie niezbędnych ram edukacji cyfrowej i kampanii informacyjnej, które powinny również przyczynić się do zwiększenia świadomości w dziedzinie ochrony danych osobowych.

1.3. EKES z zadowoleniem przyjmuje fakt, że korzystanie z europejskich portfeli tożsamości cyfrowej będzie fakultatywne i bezpłatne. Niemniej wprowadzenie nowych rozwiązań cyfrowych wiąże się nieuchronnie ze znacznymi kosztami i wymaga wiele czasu. Dlatego też Komitet zwraca się do KE o dalsze oszacowanie czasu potrzebnego do faktycznego wdrożenia nowego rozporządzenia w celu uniknięcia negatywnych skutków dla rynku oraz o przedstawienie w rozporządzeniu dalszej analizy oczekiwanych kosztów wdrożenia i ich lepsze objaśnienie.

1.4. EKES zauważa, że proponowana sekcja 9 rozporządzenia przewiduje obowiązkowe transgraniczne uznawanie kwalifikowanego elektronicznego poświadczenia atrybutów wydanego w danym państwie członkowskim. Jednak biorąc pod uwagę fakt, że postanowienia krajowych przepisów państw członkowskich często są znacznie odmienne, EKES dostrzega potrzebę wyjaśnienia, że uznawanie kwalifikowanego elektronicznego poświadczenia atrybutów w jednym państwie członkowskim ogranicza się do potwierdzenia faktów. Analogię stanowi w tym przypadku art. 2 ust. 4 rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/1191 ([1]) w sprawie promowania swobodnego przepływu obywateli poprzez uproszczenie wymogów dotyczących przedkładania określonych dokumentów urzędowych w Unii Europejskiej: „Niniejsze rozporządzenie nie ma zastosowania do uznawania w państwie członkowskim skutków prawnych związanych z treścią dokumentów urzędowych wydawanych przez organy innego państwa członkowskiego”.

([1]) Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2016/1191 z dnia 6 lipca 2016 r. w sprawie promowania swobodnego przepływu obywateli poprzez uproszczenie wymogów dotyczących przedkładania określonych dokumentów urzędowych w Unii Europejskiej i zmieniające rozporządzenie (UE) nr 1024/2012 (Dz.U. L 200 z 26.7.2016, s. 1).

1.5. Z punktu widzenia EKES-u skuteczną ochronę danych trzeba rozpatrywać szczególnie w kontekście ochrony praw podstawowych, zwłaszcza prawa do prywatności i prawa do ochrony danych osobowych. W związku z tym w pełni popiera wymóg, by europejskie ramy tożsamości cyfrowej zapewniały użytkownikom środki pozwalające kontrolować, kto ma dostęp do ich cyfrowego bliźniaka i do jakich dokładnie danych ma dostęp. Zachęca KE i państwa członkowskie, by po konsultacjach na temat technicznych aspektów europejskich ram tożsamości cyfrowej uwzględniły kwestię stworzenia rejestru umożliwiającego użytkownikom śledzenie wszelkiego dostępu do ich danych.

1.6. EKES pragnie zwrócić uwagę na obawy dotyczące bezpieczeństwa związane z procesem cyfryzacji, zwłaszcza z rozwojem rozbudowanych systemów przechowywania i przetwarzania danych narażonych na oszustwo i utratę. Ma świadomość, że obecnie brak systemu bezpieczeństwa, który mógłby zapewnić pełną ochronę danych. W związku z tym zdaniem EKES-u użytkownikom europejskich portfeli tożsamości cyfrowej trzeba zagwarantować odszkodowanie za wszelkie niepożądane sytuacje dotyczące ich danych (np. kradzież lub ujawnienie). Odpowiedzialność powinna być niezależna od tego, czy dostawca usługi ponosi winę za daną sytuację.

2. **Wprowadzanie**

2.1. Przedmiotem niniejszej opinii jest wniosek KE dotyczący rozporządzenia zmieniającego rozporządzenie Parlamentu Europejskiego i Rady (UE) nr 910/2014 ([2]) („rozporządzenie eIDAS") odnośnie do ustanowienia europejskich ram tożsamości cyfrowej.

2.2. Jak wyjaśniono w uzasadnieniu, rozporządzenie eIDAS zapewniłoby następujące zabezpieczenia i korzyści: 1) dostęp do wysoce bezpiecznych i wiarygodnych rozwiązań w zakresie tożsamości elektronicznej; 2) pewność, że usługi publiczne i prywatne mogą opierać się na zaufanych i bezpiecznych rozwiązaniach w zakresie tożsamości cyfrowej; 3) pewność, że osoby fizyczne i prawne są uprawnione do korzystania z rozwiązań w zakresie tożsamości cyfrowej; 4) gwarancję, aby rozwiązania te były powiązane z różnymi atrybutami i umożliwiały ukierunkowane udostępnianie danych dotyczących tożsamości ograniczone do potrzeb konkretnej żądanej usługi; oraz 5) akceptację kwalifikowanych usług zaufania w UE i równych warunków ich świadczenia. Proponowane zmiany są odpowiedzią na wzrost popytu na godne zaufania cyfrowe rozwiązania transgraniczne oparte na potrzebie identyfikacji i uwierzytelniania użytkowników o wysokim poziomie pewności.

3. **Uwagi ogólne**

3.1. EKES zdaje sobie sprawę z nowych wymogów rynku wewnętrznego dotyczących rozwoju identyfikacji elektronicznej i usług zaufania odnośnie do elektronicznych transakcji transgranicznych. Obecne rozwiązania przewidziane w rozporządzeniu eIDAS, które zaczęły wywoływać skutki prawne na kilku etapach, począwszy od lipca 2016 r., nie spełniają tych wymogów. Świadczy o tym fakt, że obecnie zaledwie 59 % mieszkańców UE ma dostęp do zaufanych i bezpiecznych rozwiązań w zakresie identyfikacji elektronicznej. Ponadto transgraniczny dostęp do takich usług jest ograniczony ze względu na brak interoperacyjności między systemami oferowanymi przez poszczególne państwa członkowskie.

3.2. Dlatego też EKES z zadowoleniem przyjmuje nowy wniosek KE dotyczący instrumentu zmieniającego rozporządzenie eIDAS odnośnie do ustanowienia europejskich ram tożsamości cyfrowej i dostosowujący go do bieżących potrzeb rynku. Szacuje się, że rozwiązania zaproponowane w dokumencie Komisji mogą przyczynić się do zwiększenia liczby użytkowników identyfikacji elektronicznej aż do 80 %, a nawet do 100 % wszystkich obywateli i mieszkańców UE.

3.3. EKES ze szczególnym zadowoleniem przyjmuje rozwiązania mające na celu zwiększenie bezpieczeństwa danych osobowych użytkowników dzięki zagwarantowaniu swobody udostępniania danych oraz możliwości kontrolowania charakteru i ilości danych przekazywanych stronom ufającym. Zważywszy, że zgodnie z wnioskiem państwa członkowskie zachowają kontrolę nad dostawcami usług cyfrowych, rozwiązania te będą gwarantować, że zbiory danych wrażliwych (np. dotyczących zdrowia, religii i przekonań, poglądów politycznych, pochodzenia rasowego lub etnicznego) będą przekazywane wyłącznie na wniosek dostawców usług, po podjęciu świadomej decyzji przez właściciela tożsamości zgodnie z prawem krajowym mającym zastosowanie.

3.4. EKES zwraca uwagę, że harmonogram stosowania niektórych przepisów nowego rozporządzenia jest raczej optymistyczny i zwraca się do Komisji Europejskiej, by ustalając ostateczne terminy zastosowania rozporządzenia, wzięła również pod uwagę czas potrzebny dostawcom usług na modernizację systemów informatycznych w celu dostosowania się do nowych wymogów. Wnosi zatem, by KE dokonała dalszej analizy czasu potrzebnego na faktyczne wdrożenie nowego

([2]) Rozporządzenie Parlamentu Europejskiego i Rady (UE) nr 910/2014 z dnia 23 lipca 2014 r. w sprawie identyfikacji elektronicznej i usług zaufania w odniesieniu do transakcji elektronicznych na rynku wewnętrznym oraz uchylające dyrektywę 1999/93/WE (Dz.U. L 257 z 28.8.2014, s. 73).

rozporządzenia i tym samym przedłużyła termin jego zastosowania, by nie miało to wpływu na przedmiotowy rynek. Tytułem przykładu, wejście w życie rozporządzenia będzie wymagało, aby obecni dostawcy kwalifikowanych usług zaufania oferujący możliwość zdalnego złożenia podpisu za pomocą kwalifikowanego urządzenia do składania podpisu na odległość stali się kwalifikowanymi dostawcami tej konkretnej usługi; zarówno wdrożenie aspektów technicznych, jak i dopełnienie procedury zezwolenia będzie dla nich czasochłonne.

3.5. EKES odnotowuje, że abstrahując od korzyści płynących z proponowanej cyfryzacji usług, może ona prowadzić do wykluczenia części społeczeństwa europejskiego, w szczególności osób starszych, osób o niskim poziomie umiejętności cyfrowych i osób z niepełnosprawnościami. Dostrzega kluczową rolę edukowania europejskich obywatelek i obywateli w celu przeciwdziałania wykluczeniu; edukacja powinna również przyczynić się do pogłębienia świadomości w dziedzinie ochrony danych osobowych.

4. **Dostępność i uznaniowe korzystanie z europejskich ram tożsamości cyfrowej**

4.1. EKES z zadowoleniem przyjmuje pomysł zapewnienia lepszych rozwiązań w zakresie usług cyfrowych, które to rozwiązania rozszerzyłyby dostęp nie tylko na usługi publiczne, lecz również na sektor prywatny. Ponadto zgadza się z podejmowanymi przez Komisję Europejską próbami udostępnienia europejskich ram tożsamości cyfrowej ogromnej większości obywatelek i obywateli europejskich. Ze względu na obecne przeszkody w transgranicznym dostępie do usług identyfikacji elektronicznej (np. brak interoperacyjności między systemami identyfikacji elektronicznej opracowanymi przez państwa członkowskie) wielu mieszkańców UE w ogóle z nich nie korzysta. Nowe rozwiązania oparte na europejskich portfelach tożsamości cyfrowej mogą przyczynić się do udostępnienia zaufanych usług online co najmniej 80 % Europejczyków.

4.2. Dlatego też EKES popiera propozycję ustanowienia wymogu, by państwa członkowskie wydawały europejski portfel tożsamości cyfrowej, który umożliwiałby użytkownikowi: 1) ubieganie się o niezbędne dane identyfikujące osobę prawną i elektroniczne poświadczenie atrybutów w celu uwierzytelniania elektronicznego online i offline oraz korzystania z usług publicznych i prywatnych online, a także otrzymanie tych danych, ich przechowywanie, wybranie, łączenie i udostępnianie w bezpieczny, przejrzysty i identyfikowalny dla użytkownika sposób; oraz 2) podpisywanie dokumentów za pomocą kwalifikowanego podpisu elektronicznego akceptowanego w całej UE.

4.3. Ponadto EKES z zadowoleniem przyjmuje propozycję zatroszczenia się o to, by europejski portfel tożsamości cyfrowej był równie dostępny dla osób z niepełnosprawnościami zgodnie z postanowieniami załącznika I do dyrektywy Parlamentu Europejskiego i Rady (UE) 2019/882 ([3]), co odpowiada unijnej zasadzie niedyskryminacji określonej w art. 21 Karty praw podstawowych UE. Aby uniknąć wykluczenia cyfrowego, w odniesieniu do tej kwestii EKES proponuje opracowywanie wszelkich rozwiązań we współpracy z właściwymi instytucjami i organizacjami pozarządowymi zajmującymi się sprawami osób z niepełnosprawnościami, z zastosowaniem podejścia z udziałem wielu zainteresowanych stron.

4.4. Z punktu widzenia EKES-u pozytywnym aspektem jest również to, że obywatelki i obywatele oraz mieszkańcy UE będą mieli swobodę uznania w kwestii korzystania z europejskiego portfela tożsamości cyfrowej. Uważa, że użytkownicy nie powinni być zobowiązani do korzystania z portfela w celu uzyskania dostępu do usług prywatnych lub publicznych, lecz jedynie mieć taką możliwość.

4.5. Jeśli chodzi o przystępność, EKES z zadowoleniem przyjmuje fakt, że korzystanie z europejskiego portfela tożsamości cyfrowej będzie bezpłatne dla użytkowników. Zachęca jednak Komisję Europejską do dalszej analizy i wyjaśnienia w rozporządzeniu (i) kosztów wydawania dokumentów dla osób fizycznych; (ii) kosztów (wydawania i korzystania) ponoszonych przez podmioty prawne; oraz (iii) kosztów dodawania wszelkich atrybutów tożsamości cyfrowej do portfela, ponieważ jego zdaniem każdy taki dodatek stanowiłby usługę zaufania, co wiązałoby się z kosztami dla właściciela portfela.

5. **Aspekty używalności europejskich ram tożsamości cyfrowej**

5.1. EKES z zadowoleniem przyjmuje inicjatywę Komisji Europejskiej mającą na celu zwiększenie używalności środków identyfikacji elektronicznej dzięki stworzeniu wspólnych europejskich ram tożsamości cyfrowej opartych na transgranicznym korzystaniu z europejskiego portfela tożsamości cyfrowej.

5.2. Zgodnie z wnioskiem używalność można zwiększyć za pomocą środków przewidzianych w nowym art. 12 lit. b) rozporządzenia eIDAS, który zawiera szereg wymogów dotyczących uznawania europejskiego portfela tożsamości cyfrowej i dotyczy nie tylko państw członkowskich, lecz również prywatnych stron ufających świadczących usługi oraz „bardzo dużych platform internetowych" zdefiniowanych w art. 25 ust. 1 proponowanego aktu o usługach cyfrowych ([4]). Na podstawie tych nowych przepisów niektóre sektory prywatne (tj. transport, energetyka, usługi bankowe i finansowe,

([3]) 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).

([4]) COM/2020/825 final.

zabezpieczenie społeczne, zdrowie, woda pitna, usługi pocztowe, infrastruktura cyfrowa, edukacja i telekomunikacja) powinny zaakceptować korzystanie z europejskiego portfela tożsamości cyfrowej w celu świadczenia usług w przypadkach, gdy krajowe lub unijne prawo bądź zobowiązania umowne wymagają skutecznego uwierzytelniania użytkownika do celów identyfikacji elektronicznej. W świetle wniosku Komisji taki sam wymóg miałby zastosowanie do bardzo dużych platform internetowych (np. sieci społecznościowych), które powinny zaakceptować korzystanie z europejskiego portfela tożsamości cyfrowej odnośnie do minimalnych atrybutów niezbędnych dla konkretnej usługi online wymagającej uwierzytelnienia, takiego jak dowód potwierdzający wiek.

5.3. EKES zauważa, że w celu zagwarantowania szerokiej dostępności i używalności środków identyfikacji elektronicznej, w tym europejskiego portfela tożsamości cyfrowej, prywatni dostawcy usług internetowych (którzy nie kwalifikują się jako „bardzo duże platformy") powinni być zaangażowani w opracowywanie samoregulacyjnych kodeksów postępowania ułatwiających powszechną akceptację środków identyfikacji elektronicznej. Komisja Europejska powinna odpowiadać za ocenę skuteczności i używalności takich przepisów z punktu widzenia użytkowników europejskiego portfela tożsamości cyfrowej.

6. **Kwestie dotyczące skutków prawnych europejskiego portfela tożsamości cyfrowej**

6.1. EKES popiera wniosek dotyczący poprawy dostępu do cyfrowych usług publicznych, między innymi w sytuacjach transgranicznych

6.2. Proponowana nowa sekcja 9 rozporządzenia eIDAS stanowi, że kwalifikowane elektroniczne poświadczenie atrybutów wydane w jednym państwie członkowskim powinno być za takie uznawane w każdym innym państwie członkowskim.

6.3. Jednak jeśli chodzi o prawo krajowe państw członkowskich, które może się w niektórych przypadkach znacznie różnić, EKES zwraca uwagę, że atrybuty poświadczone na podstawie źródeł autentycznych w jednym państwie członkowskim powinny się ograniczać wyłącznie do potwierdzenia okoliczności faktycznych i nie powinny wywoływać skutków prawnych w innych państwach członkowskich, chyba że poświadczone atrybuty są zgodne z prawem krajowym. Zasadniczo proponowane rozwiązania prawne nie powinny wpływać na uznawanie w jednym państwie członkowskim skutków prawnych treści atrybutów poświadczonych na podstawie źródeł autentycznych w innym państwie członkowskim, analogicznie do przepisów rozporządzenia (UE) 2016/1191. Za przykład mogą posłużyć niektóre dane osobowe (dotyczące religii lub przekonań danej osoby). W niektórych krajach UE tego rodzaju informacje wywołują skutki prawne (np. w Niemczech akty stanu cywilnego zawierają informacje o religii, na których podstawie stwierdza się, czy obowiązkowe jest uiszczenie podatku kościelnego w celu zawarcia ślubu kościelnego), a w innych krajach nie ma to miejsca (np. w Polsce).

6.4. W związku z tym EKES zwraca się do Komisji Europejskiej o rozważenie wyjaśnienia treści sekcji 9, tak aby było jasne, że uznawanie kwalifikowanego elektronicznego poświadczenia atrybutów w każdym innym państwie członkowskim ogranicza się do potwierdzenia okoliczności faktycznych związanych z danym atrybutem i nie wywołuje skutków prawnych w innych państwach członkowskich, chyba że poświadczone atrybuty są zgodne z prawem krajowym.

7. **Aspekty dotyczące bezpieczeństwa**

A. **Ochrona danych w kontekście praw podstawowych**

7.1. EKES odnotowuje, że ze względu na brak wspólnych europejskich ram tożsamości cyfrowej w większości przypadków obywatele i inni mieszkańcy UE napotykają przeszkody w cyfrowej transgranicznej wymianie informacji związanych z ich tożsamością, a dodatkowo w zapewnieniu jej bezpieczeństwa i wysokiego poziomu ochrony danych.

7.2. Dlatego też EKES z zadowoleniem przyjmuje próby stworzenia interoperacyjnego i bezpiecznego systemu opartego na europejskim portfelu tożsamości cyfrowej, który może usprawnić wymianę informacji między państwami członkowskimi, między innymi odnośnie do sytuacji zatrudnienia lub praw socjalnych. W tym kontekście oczekuje, że nowe europejskie ramy tożsamości cyfrowej umożliwią na przykład szybkie zwiększenie możliwości zatrudnienia transgranicznego oraz poszerzenie automatycznego przyznawania praw socjalnych bez konieczności dopełnienia dodatkowych procedur składania wniosków lub podołania innym obciążeniom administracyjnym.

7.3. Jednak z punktu widzenia EKES-u skuteczna ochrona danych jest główną kwestią, którą trzeba rozpatrzyć w kontekście ochrony praw podstawowych, zwłaszcza prawa do prywatności i prawa do ochrony danych osobowych.

7.4. W związku z tym Komitet w pełni popiera wymóg, by europejskie ramy tożsamości cyfrowej zapewniały każdemu możliwości kontroli, kto ma dostęp do ich cyfrowego bliźniaka i dokładnie do jakich danych (w tym dostęp ze strony sektora publicznego). Jak zauważono we wniosku, będzie to wymagało wysokiego poziomu bezpieczeństwa odnośnie 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.

7.5. W tym kontekście EKES z zadowoleniem przyjmuje propozycję, by użytkownicy mieli prawo do selektywnego ujawniania swoich atrybutów, ograniczając się do tych, które są konieczne w danej sytuacji. Zgodnie z wnioskiem, korzystając z europejskiego portfela tożsamości cyfrowej, użytkownik będzie miał kontrolę nad ilością danych przekazywanych osobom trzecim i powinien otrzymać informacje o atrybutach koniecznych do wykonania danej usługi.

7.6. EKES pochwala propozycję fizycznego i logicznego oddzielenia danych osobowych związanych z wydawaniem europejskiego portfela tożsamości cyfrowej od wszelkich innych danych przechowywanych przez wydawców takich portfeli i popiera wymóg, by dostawcy usług kwalifikowanego elektronicznego poświadczania atrybutów świadczyli usługi w ramach odrębnego podmiotu prawnego.

7.7. Oprócz zagwarantowania skutecznej ochrony danych niezbędna jest również kontrola użytkowników nad ich danymi. W tym kontekście EKES popiera również stworzenie europejskich ram tożsamości cyfrowej opartych na tożsamościach prawnych wydawanych przez państwa członkowskie oraz na dostarczaniu kwalifikowanych i niekwalifikowanych atrybutów tożsamości cyfrowej.

7.8. EKES zwraca uwagę, że aby zagwarantować wysoki poziom ochrony prawnej danych użytkowników, użytkownicy powinni mieć większą kontrolę nad europejskim portfelem tożsamości cyfrowej, w tym nad identyfikowalnością dostępu do danych każdego użytkownika. W tym celu kwestie techniczne, które zostaną określone podczas dyskusji po zatwierdzeniu wniosku, powinny obejmować stworzenie rejestru umożliwiającego użytkownikowi weryfikację na żądanie wszelkich przypadków uzyskania dostępu do jego danych.

B. **Inne aspekty związane z bezpieczeństwem i odpowiedzialnością**

7.9. Zgodnie z wnioskiem nowe europejskie ramy tożsamości cyfrowej zapewnią mechanizmy zapobiegania oszustwom i uwierzytelniania danych identyfikujących osobę. Ze względu na to, że wniosek zawiera przepis wprowadzający środki umożliwiające weryfikację atrybutów w oparciu o źródła autentyczne, może to zwiększyć na przykład bezpieczeństwo dzieci w internecie, uniemożliwiając im dostęp do treści niestosownych do ich wieku. EKES zauważa, że na szczeblu krajowym tak skuteczna ochrona jest obecnie niedostępna lub wysoce nieskuteczna.

7.10. EKES z zadowoleniem przyjmuje pomysł, by przeglądarki internetowe zapewniały wsparcie odnośnie do kwalifikowanych certyfikatów uwierzytelniania witryn internetowych i interoperacyjność z nimi zgodnie z rozporządzeniem eIDAS. Powinny one uznawać i wyświetlać kwalifikowane certyfikaty uwierzytelniania witryn internetowych w celu zapewnienia wysokiego poziomu pewności, umożliwiając właścicielom stron internetowych potwierdzenie tożsamości jako właścicieli danej strony internetowej, a użytkownikom – identyfikację właścicieli stron internetowych z zachowaniem wysokiego poziomu pewności. Jednocześnie EKES dostrzega potrzebę zapewnienia prostych, szybkich i skutecznych mechanizmów odwoławczych w celu odblokowania strony internetowej, gdy zostanie ona błędnie oznaczona jako niebezpieczna. Należy również ustanowić przepisy dotyczące odpowiedzialności odnośnie do wszystkich przypadków, w których strona internetowa została błędnie zakwalifikowana jako niebezpieczna.

7.11. EKES pragnie zwrócić uwagę, że każda cyfryzacja danych budzi obawy związane z bezpieczeństwem, zwłaszcza rozbudowane systemy przechowujące i przetwarzające dane, które stanowią źródło informacji zagrożone oszustwem i utratą danych. Ma również świadomość, że obecnie nie istnieje w pełni skuteczny system bezpieczeństwa (tj. nieobarczony lukami i błędami), który całkowicie wyeliminowałby takie zagrożenie.

7.12. W związku z tym EKES zwraca uwagę, że aby zminimalizować wszelkie niepożądane sytuacje związane z danymi użytkowników, opracowana przez państwa członkowskie we współpracy z Komisją struktura techniczna europejskich ram tożsamości cyfrowej powinna koncentrować się na środkach zapewniających większe bezpieczeństwo danych i mechanizmy ich kontroli. Mechanizmy te są istotne w kontekście na przykład wykorzystywania danych zebranych od użytkowników do celów innych niż pierwotnie zamierzone. Jednocześnie EKES uważa, że należy rozwijać strukturę techniczną z poszanowaniem praw podstawowych i zasady suwerenności państw członkowskich.

7.13. Komitet odnotowuje, że art. 13 ust. 1 rozporządzenia eIDAS stanowi, iż dostawcy usług zaufania ponoszą odpowiedzialność za szkody wyrządzone w sposób zamierzony lub z powodu zaniedbania osobie fizycznej lub prawnej w związku z niewypełnieniem obowiązków określonych w rozporządzeniu (a także – zgodnie z wnioskiem Komisji – obowiązków w zakresie zarządzania ryzykiem w cyberprzestrzeni określonych w art. 18 proponowanej dyrektywy NIS 2). Przepis ten powinien być stosowany zgodnie z krajowymi przepisami dotyczącymi odpowiedzialności (art. 13 ust. 3).

7.14. Jeśli chodzi o kwestie odpowiedzialności, EKES pragnie zwrócić uwagę, że kwestie związane z definicją szkody, jej rozmiarem i należnym odszkodowaniem reguluje prawo krajowe państw członkowskich. Zgodnie z tymi zasadami odpowiedzialność dostawców usług zaufania może być ograniczona na mocy odpowiednich przepisów prawa krajowego i zasad świadczenia usług ustalanych przez dostawców.

7.15. EKES uważa, że użytkownikom europejskiego portfela tożsamości cyfrowej należy zagwarantować odszkodowanie za wszelkie niepożądane sytuacje związane z ich danymi, takie jak kradzież, utrata, ujawnienie lub wykorzystanie danych do celów innych niż pierwotnie zamierzone itp. Odpowiedzialność powinna obejmować wszystkie wyżej wymienione sytuacje, niezależnie od zamiaru lub zaniedbania dostawcy (niezależnie od winy dostawcy).

7.16. Każda kradzież, nieuprawnione ujawnienie lub utrata danych (zwłaszcza osobowych) może spowodować długotrwałą szkodę dla ich właściciela. Po udostępnieniu informacji cyfrowych wiele podmiotów może je uzyskać w perspektywie długoterminowej wbrew woli właściciela danych. EKES zachęca Komisję i państwa członkowskie do poszukiwania i rozwijania skutecznych mechanizmów, które w takich przypadkach stanowiłyby środek zaradczy dla właścicieli danych.

7.17. Rozwiązania zaproponowane w ramach nowego systemu zmuszą dostawców usług do znacznego unowocześnienia systemów bezpieczeństwa elektronicznego, ze szczególnym uwzględnieniem cyberbezpieczeństwa. EKES spodziewa się, że pociągnie to za sobą znaczne koszty i będzie wymagać modernizacji istniejącej infrastruktury informatycznej. Może to stanowić nadmierne obciążenie dla niektórych dostawców usług i wyeliminować z niektórych rynków tych dostawców, którzy nie będą mogli sobie pozwolić na dokonanie takich inwestycji w krótkim czasie. W związku z tym jego zdaniem Komisja i państwa członkowskie powinny poszukiwać rozwiązań, które chroniłyby dostawców usług przed dyskryminacją i umożliwiałyby „miękkie lądowanie" w tej dziedzinie, między innymi umożliwiając spełnienie nowych wymogów na kilku etapach i w rozsądnym terminie.

Bruksela, dnia 20 października 2021 r.

Christa SCHWENG
Przewodnicząca
Europejskiego Komitetu Ekonomiczno-Społecznego