III

(Akty przygotowawcze)

KOMITET REGIONÓW

INTERACTIO – POSIEDZENIE HYBRYDOWE – 146. SESJA PLENARNA KR-U, 12.10.2021–14.10.2021

Opinia Europejskiego Komitetu Regionów – Europejskie ramy tożsamości cyfrowej

(2022/C 61/09)

Sprawozdawca:	Mark WEINMEISTER (DE/EPL), sekretarz stanu do spraw europejskich kraju związkowego Hesja
Dokument źródłowy:	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

I. **ZALECANE POPRAWKI**

Poprawka 1

COM(2021) 281

Art. 1 pkt 4

Rozporządzenie (UE) nr 910/2014

Art. 5

Tekst zaproponowany przez Komisję Europejską	Poprawka KR-u
Pseudonimy w transakcji elektronicznej Bez uszczerbku dla skutku prawnego, jaki prawo krajowe przyznaje pseudonimom, nie zakazuje się używania pseudonimów w transakcjach elektronicznych.	Pseudonimy w transakcji elektronicznej Bez uszczerbku dla skutku prawnego, jaki prawo krajowe przyznaje pseudonimom, nie zakazuje się używania pseudonimów w transakcjach elektronicznych ***ani przy korzystaniu z serwisów społecznościowych***.

Uzasadnienie

Portale społecznościowe nie mogą zakazywać stosowania pseudonimów podczas rejestracji, powołując się na europejski portfel tożsamości cyfrowej.

Poprawka 2

COM(2021) 281

Art. 1 pkt 7

Rozporządzenie (UE) nr 910/2014

Art. 6a ust. 1

Tekst zaproponowany przez Komisję Europejską	Poprawka KR-u
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.	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 ***24*** miesięcy od wejścia w życie niniejszego rozporządzenia.

Uzasadnienie

Doświadczenie wskazuje, że europejskie portfele tożsamości cyfrowej będą istotnym celem ataków na systemy informatyczne. W tak delikatnym środowisku danych osobowych jakość ma pierwszeństwo przed szybkością. Terminy transpozycji na szczeblu krajowym są zbyt krótkie (i częściowo zależne od przepisów dyrektywy NIS 2). Konieczne jest zatem przedłużenie okresu przejściowego.

Poprawka 3

COM(2021) 281 final – Sekcja 1

Art. 1 pkt 7

Rozporządzenie (UE) nr 910/2014

Art. 6a ust. 12 (nowy)

Tekst zaproponowany przez Komisję Europejską	Poprawka KR-u
	Europejski portfel tożsamości cyfrowej udostępnia się osobom poniżej 18. roku życia wyłącznie pod warunkiem że ich tożsamość została uwierzytelniona za pomocą elektronicznego dowodu tożsamości przedstawiciela prawnego osoby małoletniej, który ponosi za nią odpowiedzialność.

Uzasadnienie

Europejski portfel tożsamości cyfrowej będzie służył za dowód tożsamości w internecie i poza nim. Osoby nieletnie nie mogą być w pełni pociągane do odpowiedzialności i rozliczane za ewentualne skutki prawne swych działań.

Poprawka 4

COM(2021) 281 final – Sekcja 1

Art. 1 pkt 7

Rozporządzenie (UE) nr 910/2014

Art. 6c ust. 5

Tekst zaproponowany przez Komisję Europejską	Poprawka KR-u
Państwa członkowskie przekazują Komisji nazwy i adresy podmiotów publicznych lub prywatnych, o których mowa w ust. 3. Komisja udostępnia te informacje państwom członkowskim.	Państwa członkowskie przekazują Komisji nazwy i adresy podmiotów publicznych lub prywatnych, o których mowa w ust. 3. Komisja udostępnia te informacje państwom członkowskim ***nie później niż sześć miesięcy po wejściu w życie rozporządzenia***.

Uzasadnienie

Należy zmienić art. 6c ust. 5 rozporządzenia (UE) nr 910/2014, ponieważ należy wyznaczyć ostateczny termin przekazania informacji.

Poprawka 5

COM(2021) 281

Art. 1 pkt 9

Rozporządzenie (UE) nr 910/2014

Art. 7

Tekst zaproponowany przez Komisję Europejską	Poprawka KR-u
„[…] w terminie ***12*** miesięcy od wejścia w życie […]”.	„[…] w terminie ***24*** miesięcy od wejścia w życie […]”.

Uzasadnienie

Doświadczenie wskazuje, że europejskie portfele tożsamości cyfrowej będą istotnym celem ataków na systemy informatyczne. W tak delikatnym środowisku danych osobowych jakość ma pierwszeństwo przed szybkością. Terminy transpozycji na szczeblu krajowym są zbyt krótkie (i częściowo zależne od przepisów dyrektywy NIS 2). Konieczne jest zatem przedłużenie okresu przejściowego.

Poprawka 6

COM(2021) 281

Art. 1 pkt 11

Rozporządzenie (UE) nr 910/2014

Art. 10a ust. 4

Tekst zaproponowany przez Komisję Europejską	Poprawka KR-u
Komisja bez zbędnej zwłoki publikuje w Dzienniku Urzędowym Unii Europejskiej odpowiednie zmiany w wykazie, o którym mowa w art. 6d.	Komisja bez zbędnej zwłoki publikuje w Dzienniku Urzędowym Unii Europejskiej odpowiednie zmiany w wykazie, o którym mowa w art. 6d***., i udostępnia te zmiany w oddzielnym wykazie***.

Uzasadnienie

Przejrzysty wykaz (lista zablokowanych portfeli cyfrowych) ma na celu ułatwienie jego stosowania.

Poprawka 7

COM (2021) 281 – Sekcja 1

Art. 1 pkt 12

Rozporządzenie (UE) nr 910/2014

Artykuł 11a ust. 4 (nowy)

Tekst zaproponowany przez Komisję Europejską	Poprawka KR-u
	Państwa członkowskie za pomocą niepowtarzalnego środka identyfikacji gwarantują, że żaden obywatel nie może otrzymać dwóch lub większej liczby europejskich portfeli tożsamości cyfrowej na podstawie obywatelstwa różnych państw członkowskich lub miejsca zamieszkania w różnych państwach członkowskich.

Uzasadnienie

Należy zadbać o to, by obywatele posiadający różne obywatelstwa lub mający miejsce zamieszkania w różnych państwach członkowskich UE otrzymywali tylko jeden europejski portfel tożsamości cyfrowej.

Poprawka 8

COM (2021) 281 – Sekcja 1

Art. 1 pkt 14

Rozporządzenie (UE) nr 910/2014

Art. 12a ust. 3

Tekst zaproponowany przez Komisję Europejską	Poprawka KR-u
Państwa członkowskie zgłaszają Komisji nazwy i adresy podmiotów publicznych lub prywatnych, o których mowa w ust. 1. Komisja udostępnia te informacje państwom członkowskim.	Państwa członkowskie zgłaszają Komisji nazwy i adresy podmiotów publicznych lub prywatnych, o których mowa w ust. 1. Komisja udostępnia te informacje państwom członkowskim ***nie później niż sześć miesięcy po wejściu w życie rozporządzenia***.

Uzasadnienie

Należy zmienić art. 12a ust. 3 rozporządzenia (UE) nr 910/2014, ponieważ należy wyznaczyć ostateczny termin przekazania informacji.

Poprawka 9

COM(2021) 281

Art. 1 pkt 29

Rozporządzenie (UE) nr 910/2014

Art. 30 ust. 3a

Tekst zaproponowany przez Komisję Europejską	Poprawka KR-u
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.	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. ***Ponowna certyfikacja może nastąpić najwcześniej po okresie oczekiwania wynoszącym 2 lata i po nowej ocenie podatności na zagrożenia.***

Uzasadnienie

Sensowne byłoby wprowadzenie minimalnego okresu przed ponowną certyfikacją, żeby zapewnić czas na usunięcie niedociągnięć lub po wprowadzeniu zupełnie nowego systemu technicznego.

II. **ZALECENIA POLITYCZNE**

EUROPEJSKI KOMITET REGIONÓW

Wprowadzenie

1. Popiera ideę europejskiego portfela tożsamości cyfrowej. Za pomocą takiego portfela cyfrowego obywatelki i obywatele powinni mieć też możliwość udowodnić swoją tożsamość w zastosowaniach mobilnych, aby uzyskać dostęp do elektronicznych usług administracji publicznej, wymiany dokumentów cyfrowych lub by móc udowodnić określoną cechę osobistą, np. wiek. Jest to możliwe bez ujawniania ich tożsamości lub innych danych osobowych.

2. Z zadowoleniem przyjmuje propozycje Komisji Europejskiej dotyczące stworzenia europejskiej tożsamości cyfrowej w postaci bardziej kompleksowego europejskiego portfela tożsamości cyfrowej oraz niezbędne zmiany w rozporządzeniu w sprawie identyfikacji elektronicznej i usług zaufania (rozporządzenie eIDAS). Europejski portfel tożsamości cyfrowej nie ogranicza się do danych osobowych sensu stricto (EUid), ale powinien również zawierać inne dokumenty (w tym urzędowe) w formie elektronicznej, takie jak prawo jazdy lub kwalifikacje uzyskane w ramach kształcenia.

3. W świetle zmieniających się wymogów rynkowych popiera cel Komisji Europejskiej, jakim jest dalszy rozwój rozporządzenia eIDAS pod kątem zastosowań w gospodarce przy jednoczesnym dalszym wykorzystywaniu istniejących środków identyfikacji, uznanych w poszczególnych krajach. Bezpieczne środki identyfikacji elektronicznej mają szczególne znaczenie dla cyfryzacji procedur administracyjnych.

4. Apeluje o jasne przepisy dotyczące ochrony danych we wniosku Komisji Europejskiej dotyczącym europejskiej tożsamości cyfrowej, które powinny być zgodne z zasadami określonymi w ogólnym rozporządzeniu o ochronie danych (RODO), zwłaszcza z zasadami dotyczącymi gospodarki opartej na danych, prywatności danych i odpowiedniego uzasadnienia, a także zapewniać użytkownikom możliwość kontrolowania, które dane chcą udostępniać i komu.

5. Uważa europejski portfel tożsamości cyfrowej, dzięki jego uniwersalnej użyteczności, a w szczególności mobilnemu wykorzystaniu, za narzędzie, które ma ułatwić uczestniczenie w życiu społecznym, a dzięki wykorzystaniu w całej UE może w świadomości każdej obywatelki i każdego obywatela UE stać się elementem bezpośrednio doświadczanej tożsamości europejskiej.

Korzyści dla obywatelek i obywateli

6. Uważa utworzenie europejskiego portfela cyfrowego za doskonałą okazję do zakorzenienia wśród obywateli dostrzegalnej fizycznie i przydatnej na co dzień europejskiej tożsamości – również na jednolitym rynku. Europejski portfel tożsamości cyfrowej stanowi jednoznacznie integrujący identyfikator dla wszystkich użytkowników, co w symbolicznym znaczeniu znacznie wykracza poza czysto techniczną korzyść.

7. Stwierdza, że europejski portfel tożsamości cyfrowej jest zasadniczo nastawiony na zastosowania mobilne i może zachować swoją użyteczność także wraz z dalszym rozwojem obecnych urządzeń mobilnych (smartfonów lub inteligentnych zegarków). Nowe technologie, np. okulary cyfrowe (okulary rzeczywistości rozszerzonej lub cyfrowe awatary) lub podobne cyfrowe narzędzia użytku codziennego powinny za pośrednictwem odpowiedniego interfejsu (w razie potrzeby optycznie) móc korzystać z europejskiego portfela tożsamości cyfrowej.

8. Zaleca, by opracowanie i wdrożenie europejskiej identyfikacji elektronicznej i europejskiego portfela tożsamości cyfrowej było nastawione na świadczenia takich usług, które dla obywatelek i obywateli oznaczają rzeczywistą transgraniczną wartość dodaną.

9. Podkreśla, że wszystkim użytkowniczkom i użytkownikom należy zagwarantować suwerenność i niedyskryminację. Dlatego zaleca, by w komunikacie wyraźnie zaznaczyć, że przy oferowaniu usług osobom fizycznym nie można stosować pośredniego przymusu do korzystania z europejskiego portfela tożsamości cyfrowej. Jego stosowanie powinno być co do zasady dobrowolne.

10. Podkreśla, że europejski portfel tożsamości cyfrowej powinien być prezentowany jako oferta dla obywatelek i obywateli, tak aby został dobrze przyjęty przez społeczeństwo obywatelskie.

11. Wzywa, by zalecono prosty projekt portfela tożsamości cyfrowej w postaci zestawu narzędzi, wykraczający poza wymogi ochrony danych i dostępności, który również osobom z niewielkimi ograniczeniami lub nieznajomością języka umożliwiałby korzystanie z europejskiego portfela tożsamości cyfrowej (np. poprzez częstsze piktogramy).

12. Sugeruje, by przy opracowywaniu przepisów przewidzieć przypadki korzystania z tożsamości cyfrowej przez małoletnich lub w ramach opieki nad osobami małoletnimi oraz kurateli, a także by uwzględnić aspekt postępowania z tożsamością cyfrową w przypadku śmierci.

Zaangażowanie środowiska biznesu

13. Uważa, że zasadnicze znaczenie dla powodzenia tej inicjatywy ma ścisłe zaangażowanie liderów technologii, właśnie dzięki otwarciu obowiązujących przepisów w odniesieniu do przemysłu. Tylko rozwiązanie dostosowane do rynku zagwarantuje szerokie stosowanie cyfrowego portfela w UE.

14. Przypomina o zasadniczym aspekcie ekonomicznej użyteczności dzięki wykorzystaniu interfejsów płatności elektronicznych (Paypal, Google/Apple-Pay, SWIFT itp.), które w gospodarce opierają się obecnie na rachunkach właścicieli kont. Europejski portfel tożsamości cyfrowej powinien uwzględniać odpowiednie przepisy dotyczące prania pieniędzy i walut cyfrowych (Bitcoin, Ethereum, Digital EUR itp.).

15. Apeluje, by przy wykorzystywaniu europejskiego portfela tożsamości cyfrowej do celów gospodarczych uwzględniać dwa istniejące i zasadniczo konkurencyjne modele biznesowe.

Z jednej strony są to główne globalne sieci społecznościowe, które mają uzasadniony interes w uznaniu swych pseudokont, choćby za pośrednictwem instytucji publicznej. Podważyłoby to jednak swobodę korzystania z internetu i wypchnęło użytkowników z obszaru chronionego internetu do ciemnej sieci. Z punktu widzenia Komitetu Regionów nie jest to pożądane.

Z drugiej strony istnieją dostawcy tożsamości, którzy oferują konkurencyjne do europejskiego portfele cyfrowe i również chcą korzystać z opcji tożsamości potwierdzonej przez instytucję publiczną.

16. Zaleca, aby metodykę kontroli uprawnień do uzyskania dostępu przez podmioty gospodarcze za pomocą zabezpieczonego certyfikatu zaprojektować w taki sposób, aby ważność tego certyfikatu była ograniczona w czasie lub cyklicznie kontrolowana. Komitet Regionów z zadowoleniem przyjmuje podobne refleksje na temat dostawców usług zaufania i zwraca uwagę na bezwzględną konieczność zadbania o to, by uzasadnione zapotrzebowanie instytucji lub organizacji na dane z europejskiego portfela nie było nadużywane.

17. Zauważa, że w niektórych państwach członkowskich opracowano już rozwiązania cyfrowe dla sektora publicznego i prywatnego i że są one tam stosowane. Te charakterystyczne dla poszczególnych krajów rozwiązania powinny zostać w możliwie największym stopniu włączone do europejskiej identyfikacji elektronicznej z dwóch powodów. Po pierwsze, zmiany w istniejących już systemach wiązałyby się ze znacznym obciążeniem administracyjnym i finansowym, a po drugie, przez lata obywatelki i obywatele tych państw członkowskich nabrali wysokiego zaufania do wspomnianych systemów. Nie można zatem pozwolić, by wprowadzenie europejskiej identyfikacji elektronicznej podważyło to zaufanie.

Wdrażanie i uczestnictwo państw członkowskich

18. Dlatego usilnie namawia, by eksperci krajowi byli ściśle zaangażowani w realizację zalecenia dla państw członkowskich, które Komisja zawarła we wniosku ustawodawczym dotyczącym opracowania wspólnego zestawu narzędzi na potrzeby skoordynowanego podejścia w celu stworzenia niezbędnych ram technicznych dla europejskiego portfela tożsamości cyfrowej.

Należy uwzględnić istniejące przykłady najlepszych praktyk, takie jak wyniki i doświadczenia związane z krajowymi projektami w zakresie tożsamości cyfrowej i bezpiecznej tożsamości cyfrowej.

19. Uważa, że przy rozważaniu kosztów i wydatków poniesionych w związku z planowaniem konieczne jest również zebranie krajowych parametrów i połączenie ich w całościowy plan UE, współmierny do kosztów. W tym kontekście, oprócz terminów dla UE, należy zwłaszcza śledzić i uwzględniać krajowe harmonogramy wdrażania.

20. Apeluje, by w ogólnym planowaniu brać pod uwagę krajowe oraz regionalne i lokalne wydatki pieniężne i wydatki na zasoby ludzkie na realizację tego przedsięwzięcia. Europejski portfel tożsamości cyfrowej wtedy odniesie sukces, gdy będzie można go odpowiednio często wykorzystywać.

Oprócz przedsiębiorstw kluczową rolę odgrywają tu administracje krajowe wszystkich szczebli. Ze względu na ich działalność, ale również z uwagi na inicjatywy Komisji, ten trend coraz bardziej ich dotyczy. Dyrektywa usługowa UE lub portal UE wnoszą cenny wkład w cyfryzację jednolitego rynku UE.

21. Komitet sugeruje stopniowe wdrażanie, zwłaszcza w fazie początkowej. Jest to ważne ze względu na niekiedy całkowicie nowe otwarcie dotychczas nieuregulowanej gospodarki na stosowanie elektronicznych tożsamości na „istotnym" czy wręcz „wysokim" poziomie zaufania przy rozwijaniu obecnego kontekstu regulacji eIDAS.

Ochrona danych i cyberbezpieczeństwo

22. Mając na uwadze ryzyko techniczne związane ze scentralizowanym przechowywaniem danych dotyczących tożsamości w głównie mobilnych zastosowaniach, ostrzega przed pospiesznym wdrażaniem europejskiego portfela tożsamości cyfrowej. Będzie on bez wątpienia znaczącym celem dla najróżniejszych cyberataków i dlatego musi być odporny na obecne i przyszłe zagrożenia.

23. Zwraca uwagę na znaczenie odpowiedniej definicji systemów certyfikacji portfeli tożsamości cyfrowej i systemów identyfikacji elektronicznej, które nie powinny być opracowywane przez podmiot gospodarczy, lecz przez Agencję Unii Europejskiej ds. Cyberbezpieczeństwa (ENISA) w ścisłej współpracy z grupami ekspertów, w tym z przedstawicielami władz lokalnych i regionalnych.

24. Zwraca uwagę na ryzyko centralnego łączenia rodzajów tożsamości o różnym stopniu poufności w jeden element techniczny. Jeżeli zostaną one w sposób nieuprawniony użyte przez osoby trzecie, stwarza to ogromne ryzyko dla uprawnionego użytkownika. Oprócz szkód finansowych można sobie wyobrazić również naruszenie dobrego imienia i wizerunku. Także ukierunkowany phishing może spowodować znaczne szkody.

25. Wzywa do takiego technicznego wdrożenia europejskiego portfela tożsamości cyfrowej, aby był on wystarczająco zabezpieczony przed cyberatakami oraz aby odpowiednie urządzenia blokujące i specjalne zabezpieczone systemy rezerwowe umożliwiały bezpieczne ponowne zainstalowanie przez uprawnionego użytkownika.

Zabezpieczanie europejskiego portfela tożsamości cyfrowej przed zagrożeniami musi być procesem ciągłym. Uwzględnienie bezpieczeństwa już w fazie projektowania jest podstawą długofalowego i skutecznego użytkowania i ma zasadnicze znaczenie dla stosowania w gospodarce. Dlatego aspekt ten należy uwzględnić już na etapie definiowania zestawu narzędzi.

26. Uważa, że oprócz wymogów w zakresie ochrony danych, dostępności i cyberbezpieczeństwa kluczowe znaczenie dla powodzenia ma znalezienie spójnego metodologicznie i dostosowanego do grupy docelowej użytkowników rozwiązania zawierającego informacje i dokumentację.

27. Proponuje, aby wiążące przepisy nakładały na usługodawców obowiązek zasadniczo prostego i przejrzystego dostępu do danych z europejskiego portfela tożsamości cyfrowej za pomocą jednolitych narzędzi (np. pulpitu nawigacyjnego) oraz ich widocznego wyświetlania użytkownikom.

28. Wzywa do takiego ukierunkowania projektu europejskiej tożsamości cyfrowej, aby był on zgodny z celem europejskiej odporności cyfrowej i wspierał suwerenność cyfrową UE.

29. Zachęca do zastanowienia się nad możliwością stworzenia ogólnej podstawy technicznej do obsługi podstawowych funkcji europejskiego portfela tożsamości cyfrowej poprzez zapewnienie certyfikowanego i udostępnianego przez UE zestawu narzędzi w ramach otwartego oprogramowania. Utrzymanie i dalszy rozwój tego zestawu narzędzi powinno być następnie koordynowane przez UE.

Włączenie w procesy użytkowania

30. Zaleca, aby przy przekładaniu europejskiego portfela tożsamości cyfrowej na konkretne zastosowania wprowadzić obowiązek przedstawienia całego procesu użytkowania w formie zrozumiałej i adresowanej do docelowej grupy użytkowników.

Europejski portfel tożsamości cyfrowej należy prezentować w instrukcjach użytkowania jako jednorodny element z unikalnymi interfejsami do przesyłania danych i za pomocą wyraźnej symboliki i elementów projektu przedstawiać jako produkt UE.

31. Sugeruje, aby operacje z wykorzystaniem europejskiego portfela tożsamości cyfrowej zostały w jak największym stopniu ujednolicone, tak aby użytkownicy mogli niemal rutynowo je wykonywać, przy jednoczesnym uwzględnieniu wymogów dotyczących minimalizacji danych. Taka rutyna nie tylko ułatwia korzystanie, ale też pozwoli osobom nieobeznanym z narzędziami informatycznymi uniknąć nieprawidłowego stosowania.

Komunikacja i akceptacja

32. Uważa, że konieczne jest intensywne informowanie obywatelek i obywateli UE o europejskim portfelu tożsamości cyfrowej oraz o możliwościach, jakie oferuje on na rynku wewnętrznym UE, a także o dbałości o wysoki poziom ochrony i bezpieczeństwa danych. Zwraca uwagę na to, że szybka łączność dla wszystkich w Unii Europejskiej, również na obszarach wiejskich i oddalonych, jest niezbędnym warunkiem dla tego, by obywatelki i obywatele korzystali z europejskiego portfela tożsamości cyfrowej i go zaakceptowali.

33. Opowiada się za tym, by podstawowe zastosowanie europejskiego portfela tożsamości cyfrowej rozszerzyć do nośnika europejskiej tożsamości na całym świecie, obejmującego takie komponenty jak paszport (np. cyfrowe rejestrowanie wiz) czy oficjalne świadectwo szczepienia UE. W tym sensie warto zawrzeć porozumienia, które umożliwiałyby korzystanie z europejskiego portfela tożsamości cyfrowej wraz z zawartymi w nim danymi uwierzytelniającymi również poza UE.

34. Apeluje do Komisji Europejskiej o podjęcie intensywnych rozmów i negocjacji z dostawcami sprzętu na temat technicznych aspektów udostępnienia europejskiego portfela tożsamości cyfrowej użytkownikom końcowym. Celem jest jak najszybsze udostępnienie bazy technicznej również w segmencie niskich cen.

Już teraz dostępne są typy urządzeń ze średniego i wyższego segmentu cenowego z wystarczającą certyfikacją wymaganą dla „znacznego” poziomu zaufania według systemu eIDAS. Dla upowszechnienia europejskiego portfela tożsamości cyfrowej warto zadbać także o jak największe zaangażowanie przemysłu jako dostawcy usług.

Zasada pomocniczości

35. Stwierdza, że wniosek jest zgodny z zasadą pomocniczości. Tego typu ogólnounijny projekt techniczny przyniesie efekt tylko wtedy, gdy jego przepisy będą wystarczająco jednolite. Odpowiednie przepisy krajowe będą regulować ostateczny kształt, zaś ocenie podlegać będą jedynie narzędzia przekrojowe z zestawu narzędzi.

Bruksela, dnia 12 października 2021 r.

Apostolos TZITZIKOSTAS

Przewodniczący
Europejskiego Komitetu Regionów