Parlament Europejski
2019-2024

Komisja Wolności Obywatelskich, Sprawiedliwości i Spraw Wewnętrznych

2021/0136(COD)

18.5.2022

PROJEKT OPINII

Komisji Wolności Obywatelskich, Sprawiedliwości i Spraw Wewnętrznych

dla Komisji Przemysłu, Badań Naukowych i Energii

w sprawie wniosku dotyczącego rozporządzenia Parlamentu Europejskiego i Rady zmieniającego rozporządzenie (UE) nr 910/2014 w odniesieniu do ustanowienia europejskich ram tożsamości cyfrowej
(COM(2021)0281 – C9-0200/2021 – 2021/0136(COD))

Sprawozdawca komisji opiniodawczej: Cristian Terheş

PA_Legam

ZWIĘZŁE UZASADNIENIE

W niniejszym projekcie opinii poruszono kilka kwestii dotyczących wniosku Komisji, w szczególności aspekty ochrony danych i prywatności, które wchodzą w zakres kompetencji Komisji Wolności Obywatelskich, Sprawiedliwości i Spraw Wewnętrznych (LIBE). Niektóre z tych kwestii były już podnoszone przez Europejskiego Inspektora Ochrony Danych oraz zainteresowane strony, z którymi przeprowadzono konsultacje w trakcie przygotowywania projektu opinii. Sprawozdawca komisji opiniodawczej pragnie je uwypuklić, opierając się przy tym na pisemnych uwagach otrzymanych od różnych ekspertów w tej dziedzinie.

Obecny wniosek ma charakter bardzo techniczny, a przy tym dotyczy kluczowych aspektów praw podstawowych, takich jak ochrona danych i prywatność. Jeżeli Parlament nie przedstawi spójnych ram i solidnego technicznie aktu prawnego, obywatele utracą wszelką kontrolę nad swoimi prywatnymi danymi, które staną się towarem. Niestety o technicznych opcjach wdrożenia wniosku ma zadecydować Komisję w drodze kolejnych aktów o charakterze nieustawodawczym. Jest to niebezpieczne podejście, ponieważ pewne opcje techniczne mogą być bardziej inwazyjne niż inne, kosztem praw podstawowych obywateli.

Bardziej szczegółowe obawy można by zgłosić odnośnie do niejasnego związku między eIDAS a RODO, a mianowicie: poszanowanie podstawowych elementów ochrony danych, takich jak minimalizacja danych i selektywne ujawnianie, uwzględnianie ochrony prywatności już w fazie projektowania a stosowanie niepowtarzalnych identyfikatorów, brak otwartości i przejrzystości w opracowywaniu specyfikacji bezpieczeństwa portfela eIDAS oraz brak zaangażowania społeczeństwa obywatelskiego lub pracowników naukowych; zależność od dużych przedsiębiorstw technologicznych; osłabienie bezpieczeństwa przeglądarki.

Za pomocą proponowanych poprawek sprawozdawca komisji opiniodawczej LIBE dąży do skorygowania wyżej wymienionych kwestii, które wchodzą w zakres kompetencji komisji LIBE. Aby ochronić prywatność osób fizycznych i nie szkodzić standardom prywatności użytkowników europejskiego portfela tożsamości cyfrowej, sprawozdawca komisji opiniodawczej rozważa scenariusz, w którym stosowanie pseudonimów musi być opcją dostępną we wszystkich przypadkach, w których pełna identyfikacja nie jest prawnie wymagana. Ponadto przywrócono odniesienia do związku między eIDAS a europejskimi przepisami dotyczącymi ochrony danych przy poziomie ochrony z 2014 r.

Eksperci w tej dziedzinie powszechnie uznali potrzebę zapobieżenia możliwości tworzenia powiązań i identyfikacji. Transakcje użytkowników ujawniają duże ilości danych, w tym dane o wysoce osobistym charakterze, takie jak informacje o sytuacji ekonomicznej osób fizycznych lub informacje o sytuacji medycznej, historii podróży, wzorcach konsumpcji i interakcjach społecznych obywateli. W związku z tym w rozważanej strukturze przepisów należy chronić przed scentralizowanym nadzorem te dane dotyczące szerokiego zakresu zachowań użytkowników w internecie i poza nim.

Ponadto niepowtarzalny i trwały identyfikator osób fizycznych byłby w niektórych państwach członkowskich niezgodny z prawem, a nawet niezgodny z konstytucją (np. w Niemczech stosowanie niepowtarzalnych trwałych identyfikatorów jest zabronione na mocy orzeczenia w sprawie ustawy o spisie powszechnym z 1983 r.). Ryzyka związanego z niepowtarzalnym, przypisanym na całe życie identyfikatorem nie można uznać za najmniej inwazyjną metodę

stosowaną do celów jednoznacznej identyfikacji osoby fizycznej. Art. 11a również nie jest potrzebny, ponieważ istniejące ramy interoperacyjności systemów identyfikacji zgodnie z pierwotnym art. 12 ust. 4 lit. d) przewidują już jednoznaczne reprezentowanie osoby fizycznej w przypadku spraw transgranicznych, w związku z czym zaproponowano jego skreślenie.

Niemniej jednak wniosek zawiera wiele luk wykraczających poza kompetencje komisji LIBE, dlatego też, aby chronić prawa podstawowe Europejczyków, cały wniosek powinien zostać odesłany do Komisji w celu całkowitego przeprojektowania. Wniosek ten w obecnym kształcie doprowadziłby do „schińszczenia" Europy i umożliwiłoby stworzenie podobnego do chińskiego systemu wiarygodności społecznej, który oznaczałby masowy nadzór i kontrolę nad wszystkimi Europejczykami, czego nie można zaakceptować. UE została stworzona jako „przestrzeń wolności" i należy kontynuować wysiłki na rzecz utrzymania jej jako takiej.

POPRAWKI

Komisja Wolności Obywatelskich, Sprawiedliwości i Spraw Wewnętrznych zwraca się do Komisji Przemysłu, Badań Naukowych i Energii, jako komisji przedmiotowo właściwej, o wzięcie pod uwagę następujących poprawek:

Poprawka 1

Wniosek dotyczący rozporządzenia
Motyw 6

Tekst proponowany przez Komisję	*Poprawka*
(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.	(6) ***Podmiotem tożsamości cyfrowej jest osoba fizyczna lub prawna, do której należą dane identyfikujące tę osobę.*** 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.
[19] Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku	[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.	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.

Or. en

Poprawka 2

Wniosek dotyczący rozporządzenia
Motyw 11

Tekst proponowany przez Komisję	*Poprawka*
(11) Europejskie portfele tożsamości cyfrowej powinny zapewniać najwyższy poziom bezpieczeństwa danych osobowych wykorzystywanych do uwierzytelniania 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.	(11) Europejskie portfele tożsamości cyfrowej powinny zapewniać najwyższy poziom bezpieczeństwa danych osobowych wykorzystywanych do uwierzytelniania 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 ***nie powinno być warunkiem wstępnym korzystania*** z ***europejskiego portfela tożsamości cyfrowej, niezależnie od wymogu silnego uwierzytelniania użytkownika. Dane biometryczne do celów jednoznacznej*** identyfikacji ***osoby fizycznej w kontekście niniejszego rozporządzenia nie powinny być przechowywane w chmurze***. 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.

Or. en

Uzasadnienie

Aby zapewnić użytkownikom kontrolę nad ich danymi w europejskich portfelach tożsamości cyfrowej, planowany system nie powinien zależeć od infrastruktury opartej na chmurze.

Poprawka 3

Wniosek dotyczący rozporządzenia
Motyw 29

Tekst proponowany przez Komisję	*Poprawka*
(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.	(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. ***Mechanizmy walidacji europejskiego portfela tożsamości cyfrowej, selektywne ujawnianie i uwierzytelnianie użytkowników w celu uzyskania dostępu do usług online powinny zapewniać ochronę prywatności, uniemożliwiać śledzenie użytkownika i gwarantować poszanowanie prawa do anonimowości i pseudonimizacji.***

Or. en

Uzasadnienie

Podstawowe funkcje portfela muszą być wdrażane w sposób chroniący prywatność, aby ograniczyć możliwość automatycznego śledzenia użytkowników w przypadkach, gdy decydują się oni anulować już zainicjowany wniosek o udostępnienie informacji od strony ufającej, decydując się jedynie na selektywne ujawnienie poszczególnych atrybutów ich dotyczących (np. weryfikacja wieku w sklepie alkoholowym) lub korzystają z portfela w celu zalogowania się do usług, nie stając się następnie dla nich obiektem śledzenia. Ostatnią funkcję oferuje Apple „Logowanie za pomocą konta Apple ID”, którą portfel ma zastąpić.

Poprawka 4

Wniosek dotyczący rozporządzenia
Artykuł 1 – akapit 1 – punkt 3 – litera i

Rozporządzenie (UE) nr 910/2014
Artykuł 3 – akapit 1 – punkt 47

Tekst proponowany przez Komisję	*Poprawka*
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***;	47) »archiwizacja elektroniczna« oznacza usługę zapewniającą ***otrzymywanie***, przechowywanie, usuwanie i transmisję danych lub dokumentów elektronicznych w celu ***zapewnienia dowodu*** ich ***autentyczności*** i ***integralności*** przez cały okres ***ich przechowywania***;

Or. en

Poprawka 5

Wniosek dotyczący rozporządzenia
Artykuł 1 – akapit 1 – punkt 4
Rozporządzenie (UE) nr 910/2014
Artykuł 5 – akapit 1

Tekst proponowany przez Komisję	*Poprawka*
Bez uszczerbku dla skutku prawnego, jaki prawo krajowe przyznaje pseudonimom, nie zakazuje się używania pseudonimów w transakcjach elektronicznych.;	Bez uszczerbku dla skutku prawnego, jaki prawo krajowe przyznaje pseudonimom, nie zakazuje się używania pseudonimów ***i tożsamości suwerennych*** w transakcjach elektronicznych.***"; zawsze istnieje możliwość stosowania pseudonimów w celu zastąpienia niepowtarzalnego identyfikatora lub w przypadku uwierzytelniania przez prywatne strony ufające;*** ***przetwarzanie danych osobowych odbywa się zgodnie z rozporządzeniem (UE) 2016/679, w szczególności poprzez wdrożenie zasady uwzględniania ochrony danych już w fazie projektowania i domyślnej ochrony danych;***

Or. en

Uzasadnienie

Aby ochronić prywatność osób fizycznych i nie szkodzić standardom prywatności

użytkowników europejskiego portfela tożsamości cyfrowej, stosowanie pseudonimów musi być opcją dostępną we wszystkich przypadkach, w których pełna identyfikacja nie jest prawnie wymagana. Przywrócenie odniesienia do związku między eIDAS a europejskimi przepisami dotyczącymi ochrony danych przy poziomie ochrony z 2014 r. Pierwotne rozporządzenie eIDAS zapewniało wyższy standard ochrony danych niż ten przewidziany w dyrektywie 95/46/WE, przewidując w art. 12 ust. 3 lit. c) wymóg ułatwienia realizacji zasady uwzględnienia ochrony prywatności już w fazie projektowania.

Poprawka 6

Wniosek dotyczący rozporządzenia
Artykuł 1 – akapit 1 – punkt 7
Rozporządzenie (UE) nr 910/2014
Artykuł 6 a – ustęp 4 – litera a – punkt 2 a (nowy)

Tekst proponowany przez Komisję	*Poprawka*
	2a) dla stron ufających w celu jednoznacznej identyfikacji, a także, aby ich wnioski o informacje ograniczały się do elementów zatwierdzonych przez państwo członkowskie zgodnie z art. 6b ust. 1;

Or. en

Uzasadnienie

Wspólny interfejs powinien zawierać to zabezpieczenie, aby uniemożliwić niezatwierdzonym lub niezidentyfikowanym ufającym stronom zwracanie się o informacje wykraczające poza to, co w danym przypadku jest przewidziane. Grupa ekspertów eIDAS zorganizowana przez Komisję Europejską uznała potrzebę „uzgodnionej polityki", która ograniczałaby informacje, których strona ufająca może zażądać od użytkownika, i zapobiegałaby wnioskom o udzielenie zbyt wielu informacji (zob. rozdział 4.6.1 i przypis 22 dokumentu końcowego z dnia 17 lutego 2022 r.).

Poprawka 7

Wniosek dotyczący rozporządzenia
Artykuł 1 – akapit 1 – punkt 7
Rozporządzenie (UE) nr 910/2014
Artykuł 6 a – ustęp 4 – litera a – punkt 2 b (nowy)

Tekst proponowany przez Komisję	*Poprawka*

2b) w celu należy dopilnowania, aby podmioty zastępcze, które działają jako pośrednicy między stronami ufającymi a europejskimi portfelami tożsamości cyfrowej, nie uzyskiwały wiedzy na temat treści transakcji;

Or. en

Uzasadnienie

Wspólny interfejs powinien zapewniać, aby pełnomocnicy działający jako pośrednicy między stronami ufającymi a użytkownikami europejskiego portfela tożsamości cyfrowej nie mieli dostępu do treści przekazywanej przez siebie transakcji. Takie zabezpieczenia techniczne są powszechne i nie ograniczają funkcjonowania systemu. Istnienie takich pełnomocnictw zostało uznane przez grupę ekspertów eIDAS (zob. rozdział 4.8.3 dokumentu końcowego z dnia 17 lutego 2022 r.).

Poprawka 8

Wniosek dotyczący rozporządzenia
Artykuł 1 – akapit 1 – punkt 7
Rozporządzenie (UE) nr 910/2014
Artykuł 6 a – ustęp 4 – litera a – punkt 3

Tekst proponowany przez Komisję	*Poprawka*
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***;***	3) w celu przedstawiania stronom ufającym danych identyfikujących osobę, ***takich jak dane uwierzytelniające,*** elektronicznego poświadczenia atrybutów lub innych danych, w trybie lokalnym niewymagającym dostępu internetowego do portfela ***oraz w celu podjęcia przez użytkownika świadomej decyzji w sprawie udostępnienia stronom ufającym informacji osobowych. Obejmuje to identyfikację strony ufającej, całkowitą lub częściową odmowę udzielenia informacji stronom ufającym, pełną historię transakcji oraz informacje na temat wykonywania praw przysługujących osobie, której dane dotyczą.***

Or. en

Uzasadnienie

Pomyślna realizacja europejskiego portfela tożsamości cyfrowej zależy od możliwości podejmowania przez obywateli świadomych decyzji w sprawie informacji udostępnianych stronom ufającym. Podobne wytyczne dotyczące obowiązkowych informacji na temat celu przetwarzania danych przez stronę ufającą, a także możliwości odrzucenia wniosków o udzielenie informacji zostały sformułowane przez grupę ekspertów eIDAS, która obecnie opracowuje zestaw narzędzi. (zob. rozdział 4.6.1 dokumentu końcowego z dnia 17 lutego 2022 r.).

Poprawka 9

Wniosek dotyczący rozporządzenia
Artykuł 1 – akapit 1 – punkt 7
Rozporządzenie (UE) nr 910/2014
Artykuł 6 a – ustęp 4 – litera b

Tekst proponowany przez Komisję	*Poprawka*
b) zapewniają, aby dostawcy usług zaufania w zakresie kwalifikowanych poświadczeń atrybutów nie mogli otrzymywać żadnych informacji o wykorzystaniu tych atrybutów;	b) zapewniają, aby dostawcy usług zaufania w zakresie kwalifikowanych ***i niekwalifikowanych*** poświadczeń atrybutów nie mogli otrzymywać żadnych informacji o wykorzystaniu tych atrybutów;

Or. en

Uzasadnienie

Niniejsza poprawka rozszerza zabezpieczenia mające na celu objęcie zachowania użytkowników ochroną przed śledzeniem. Przykładami podmiotów oferujących niekwalifikowane poświadczenia atrybutów są prywatne przedsiębiorstwa, kluby członkowskie lub uniwersytety. Dzięki tej zmianie w tekście istniejące zabezpieczenie techniczne europejskiego portfela tożsamości cyfrowej zostało po prostu rozszerzone na większą liczbę zainteresowanych stron.

Poprawka 10

Wniosek dotyczący rozporządzenia
Artykuł 1 – akapit 1 – punkt 7
Rozporządzenie (UE) nr 910/2014
Artykuł 6 a – ustęp 4 – litera e

Tekst proponowany przez Komisję	*Poprawka*

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***.***	e) zapewniają, aby dane identyfikujące osobę, o których mowa w art. 12 ust. 4 lit. d), ***w sposób unikalny*** i ***trwały reprezentujący daną*** osobę fizyczną lub prawną ***były udostępniane wyłącznie pod pseudonimem w taki sposób, aby różniły się w przypadku różnych stron ufających, tak aby zapobiec tworzeniu powiązań lub śledzeniu użytkownika między stronami ufającymi oraz aby uniemożliwić wydawcy europejskiego portfela tożsamości cyfrowej, powiązanym z nimi usługom osób trzecich lub państwu członkowskiemu uzyskanie jakichkolwiek informacji na temat korzystania z europejskiego portfela tożsamości cyfrowej;***

Or. en

Uzasadnienie

Grupa ekspertów eIDAS uznała, że konieczne jest zapobieżenie możliwości tworzenia powiązań i identyfikacji (zob. rozdział 5 s. 26 dokumentu końcowego z dnia 17 lutego 2022 r.). Transakcje użytkowników będą ujawniać duże ilości danych, w tym dane o wysoce osobistym charakterze, takie jak informacje o sytuacji ekonomicznej osób fizycznych lub informacje o sytuacji medycznej, historii podróży, wzorcach konsumpcji i interakcji społecznych obywateli.

Poprawka 11

Wniosek dotyczący rozporządzenia
Artykuł 1 – akapit 1 – punkt 7
Rozporządzenie (UE) nr 910/2014
Artykuł 6 a – ustęp 7

Tekst proponowany przez Komisję	*Poprawka*
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***	7. Użytkownik ma pełną kontrolę nad europejskim portfelem tożsamości cyfrowej ***i nad swoimi danymi***. ***Struktura techniczna uniemożliwia wydawcy*** europejskiego portfela tożsamości cyfrowej ***lub powiązanym z nim usługom osób trzecich lub państwu członkowskiemu gromadzenie lub uzyskiwanie informacji na temat korzystania z portfela przez***

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.	***użytkownika. Wymiana informacji za pośrednictwem europejskiego portfela tożsamości cyfrowej nie może prowadzić do tego, by inne strony ufające lub dostawcy elektronicznych poświadczeń atrybutów byli w stanie śledzić, łączyć**, **zestawiać transakcje lub zachowania użytkowników lub w inny sposób uzyskiwać wiedzę ta temat tych transakcji i zachowań***. 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. ***Wydawca europejskiego portfela tożsamości cyfrowej jest administratorem zgodnie z rozporządzeniem (UE) 2016/679 w odniesieniu do przetwarzania danych osobowych zawartych w europejskim portfelu tożsamości cyfrowej.***

Or. en

Uzasadnienie

Elektronicznym systemem tożsamości zasługującym na zaufanie obywateli może być jedynie struktura chroniąca takie dane, jak te dotyczące kwestii medycznych, historii podróży, wzorców konsumpcji i interakcji społecznych obywateli, a także która chroni szeroki zakres zachowań użytkowników w internecie i poza nim przed scentralizowanym nadzorem. Wydawca portfela jest administratorem danych, ponieważ ustala sposoby przetwarzania danych osobowych poprzez określenie konkretnego systemu, tj. sposobu przetwarzania, niezależnie od tego, czy system ten jest wdrażany na urządzeniu pozostającym pod jego kontrolą (zob. C-40/17 i C-25/17).

Poprawka 12

Wniosek dotyczący rozporządzenia
Artykuł 1 – akapit 1 – punkt 12
Rozporządzenie (UE) nr 910/2014
Artykuł 11 a

Tekst proponowany przez Komisję	*Poprawka*

12) dodaje się art. 11a w brzmieniu:		***skreśla się***
„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.”;		

Or. en

Uzasadnienie

Niepowtarzalny i trwały identyfikator osób fizycznych byłby w niektórych państwach członkowskich niezgodny z prawem, a nawet niezgodny z konstytucją (w Niemczech stosowanie niepowtarzalnych trwałych identyfikatorów jest zabronione na mocy orzeczenia w sprawie ustawy o spisie powszechnym z 1983 r.). Ryzyka związanego z niepowtarzalnym, przypisanym na całe życie identyfikatorem nie można uznać za najmniej inwazyjną metodę do celów jednoznacznej identyfikacji osoby fizycznej. Art. 11a również nie jest potrzebny, ponieważ istniejące ramy interoperacyjności systemów identyfikacji zgodnie z pierwotnym art. 12 ust. 4 lit. d) przewidują już jednorodne reprezentowanie osoby fizycznej w przypadku spraw transgranicznych.

Poprawka 13

Wniosek dotyczący rozporządzenia
Artykuł 1 – akapit 1 – punkt 13 – litera b

Rozporządzenie (UE) nr 910/2014
Artykuł 12 – ustęp 4 – litera d

Tekst proponowany przez Komisję	*Poprawka*
d) odniesienie do minimalnego zbioru danych identyfikujących osobę ***niezbędnych do unikalnego i trwałego reprezentowania osoby fizycznej lub prawnej***;	d) odniesienie do minimalnego zbioru danych identyfikujących osobę ***unikalnie reprezentujących osobę fizyczną lub prawną, dostępnego w ramach systemów identyfikacji elektronicznej***;

Or. en

Uzasadnienie

Wniosek Komisji wymagałby niepowtarzalnej i trwałej identyfikacji niezależnej od konkretnego systemu identyfikacji elektronicznej. W rezultacie ta pozornie techniczna zmiana ram interoperacyjności miałaby taki sam skutek jak art. 11a.

Poprawka 14

Wniosek dotyczący rozporządzenia
Artykuł 1 – akapit 1 – punkt 22 – litera b
Rozporządzenie (UE) nr 910/2014
Artykuł 20 – ustęp 2

Tekst proponowany przez Komisję	*Poprawka*
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.;	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 ***oraz administratora europejskiego portfela tożsamości cyfrowej***.;

Or. en

Uzasadnienie

Zgodnie z art. 33 i 34 RODO administrator ma pewne obowiązki w przypadku naruszenia ochrony danych. Aby móc wypełniać te obowiązki, administratorzy powinni być informowani o potencjalnym naruszeniu ochrony danych w ich systemie.

Poprawka 15

Wniosek dotyczący rozporządzenia
Artykuł 1 – akapit 1 – punkt 22 – litera b
Rozporządzenie (UE) nr 910/2014
Artykuł 20 – ustęp 2 – akapit 1 a (nowy)

Tekst proponowany przez Komisję	*Poprawka*
	Zainteresowana strona korzystająca w przedsiębiorstwie z kwalifikowanych usług zaufania, takich jak kwalifikowane elektroniczne poświadczenie atrybutów, może złożyć do organu nadzorczego skargę dotyczącą bezpieczeństwa lub wiarygodności kwalifikowanej usługi zaufania.

Or. en

Poprawka 16

Wniosek dotyczący rozporządzenia
Artykuł 1 – akapit 1 – punkt 25 – litera c – punkt 2
Rozporządzenie (UE) nr 910/2014
Artykuł 24 – ustęp 2 – litera fb a (nowa)

Tekst proponowany przez Komisję	*Poprawka*
	fba) zapewnia zgodne z prawem przetwarzanie danych osobowych zgodnie z rozporządzenie (UE) 2016/679;

Or. en

ZAŁĄCZNIK: WYKAZ PODMIOTÓW LUB OSÓB, OD KTÓRYCH SPRAWOZDAWCA OTRZYMAŁ INFORMACJE

Poniższy wykaz opracowano na zasadzie zupełnej dobrowolności, na wyłączną odpowiedzialność sprawozdawcy. Przygotowując projekt opinii, sprawozdawca komisji opiniodawczej otrzymał informacje od następujących podmiotów lub osób:

Podmiot i/lub osoba

1. European Commission DG CNECT

2. The European Data Protection Supervisor
3. Brussels Privacy Hub, *THE EUROPEAN COMMISSION PROPOSAL AMENDING THE eIDAS REGULATION (EU) No 910/2014: A PERSONAL DATA PROTECTION PERSPECTIVE*
4. Professor Ricardo Genghini, Chairman of the European Standardization Committee E-Signature and Infrastructures (ESI) within the European Telecommunications Standards Institute (ETSI) - *Notes on the current draft of eIDAS Revision Proposal*
5. epicenter.works & European Digital Rights (EDRI)
6. Luukas Ilves, Deputy Secretary General of the Estonian Ministry of Economic Affairs and Communications for Digital Development
7. European Consumer Organisation (BEUC) - *Making European Digital Identity as Safe as It Is needed - BEUC Position Paper*
8. Jaap-Henk Hoepman, Associate Professor of privacy enhancing protocols and privacy by design in the Digital Security group at the Institute for Computing and Information Sciences of the Radboud University Nijmegen, *Civil liberties aspects of the commission proposal to amend the eIDAS regulation*
9. Eric Verheul, professor in the Digital Security Group of the Radboud University Nijmegen - *Issues and recommendations on the eIDAS wallet as proposed in the eIDAS update*
10. Manuel Atug expert in IT Security and engineering Chaos Computer Club & Christian Kahlo eID expert - *written input*
11. Lukasz Olejnik, PhD, https://lukaszolejnik.com, *written contribution*
12. Carmela Troncoso - Professor on Security and Privacy at Swiss Federal Institute of Technology Lausanne - *written input*
13. Dr. F. S. Gürses, Associat Professor at the Faculty of Technology, Policy and Management, TU Delft - *written input*
14. Eurosmart - The Voice Of The Digital Security Industry - Feedback on the revision of eIDAS
15. Mozzila
16. Google
17. Apple
18. The International Association for Trusted Blockchain Applications (INATBA) - Establishing a Framework for a European Digital Identity (eIDAS) - Policy Position
19. TWG Trusted Information of the EU Observatory for ICT Standardisation - report on "Trust in the European digital space in the age of automated bots and fakes"
20. Rule of Law Defense Coalition, Bucharest Romania
21. American Chamber of Commerce to the European Union, Brussels - *written input*