Parlament Europejski
2019-2024

Komisja Wolności Obywatelskich, Sprawiedliwości i Spraw Wewnętrznych

2021/0136(COD)

11.10.2022

OPINIA

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

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) ***Osoby fizyczne lub prawne będące właścicielami danych identyfikujących osobę należy uznać za podmioty tożsamości cyfrowej.*** W ramach wdrażania niniejszego rozporządzenia do przetwarzania danych osobowych ***mają*** zastosowanie rozporządzenie (UE) 2016/679[19]***, rozporządzenie (UE) 2018/1725[19a] oraz dyrektywa 2002/58/WE[19b]***. 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. ***W niniejszym rozporządzeniu określa się również stosowanie zasad ograniczenia celu, minimalizacji danych, uwzględnienia ochrony danych w fazie projektowania i domyślnej ochrony danych w odniesieniu do konkretnych przypadków użycia, nie naruszając rozporządzenia (UE) 2016/679.***
[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	[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.	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.
	[19a] Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2018/1725 z dnia 23 października 2018 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych przez instytucje, organy i jednostki organizacyjne Unii i swobodnego przepływu takich danych oraz uchylenia rozporządzenia (WE) nr 45/2001 i decyzji nr 1247/2002/WE (Dz.U. L 295 z 21.11.2018, s. 39).
	[19b] Dyrektywa 2002/58/WE Parlamentu Europejskiego i Rady z dnia 12 lipca 2002 r. dotycząca przetwarzania danych osobowych i ochrony prywatności w sektorze łączności elektronicznej (Dz.U. L 201 z 31.7.2002, s. 37).

Poprawka 2

Wniosek dotyczący rozporządzenia
Motyw 8

Tekst proponowany przez Komisję	*Poprawka*
(8) W celu zapewnienia zgodności z prawem Unii lub prawem krajowym ***zgodnym z prawem Unii dostawcy usług powinni informować państwa członkowskie o zamiarze polegania*** na europejskich portfelach tożsamości cyfrowej. Pozwoli to państwom członkowskim chronić użytkowników przed oszustwami i zapobiegać nielegalnemu wykorzystywaniu danych dotyczących tożsamości i elektronicznych poświadczeń atrybutów, a także zapewnić, aby przetwarzanie danych wrażliwych, takich jak dane dotyczące zdrowia, mogło być weryfikowane przez strony ufające zgodnie z prawem Unii lub prawem	(8) W celu zapewnienia zgodności z prawem Unii lub prawem krajowym ***dostawcy usług powinni zarejestrować się w państwach członkowskich, zanim będą mogli polegać*** na europejskich portfelach tożsamości cyfrowej. ***Osoby fizyczne lub prawne powinny mieć możliwość złożenia skargi dotyczącej korzystania z europejskich portfeli tożsamości cyfrowej przez stronę ufającą.*** Pozwoli to państwom członkowskim chronić użytkowników przed oszustwami i zapobiegać nielegalnemu wykorzystywaniu danych dotyczących tożsamości i elektronicznych poświadczeń atrybutów, a także zapewnić, aby przetwarzanie danych wrażliwych, takich jak dane dotyczące zdrowia, mogło

krajowym.

być weryfikowane przez strony ufające zgodnie z prawem Unii lub prawem krajowym. ***Państwa członkowskie powinny zapobiegać bezprawnemu wykorzystaniu danych dotyczących tożsamości i zapewnić, aby strony ufające wymagały jedynie danych ściśle koniecznych do świadczenia określonej usługi.***

Poprawka 3

Wniosek dotyczący rozporządzenia
Motyw 9

Tekst proponowany przez Komisję	*Poprawka*
(9) Wszystkie europejskie portfele tożsamości cyfrowej powinny umożliwiać użytkownikom elektroniczną identyfikację i uwierzytelnianie online i offline w kontekście transgranicznym na potrzeby dostępu do szerokiego zakresu usług publicznych i prywatnych. Bez uszczerbku dla prerogatyw państw członkowskich w zakresie identyfikacji ich obywateli i rezydentów, portfele mogą również zaspokajać potrzeby instytucjonalne administracji publicznych, organizacji międzynarodowych oraz instytucji, organów i jednostek organizacyjnych Unii. Korzystanie z portfeli offline byłoby ważne w wielu sektorach, w tym w sektorze opieki zdrowotnej, w którym usługi są często świadczone w ramach kontaktu osobistego, a w przypadku recept elektronicznych powinna istnieć możliwość stosowania kodów QR lub podobnych technologii do weryfikacji autentyczności. W opartych na „wysokim" poziomie bezpieczeństwa europejskich portfelach tożsamości cyfrowej należy wykorzystać potencjał, jaki ***oferują rozwiązania odporne*** na ingerencję, ***takie*** jak zabezpieczenia, by zapewnić zgodność z wymogami bezpieczeństwa określonymi w niniejszym rozporządzeniu. Europejskie portfele tożsamości cyfrowej powinny	(9) Wszystkie europejskie portfele tożsamości cyfrowej powinny umożliwiać użytkownikom elektroniczną identyfikację i uwierzytelnianie online i offline w kontekście transgranicznym na potrzeby dostępu do szerokiego zakresu usług publicznych i prywatnych. Bez uszczerbku dla prerogatyw państw członkowskich w zakresie identyfikacji ich obywateli i rezydentów, portfele mogą również zaspokajać potrzeby instytucjonalne administracji publicznych, organizacji międzynarodowych oraz instytucji, organów i jednostek organizacyjnych Unii. Korzystanie z portfeli offline byłoby ważne w wielu sektorach, w tym w sektorze opieki zdrowotnej, w którym usługi są często świadczone w ramach kontaktu osobistego, a w przypadku recept elektronicznych powinna istnieć możliwość stosowania kodów QR lub podobnych technologii do weryfikacji autentyczności. ***Użytkownicy powinni mieć dostęp do prostego interfejsu, który pozwoli im na wgląd w bieżące i archiwalne zezwolenia dotyczące udostępnienia danych osobowych lub elektronicznych poświadczeń atrybutów. Powinni oni mieć możliwość wycofania swojej zgody.*** W opartych na „wysokim" poziomie bezpieczeństwa europejskich

również umożliwiać użytkownikom tworzenie i używanie kwalifikowanych podpisów i pieczęci elektronicznych akceptowanych w całej ***UE***. Aby zapewnić obywatelom i przedsiębiorstwom w całej ***UE*** korzyści w zakresie uproszczenia przepisów i zmniejszenia kosztów, w tym poprzez umożliwienie korzystania z uprawnień do reprezentowania i zgód elektronicznych, państwa członkowskie powinny wydawać europejskie portfele tożsamości cyfrowej oparte na wspólnych normach, aby zapewnić niezakłóconą interoperacyjność i wysoki poziom bezpieczeństwa. Wyłącznie właściwe organy państw członkowskich mogą zapewnić wysoki stopień pewności przy ustalaniu tożsamości danej osoby, gwarantując tym samym, że osoba podająca daną tożsamość jest faktycznie osobą, za którą się podaje. Europejskie portfele tożsamości cyfrowej muszą być zatem oparte się na tożsamości prawnej obywateli, innych rezydentów lub osób prawnych. Zaufanie do europejskich portfeli tożsamości cyfrowej ulegnie zwiększeniu ze względu na fakt, że podmioty je wydające są zobowiązane do wdrożenia odpowiednich środków technicznych i organizacyjnych w celu zapewnienia poziomu bezpieczeństwa współmiernego do stwarzanego ryzyka dla praw i wolności osób fizycznych zgodnie z rozporządzeniem (UE) 2016/679.

portfelach tożsamości cyfrowej należy wykorzystać potencjał, jaki ***oferuje technologia odporna*** na ingerencję, ***taka*** jak zabezpieczenia, by zapewnić zgodność z wymogami bezpieczeństwa ***i integralności*** określonymi w niniejszym rozporządzeniu. Europejskie portfele tożsamości cyfrowej powinny również umożliwiać użytkownikom tworzenie i używanie kwalifikowanych podpisów i pieczęci elektronicznych akceptowanych w całej ***Unii***. Aby zapewnić obywatelom i przedsiębiorstwom w całej ***Unii*** korzyści w zakresie uproszczenia przepisów i zmniejszenia kosztów, w tym poprzez umożliwienie korzystania z uprawnień do reprezentowania i zgód elektronicznych, państwa członkowskie powinny wydawać europejskie portfele tożsamości cyfrowej oparte na wspólnych normach, aby zapewnić niezakłóconą interoperacyjność i wysoki poziom bezpieczeństwa. Wyłącznie właściwe organy państw członkowskich mogą zapewnić wysoki stopień pewności przy ustalaniu tożsamości danej osoby, gwarantując tym samym, że osoba podająca daną tożsamość jest faktycznie osobą, za którą się podaje. ***W odniesieniu do pewnych przypadków użycia*** europejskie portfele tożsamości cyfrowej muszą być zatem oparte się na tożsamości prawnej obywateli, innych rezydentów lub osób prawnych. Zaufanie do europejskich portfeli tożsamości cyfrowej ulegnie zwiększeniu ze względu na fakt, że podmioty je wydające są zobowiązane do wdrożenia odpowiednich środków technicznych i organizacyjnych w celu zapewnienia poziomu bezpieczeństwa współmiernego do stwarzanego ryzyka dla praw i wolności osób fizycznych zgodnie z rozporządzeniem (UE) 2016/679.

Poprawka 4

Wniosek dotyczący rozporządzenia
Motyw 9 a (nowy)

Tekst proponowany przez Komisję	*Poprawka*
	(9a) W celu zapewnienia pomyślnego upowszechnienia europejskiego portfela tożsamości cyfrowej kluczowe znaczenie ma zapewnienie zaufania do leżących u jego podstaw ram technicznych oraz do otaczającego go ekosystemu cyfrowego. Wysoki stopień przejrzystości może przyczynić się do budowania zaufania, umożliwiając użytkownikom podejmowanie świadomych decyzji dotyczących właściwości europejskiego portfela tożsamości cyfrowej dotyczących bezpieczeństwa i prywatności, a także umożliwiając publiczną kontrolę działań związanych z tymi ramami i zaangażowanych w nie podmiotów. Z tego powodu państwa członkowskie powinny zapewnić, aby odpowiednie informacje, takie jak ustawienia ochrony prywatności, architektura techniczna, ramy bezpieczeństwa oraz informacje o miejscu przetwarzania danych osobowych, były zawarte w zestawie minimalnych informacji o europejskim portfelu tożsamości cyfrowej i były dostępne publicznie.

Poprawka 5

Wniosek dotyczący rozporządzenia
Motyw 9 b (nowy)

Tekst proponowany przez Komisję	*Poprawka*
	(9b) Jednym z celów europejskiego portfela tożsamości cyfrowej powinno być zwiększenie możliwości obywateli w zakresie podejmowania decyzji o tym, jakie dane udostępniają, aby minimalizować ilość danych udostępnianych na potrzeby usług, z których obywatele chcą skorzystać, a także, by lepiej zarządzać udostępnianymi

danymi i je kontrolować.

Poprawka 6

Wniosek dotyczący rozporządzenia
Motyw 10

Tekst proponowany przez Komisję	*Poprawka*
(10) W celu osiągnięcia wysokiego poziomu bezpieczeństwa i wiarygodności w niniejszym rozporządzeniu ustanowiono wymogi dotyczące europejskich portfeli tożsamości cyfrowej. Zgodność europejskich portfeli tożsamości cyfrowej z tymi wymogami powinna być certyfikowana przez akredytowane podmioty sektora publicznego lub prywatnego wyznaczone przez państwa członkowskie. Poleganie na systemie certyfikacji opartym na ***dostępności norm*** wspólnie uzgodnionych z państwami członkowskimi powinno zapewnić wysoki poziom zaufania i ***interoperacyjności***. Certyfikacja powinna w szczególności opierać się na odpowiednich europejskich programach certyfikacji cyberbezpieczeństwa ustanowionych na podstawie rozporządzenia (UE) 2019/881[20]. Certyfikacja taka powinna pozostawać bez uszczerbku dla certyfikacji w odniesieniu do przetwarzania danych osobowych na podstawie rozporządzenia (UE) 2016/679.	(10) W celu osiągnięcia wysokiego poziomu bezpieczeństwa i wiarygodności w niniejszym rozporządzeniu ustanowiono wymogi dotyczące europejskich portfeli tożsamości cyfrowej. Zgodność europejskich portfeli tożsamości cyfrowej z tymi wymogami powinna być certyfikowana przez akredytowane podmioty sektora publicznego lub prywatnego wyznaczone przez państwa członkowskie. Poleganie na systemie certyfikacji opartym na ***najnowocześniejszej technologii i normach*** wspólnie uzgodnionych z państwami członkowskimi powinno zapewnić wysoki poziom zaufania**,** ***interoperacyjności*** i ***ochrony danych***. Certyfikacja powinna w szczególności opierać się na odpowiednich europejskich programach certyfikacji cyberbezpieczeństwa ustanowionych na podstawie rozporządzenia (UE) 2019/881[20]. Certyfikacja taka powinna pozostawać bez uszczerbku dla certyfikacji w odniesieniu do przetwarzania danych osobowych na podstawie rozporządzenia (UE) 2016/679.
[20] Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2019/881 z dnia 17 kwietnia 2019 r. w sprawie ENISA (Agencji Unii Europejskiej ds. Cyberbezpieczeństwa) oraz certyfikacji cyberbezpieczeństwa w zakresie technologii informacyjno-komunikacyjnych oraz uchylenia rozporządzenia (UE) nr 526/2013 (akt o cyberbezpieczeństwie), Dz.U. L 151	[20] Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2019/881 z dnia 17 kwietnia 2019 r. w sprawie ENISA (Agencji Unii Europejskiej ds. Cyberbezpieczeństwa) oraz certyfikacji cyberbezpieczeństwa w zakresie technologii informacyjno-komunikacyjnych oraz uchylenia rozporządzenia (UE) nr 526/2013 (akt o cyberbezpieczeństwie), Dz.U. L 151

z 7.6.2019, s. 15.

z 7.6.2019, s. 15.

Poprawka 7

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, przy użyciu rozwiązań opartych na chmurze ***czy w sposób łączący te dwie możliwości***, 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***. Ponieważ dane biometryczne dotyczą unikalnych cech danej osoby, korzystanie z danych ***biometrycznych ogranicza się do konkretnych scenariuszy na podstawie rozporządzenia (UE) 2016/679*** i ***wymaga technicznych i organizacyjnych*** środków bezpieczeństwa współmiernych do ryzyka, jakie takie przetwarzanie może stwarzać dla praw i wolności osób fizycznych, oraz musi być zgodne z ***tym*** rozporządzeniem***. Zdolność przechowywania w chmurze informacji pochodzących z europejskiego portfela tożsamości cyfrowej powinna być funkcją aktywowaną tylko po wyrażeniu wyraźnej zgody przez użytkownika. Państwa członkowskie powinny umożliwiać przechowywanie przez europejski portfel tożsamości cyfrowej materiału kryptograficznego i obsługiwanie transakcji na urządzeniu użytkownika bez konieczności korzystania z usług w chmurze, chyba że użytkownik wyraźnie wydał zgodę na takie***

	przechowywanie. Jeżeli europejski portfel tożsamości cyfrowej zapewnia się na urządzeniu użytkownika, jego materiał kryptograficzny należy przechowywać w bezpiecznych elementach urządzenia.

Poprawka 8

Wniosek dotyczący rozporządzenia
Motyw 12

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

Poprawka 9

Wniosek dotyczący rozporządzenia
Motyw 17

Tekst proponowany przez Komisję	*Poprawka*
(17) Dostawcy usług wykorzystują dane	(17) Dostawcy usług wykorzystują dane

dotyczące tożsamości dostarczone przez zbiór danych identyfikujących osobę dostępnych w ramach systemów identyfikacji elektronicznej na podstawie rozporządzenia (UE) nr 910/2014, aby dopasować użytkownika z innego państwa członkowskiego do tożsamości prawnej danego użytkownika. Pomimo korzystania ze zbioru danych eIDAS w wielu przypadkach zapewnienie dokładnego dopasowania wymaga jednak dodatkowych informacji na temat użytkownika oraz określonych procedur unikalnej identyfikacji na szczeblu krajowym. W celu dalszego wspomagania używalności środków identyfikacji elektronicznej w niniejszym rozporządzeniu należy zobowiązać państwa członkowskie do wprowadzenia konkretnych środków służących zapewnieniu prawidłowego dopasowania tożsamości w procesie identyfikacji elektronicznej. W tym ***samym celu w niniejszym rozporządzeniu należy również rozszerzyć obowiązkowy minimalny zbiór danych i wprowadzić wymóg stosowania unikalnego i trwałego identyfikatora elektronicznego zgodnego z prawem Unii w przypadkach***, w ***których konieczna jest zgodna z*** prawem ***unikalna*** i ***trwała identyfikacja użytkownika*** na ***jego żądanie***.	dotyczące tożsamości dostarczone przez zbiór danych identyfikujących osobę dostępnych w ramach systemów identyfikacji elektronicznej na podstawie rozporządzenia (UE) nr 910/2014, aby dopasować użytkownika z innego państwa członkowskiego do tożsamości prawnej danego użytkownika. Pomimo korzystania ze zbioru danych eIDAS w wielu przypadkach zapewnienie dokładnego dopasowania wymaga jednak dodatkowych informacji na temat użytkownika oraz określonych procedur unikalnej identyfikacji na szczeblu krajowym. W celu dalszego wspomagania używalności środków identyfikacji elektronicznej w niniejszym rozporządzeniu należy zobowiązać państwa członkowskie do wprowadzenia konkretnych środków służących zapewnieniu prawidłowego dopasowania tożsamości w procesie identyfikacji elektronicznej. ***Wykorzystanie danych identyfikujących osobę lub kombinacji danych identyfikujących osobę,*** w tym ***stosowanie unikalnych i trwałych identyfikatorów wydawanych przez państwa członkowskie lub generowanych przez europejski portfel tożsamości cyfrowej, ma zasadnicze znaczenie dla zapewnienia możliwości weryfikacji tożsamości użytkownika***, w ***szczególności w sektorze publicznym oraz w przypadku gdy wymaga tego prawo Unii lub prawo krajowe. Należy przewidzieć możliwość wymagania*** prawem ***państwa członkowskiego stosowania unikalnych i trwałych identyfikatorów specyficznych dla danego sektora lub strony ufającej. Europejski portfel tożsamości cyfrowej powinien umożliwiać przechowywanie tych identyfikatorów i ujawnianie ich na żądanie użytkownika.***

Poprawka 10

Wniosek dotyczący rozporządzenia
Motyw 25

Tekst proponowany przez Komisję	*Poprawka*
(25) ***W*** większości przypadków obywatele i inni rezydenci nie mogą prowadzić transgranicznej cyfrowej wymiany informacji związanych z tożsamością, takich jak: adresy, wiek i kwalifikacje zawodowe, prawa jazdy i inne zezwolenia oraz dane dotyczące płatności, w sposób bezpieczny i z zapewnieniem wysokiego stopnia ochrony danych.	(25) ***Na rynku wewnętrznym obywatele muszą mieć możliwość wymiany między granicami państw informacji dotyczących ich tożsamości. Jednak w*** większości przypadków obywatele i inni rezydenci nie mogą prowadzić transgranicznej cyfrowej wymiany ***oficjalnie poświadczonych*** informacji związanych z tożsamością, takich jak: adresy, wiek i kwalifikacje zawodowe, prawa jazdy i inne zezwolenia oraz dane dotyczące płatności, w sposób bezpieczny i z zapewnieniem wysokiego stopnia ochrony danych. ***Mogłoby to skutkować mniej bezpiecznym i mniej zorganizowanym przekazywaniem tych danych.***

Poprawka 11

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 ***w sposób bezpieczny i przyjazny użytkownikom, przy czym ta możliwość jest jedną z jego najważniejszych funkcji i zalet***. ***Należy również dopilnować, aby żadne atrybuty nie były ujawniane stronom, które nie są uprawnione poprzez rejestrację do uzyskiwania dostępu do takich atrybutów.*** Funkcja ta powinna stać się podstawową cechą projektową, co zwiększy wygodę i ochronę danych osobowych, w tym jeżeli chodzi o minimalizację przetwarzania danych osobowych***, a w szczególności o uwzględnienie ochrony prywatności już w fazie projektowania i o domyślną***

	ochronę prywatności. Mechanizmy walidacji europejskiego portfela tożsamości cyfrowej, selektywne ujawnianie i uwierzytelnianie użytkowników przed udostępnieniem im usług internetowych powinny służyć ochronie prywatności, a więc zapobiegają śledzeniu użytkownika, a także są zgodne z zasadą ograniczenia celu, co oznacza w konsekwencji prawo do posługiwania się pseudonimem, aby nie można było ustalić przyporządkowania użytkownika między różnymi stronami ufającymi. Architektura techniczna i wdrażanie europejskiego portfela tożsamości cyfrowej powinny być w pełni zgodne z rozporządzeniem (UE) 2016/679. Ponadto zdecentralizowany charakter portfela powinien umożliwić samodzielne podpisywanie i odwoływalność atrybutów i identyfikatorów.

Poprawka 12

Wniosek dotyczący rozporządzenia
Motyw 29 a (nowy)

Tekst proponowany przez Komisję	*Poprawka*
	(29a) O ile przepisy szczególne prawa Unii lub prawa krajowego nie wymagają od użytkowników identyfikacji – korzystanie z usług pod pseudonimem powinno być dozwolone i nie powinno być ograniczane przez państwa członkowskie, na przykład poprzez nałożenie na dostawców usług ogólnego obowiązku ograniczenia korzystania z ich usług pod pseudonimem.

Poprawka 13

Wniosek dotyczący rozporządzenia
Motyw 35

Tekst proponowany przez Komisję	*Poprawka*
(35) Certyfikacja w charakterze kwalifikowanych dostawców usług zaufania powinna zapewniać pewność prawa w odniesieniu do przypadków użycia, które opierają się na rejestrach elektronicznych. Ta usługa zaufania do celów rejestrów elektronicznych i kwalifikowanych rejestrów elektronicznych oraz certyfikacja w charakterze kwalifikowanego dostawcy usług zaufania w odniesieniu do rejestrów elektronicznych powinny obowiązywać niezależnie od wymogu, by przypadki użycia były zgodne z prawem Unii lub prawem krajowym zgodnym z prawem Unii. Przypadki użycia związane z przetwarzaniem danych osobowych muszą być zgodne z rozporządzeniem (UE) 2016/679. Przypadki użycia związane z kryptoaktywami powinny być zgodne ze wszystkimi mającymi zastosowanie przepisami finansowymi, np. z dyrektywą w sprawie rynków instrumentów finansowych[23], dyrektywą w sprawie usług płatniczych[24] ***i*** przyszłym rozporządzeniem w sprawie rynków kryptoaktywów[25].	(35) Certyfikacja w charakterze kwalifikowanych dostawców usług zaufania powinna zapewniać pewność prawa w odniesieniu do przypadków użycia, które opierają się na rejestrach elektronicznych. Ta usługa zaufania do celów rejestrów elektronicznych i kwalifikowanych rejestrów elektronicznych oraz certyfikacja w charakterze kwalifikowanego dostawcy usług zaufania w odniesieniu do rejestrów elektronicznych powinny obowiązywać niezależnie od wymogu, by przypadki użycia były zgodne z prawem Unii lub prawem krajowym zgodnym z prawem Unii. Przypadki użycia związane z przetwarzaniem danych osobowych muszą być zgodne z rozporządzeniem (UE) 2016/679. Przypadki użycia związane z kryptoaktywami powinny być zgodne ze wszystkimi mającymi zastosowanie przepisami finansowymi, np. z dyrektywą w sprawie rynków instrumentów finansowych[23], dyrektywą w sprawie usług płatniczych[24]***,*** przyszłym rozporządzeniem w sprawie rynków kryptoaktywów[25] ***i rozporządzeniu w sprawie transferu środków pieniężnych[25a]***.
[23] Dyrektywa Parlamentu Europejskiego i Rady 2014/65/UE z dnia 15 maja 2014 r. w sprawie rynków instrumentów finansowych oraz zmieniająca dyrektywę 2002/92/WE i dyrektywę 2011/61/UE (Tekst mający znaczenie dla EOG), Dz.U. L 173 z 12.6.2014, s. 349.	[23] Dyrektywa Parlamentu Europejskiego i Rady 2014/65/UE z dnia 15 maja 2014 r. w sprawie rynków instrumentów finansowych oraz zmieniająca dyrektywę 2002/92/WE i dyrektywę 2011/61/UE (Tekst mający znaczenie dla EOG), Dz.U. L 173 z 12.6.2014, s. 349.
[24] Dyrektywa Parlamentu Europejskiego i Rady (UE) 2015/2366 z dnia 25 listopada 2015 r. w sprawie usług płatniczych w ramach rynku wewnętrznego, zmieniająca dyrektywy 2002/65/WE, 2009/110/WE, 2013/36/UE i rozporządzenie (UE) nr 1093/2010 oraz uchylająca dyrektywę 2007/64/WE, Dz.U. L 337 z 23.12.2015, s. 35.	[24] Dyrektywa Parlamentu Europejskiego i Rady (UE) 2015/2366 z dnia 25 listopada 2015 r. w sprawie usług płatniczych w ramach rynku wewnętrznego, zmieniająca dyrektywy 2002/65/WE, 2009/110/WE, 2013/36/UE i rozporządzenie (UE) nr 1093/2010 oraz uchylająca dyrektywę 2007/64/WE, Dz.U. L 337 z 23.12.2015, s. 35.

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

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

[25a] Wniosek dotyczący rozporządzenia Parlamentu Europejskiego i Rady w sprawie informacji towarzyszących transferom środków pieniężnych i niektórych kryptoaktywów (wersja przekształcona), 2021/0241(COD).

Poprawka 14

Wniosek dotyczący rozporządzenia
Artykuł 1 – akapit 1 – punkt 3 – litera i
Rozporządzenie (UE) nr 910/2014
Artykuł 3 – akapit 1 – punkt 42

Tekst proponowany przez Komisję	*Poprawka*
42) »europejski portfel tożsamości cyfrowej« jest ***produktem i usługą***, ***które umożliwiają*** użytkownikowi przechowywanie danych dotyczących tożsamości, danych uwierzytelniających i atrybutów powiązanych z ***jego tożsamością***, dostarczanie ich na żądanie stronom ufającym oraz wykorzystywanie ich do uwierzytelniania online i offline na potrzeby usługi zgodnie z art. 6a, jak również składanie kwalifikowanych podpisów i pieczęci elektronicznych;	42) »europejski portfel tożsamości cyfrowej« jest ***środkiem identyfikacji elektronicznej***, ***który umożliwia*** użytkownikowi przechowywanie ***na urządzeniu będącym pod jego kontrolą*** danych dotyczących tożsamości, ***wyraźnych potwierdzeń zgód na udostępnianie danych osobowych,*** danych uwierzytelniających i atrybutów powiązanych z ***tożsamością użytkownika oraz zarządzanie wymienionymi***, dostarczanie ich na żądanie ***w sposób selektywny należycie zarejestrowanym*** stronom ufającym oraz wykorzystywanie ich do uwierzytelniania online i offline na potrzeby usługi zgodnie z art. 6a, jak również składanie kwalifikowanych podpisów i pieczęci elektronicznych;

Poprawka 15

Wniosek dotyczący rozporządzenia
Artykuł 1 – akapit 1 – punkt 3 – litera i
Rozporządzenie (UE) nr 910/2014
Artykuł 3 – akapit 1 – punkt 43

Tekst proponowany przez Komisję	*Poprawka*
43) »atrybut« ***jest cechą***, ***właściwością*** lub ***przymiotem*** osoby fizycznej lub prawnej lub podmiotu, ***wyrażonymi*** w postaci elektronicznej;	43) »atrybut« ***oznacza elektroniczną reprezentację cechy***, ***właściwości*** lub ***przymiotu*** osoby fizycznej lub prawnej lub podmiotu, ***wyrażoną*** w postaci elektronicznej;

Poprawka 16

Wniosek dotyczący rozporządzenia
Artykuł 1 – akapit 1 – punkt 3 – litera i
Rozporządzenie (UE) nr 910/2014
Artykuł 3 – akapit 1 – punkt 55

Tekst proponowany przez Komisję	*Poprawka*
55) ***»unikalna identyfikacja«*** oznacza proces, w którym dane identyfikujące osobę lub środki identyfikacji osoby są dopasowywane do istniejącego konta należącego do tej samej osoby lub z nim wiązane.”;	55) ***»dopasowywanie tożsamości«*** oznacza proces, w którym dane identyfikujące osobę lub środki identyfikacji osoby są dopasowywane do istniejącego konta należącego do tej samej osoby lub z nim wiązane.”;

Poprawka 17

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

Tekst proponowany przez Komisję	*Poprawka*
Pseudonimy w ***transakcji elektronicznej***	***Ochrona danych osobowych oraz*** pseudonimy w ***transakcjach elektronicznych.***

Poprawka 18

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.***;***	***1. Przetwarzanie danych osobowych odbywa się zgodnie z rozporządzeniami (UE) 2016/679 i (UE) 2018/1725 oraz, w stosownych przypadkach, z dyrektywą 2002/58/WE, poprzez wdrożenie zasad minimalizacji danych, ograniczenia celu oraz uwzględniania ochrony danych już w fazie projektowania i domyślnej ochrony danych, w szczególności w odniesieniu do środków technicznych służących wdrożeniu niniejszego rozporządzenia i ram interoperacyjności zgodnie z jego art. 12.*** ***2.*** Bez uszczerbku dla skutku prawnego, jaki prawo krajowe przyznaje pseudonimom***, zezwala się na używanie*** pseudonimów w transakcjach elektronicznych. ***Używanie pseudonimów swobodnie wybranych przez użytkownika jest zawsze jedną z opcji zastępujących unikalny identyfikator, gdy identyfikacja użytkownika nie jest wymagana prawem Unii lub prawem krajowym.*** ***3. Strony ufające podejmują racjonalne działania, aby umożliwić korzystanie z ich usług bez elektronicznej identyfikacji lub elektronicznego uwierzytelniania.***

Poprawka 19

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

Tekst proponowany przez Komisję	*Poprawka*
	ba) podejmowanie świadomych decyzji na temat udostępniania danych osobowych stronom ufającym. Obejmuje to identyfikację strony ufającej, możliwość zupełnej lub częściowej odmowy przekazania informacji stronom ufającym

oraz pełną historię transakcji.

Poprawka 20

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

Tekst proponowany przez Komisję	*Poprawka*
2) dla stron ufających w celu wnioskowania o dane identyfikujące osobę i elektroniczne poświadczenia atrybutów oraz ich walidację;	2) dla stron ufających w celu wnioskowania o dane identyfikujące osobę i elektroniczne poświadczenia atrybutów oraz ich walidację ***zgodnie z rozporządzeniem (UE) 2016/679***;

Poprawka 21

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) aby strony ufające były należycie zarejestrowane w publicznie dostępnym wykazie i aby ich wnioski o udzielenie informacji były widoczne w tym publicznie dostępnym wykazie;

Poprawka 22

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	3) w celu ***przedstawienia*** stronom ufającym***, zgodnie z rozporządzeniem (UE) 2016/679,*** danych identyfikujących osobę, ***takich jak dane uwierzytelniające, elektroniczne poświadczenie atrybutów***

niewymagającym dostępu internetowego ***do portfela***;	***lub inne*** dane, w trybie lokalnym niewymagającym dostępu ***do*** internetowego ***portfela, a także w celu umożliwienia użytkownikowi podjęcia świadomej decyzji o udostępnieniu danych osobowych stronom ufającym, przy jednoczesnym zapewnieniu możliwości selektywnego ujawnienia, przy czym obejmuje to całkowitą lub częściową odmowę przekazania informacji stronom ufającym, pełną historię transakcji, możliwość wycofania uprzednio wyrażonej zgody na wniosek o informacje oraz informacje o wykonywaniu praw w charakterze osoby, której dane dotyczą***;

Poprawka 23

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 ***kwalifikowanych i niekwalifikowanych elektronicznych*** poświadczeń atrybutów ***byli technologicznie pozbawieni możliwości otrzymywania jakichkolwiek*** informacji o wykorzystaniu tych atrybutów;

Poprawka 24

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

fizyczną lub prawną**.**	fizyczną lub prawną ***oraz by odniesienia do tych danych były różne dla różnych stron ufających, jeśli wymaga tego prawo;***

Poprawka 25

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

Tekst proponowany przez Komisję	*Poprawka*
	ea) umożliwiają użytkownikowi dostęp do mającego format nadający się do odczytu wykazu działań, transakcji lub przypadków użycia elektronicznych poświadczeń atrybutów lub danych identyfikujących osobę, które zostały zatwierdzone przez użytkownika;

Poprawka 26

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

Tekst proponowany przez Komisję	*Poprawka*
	eb) umożliwiają użytkownikowi przekazywanie danych europejskiego portfela tożsamości cyfrowej oraz blokowanie dostępu do niego w przypadku naruszenia bezpieczeństwa, z możliwością zawieszenia, unieważnienia lub wycofania danych.

Poprawka 27

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

Tekst proponowany przez Komisję	*Poprawka*
	4a. W przypadku, gdy istnieje łańcuch stron ufających, pośrednicy nie uzyskują wiedzy o przedmiocie transakcji.

Poprawka 28

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 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.***	7. ***Ramy techniczne europejskiego portfela tożsamości cyfrowej podlegają następującym zasadom:***
	a) Użytkownik ma pełną kontrolę nad europejskim portfelem tożsamości cyfrowej i swoimi danymi, łącznie z

autocertyfikacją.

b) Europejski portfel tożsamości cyfrowej wykorzystuje elementy zdecentralizowane na potrzeby architektury tożsamości.

c) Zestaw środków identyfikacji elektronicznej, atrybutów i certyfikatów zawartych w europejskim portfelu tożsamości cyfrowej jest przechowywany w sposób bezpieczny i wyłącznie na urządzeniach kontrolowanych przez użytkownika, chyba że użytkownik dobrowolnie wyrazi zgodę na przechowywanie ich na urządzeniach osób trzecich lub na przechowywanie w chmurze.

d) Europejski portfel tożsamości cyfrowej zapewnia możliwe do zweryfikowania dane uwierzytelniające.

e) Europejski portfel tożsamości cyfrowej umożliwia bezpieczne połączenia między użytkownikiem a stronami ufającymi.

f) Architektura techniczna europejskiego portfela tożsamości cyfrowej uniemożliwia wydawcy europejskiego portfela tożsamości cyfrowej, państwu członkowskiemu lub innym stronom gromadzenie lub uzyskiwanie środków identyfikacji elektronicznej, atrybutów, dokumentów elektronicznych zawartych w europejskim portfelu tożsamości cyfrowej oraz informacji o korzystaniu z portfela przez użytkownika, z wyjątkiem sytuacji, gdy zażąda tego użytkownik korzystający z urządzenia będącego pod jego kontrolą. Wymiana informacji za pośrednictwem europejskiego portfela tożsamości cyfrowej nie pozwala dostawcom elektronicznych poświadczeń atrybutów na śledzenie, powiązanie, ustalenie korelacji ani uzyskiwanie w inny sposób wiedzy o transakcjach lub zachowaniu użytkownika.

g) Unikalne i trwałe identyfikatory

nie są dostępne dla stron ufających w przypadkach innych niż te, w których identyfikacja użytkownika jest wymagana prawem Unii lub prawem krajowym.

h) Państwa członkowskie dopilnowują, by odpowiednie informacje na temat europejskiego portfela tożsamości cyfrowej były publicznie dostępne.

i) Dane osobowe związane z udostępnianiem europejskich portfeli tożsamości cyfrowej muszą być fizycznie i logicznie oddzielone od wszelkich innych przechowywanych danych.

j) 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.

k) Jeżeli poświadczenie atrybutów nie wymaga identyfikacji użytkownika, wykonuje się poświadczenia z wiedzą zerową.

l) Administratorem danych do celów rozporządzenia (UE) 2016/679 w odniesieniu do przetwarzania danych osobowych w europejskim portfelu tożsamości cyfrowej jest wydawca europejskiego portfela tożsamości cyfrowej.

m) Europejski portfel tożsamości cyfrowej zapewnia mechanizm składania skarg, aby umożliwić użytkownikom bezpośrednie informowanie organu nadzorczego na mocy niniejszego rozporządzenia oraz organów nadzorczych ustanowionych na mocy rozporządzenia (UE) 2016/679 w przypadku gdy strona ufająca zażąda nieproporcjonalnej ilości danych, niezgodnie z zarejestrowanym zamierzonym wykorzystaniem tych danych.

Poprawka 29

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

Tekst proponowany przez Komisję	*Poprawka*
	7a. Dostęp osób fizycznych do usług publicznych i prywatnych, do platform internetowych w rozumieniu rozporządzenia (UE) XXX/XXX [akt o usługach cyfrowych] lub do rynku pracy nie jest uzależniony od korzystania z europejskiego portfela tożsamości cyfrowej.
	Korzystanie z europejskich portfeli tożsamości cyfrowej jest opcjonalne, bezpłatne i w żadnym razie nie może stanowić podstawy dla żadnego rodzaju dyskryminacji.
	Osoby fizyczne nie są dyskryminowane w związku z niekorzystaniem z europejskiego portfela tożsamości cyfrowej.

Poprawka 30

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

Tekst proponowany przez Komisję	*Poprawka*
Unikalna identyfikacja	***Dopasowywanie tożsamości***

Poprawka 31

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

Tekst proponowany przez Komisję	*Poprawka*
1. W przypadku gdy notyfikowane	1. W przypadku gdy notyfikowane

środki identyfikacji elektronicznej i europejskie portfele tożsamości cyfrowej są używane do celów ***uwierzytelniania***, państwa członkowskie zapewniają ***unikalną identyfikację***.	środki identyfikacji elektronicznej i europejskie portfele tożsamości cyfrowej są używane do celów ***identyfikacji elektronicznej***, państwa członkowskie zapewniają ***dopasowywanie tożsamości***.

Poprawka 32

Wniosek dotyczący rozporządzenia
Artykuł 1 – akapit 1 – punkt 12
Rozporządzenie (UE) nr 910/2014
Artykuł 11 a – ustęp 2

Tekst proponowany przez Komisję	*Poprawka*
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***.	2. ***Aby zidentyfikować użytkownika na jego wniosek w przypadkach, w których identyfikacja użytkownika jest wymagana przepisami prawa, unikalne i trwałe identyfikatory wydane przez*** państwa członkowskie ***lub wygenerowane przez europejskie portfele tożsamości cyfrowej przekazuje się wraz z minimalnym zestawem*** danych identyfikujących osobę, o którym mowa w art. 12 ust. 4 lit. d)***. Państwa członkowskie mogą wymagać, aby unikalne i trwałe identyfikatory były specyficzne dla sektora lub strony ufającej, o ile jednoznacznie identyfikują użytkownika w całej Unii.***

Poprawka 33

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 zbioru danych identyfikujących osobę niezbędnych do unikalnego reprezentowania osoby fizycznej lub prawnej***, dostępnego w ramach systemów identyfikacji elektronicznej***;

Poprawka 34

Wniosek dotyczący rozporządzenia
Artykuł 1 – akapit 1 – punkt 20 – litera a – punkt 2
Rozporządzenie (UE) nr 910/2014
Artykuł 17 – ustęp 4 – litera f

Tekst proponowany przez Komisję	*Poprawka*
f) współpracę z organami nadzorczymi ustanowionymi na mocy rozporządzenia (UE) 2016/679, w szczególności przez informowanie ich, bez zbędnej zwłoki, o wynikach audytów kwalifikowanych dostawców usług zaufania, w przypadku gdy doszło do naruszenia przepisów dotyczących ochrony danych osobowych, a także o naruszeniach bezpieczeństwa stanowiących naruszenie ochrony danych osobowych***;;***	f) współpracę z organami nadzorczymi ustanowionymi na mocy rozporządzenia (UE) 2016/679, w szczególności przez informowanie ich, bez zbędnej zwłoki, o wynikach audytów kwalifikowanych dostawców usług zaufania, w przypadku gdy ***istnieją dowody, że*** doszło do naruszenia przepisów dotyczących ochrony danych osobowych, a także o naruszeniach bezpieczeństwa stanowiących ***prawdopodobnie*** naruszenie ochrony danych osobowych ***lub o podejrzeniach takich naruszeń, o których powezmą wiedzę w toku realizacji swoich zadań, nie naruszając rozporządzenia (UE) 2016/679.***

Poprawka 35

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***.***;	***Nie naruszając dalszych obowiązków spoczywających na administratorach danych lub przetwarzających, które to obowiązki wynikają z rozporządzenia (UE) 2016/679, w*** przypadku gdy ***istnieje jakakolwiek podstawa, by sądzić***, że ***mogły zostać*** naruszone przepisy dotyczące ochrony danych, organ nadzoru informuje o ***tym bezzwłocznie*** organy nadzorcze na podstawie rozporządzenia (UE) 2016/679***, a także wydawcę i administratora***

europejskiego portfela tożsamości cyfrowej oraz przekazuje im wyniki swoich audytów, jak tylko będą one dostępne;

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

Poniższy wykaz opracowano na zasadzie zupełnej dobrowolności, na wyłączną odpowiedzialność sprawozdawcy. Podczas sporządzania opinii, do czasu przyjęcia jej w komisji, 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*

PROCEDURA W KOMISJI OPINIODAWCZEJ

Tytuł	Zmiana rozporządzenia (UE) nr 910/2014 w odniesieniu do utworzenia europejskich ram tożsamości cyfrowej
Odsyłacze	COM(2021)0281 – C9-0200/2021 – 2021/0136(COD)
Komisja przedmiotowo właściwa Data ogłoszenia na posiedzeniu	ITRE 8.7.2021
Opinia wydana przez Data ogłoszenia na posiedzeniu	LIBE 8.7.2021
Zaangażowane komisje - Data ogłoszenia na posiedzeniu	16.12.2021
Sprawozdawca(-czyni) (komisji opiniodawczej) Data powołania	Cristian Terheş 29.11.2021
Rozpatrzenie w komisji	12.1.2022 30.5.2022
Data przyjęcia	10.10.2022
Wynik głosowania końcowego	+: 51 –: 1 0: 4
Posłowie obecni podczas głosowania końcowego	Abir Al-Sahlani, Konstantinos Arvanitis, Malik Azmani, Pietro Bartolo, Malin Björk, Patrick Breyer, Saskia Bricmont, Patricia Chagnon, Clare Daly, Andrzej Halicki, Evin Incir, Sophia in ‘t Veld, Assita Kanko, Alice Kuhnke, Jeroen Lenaers, Lukas Mandl, Nuno Melo, Nadine Morano, Javier Moreno Sánchez, Maite Pagazaurtundúa, Emil Radev, Paulo Rangel, Terry Reintke, Karlo Ressler, Diana Riba i Giner, Isabel Santos, Birgit Sippel, Sara Skyttedal, Vincenzo Sofo, Ramona Strugariu, Tomas Tobé, Yana Toom, Milan Uhrík, Elissavet Vozemberg-Vrionidi, Elena Yoncheva, Javier Zarzalejos
Zastępcy obecni podczas głosowania końcowego	Romeo Franz, Erik Marquardt, Fulvio Martusciello, Peter Pollák, Paul Tang, Róża Thun und Hohenstein, Miguel Urbán Crespo
Zastępcy (art. 209 ust. 7) obecni podczas głosowania końcowego	Marek Paweł Balt, Gilles Boyer, Jonás Fernández, Hannes Heide, Othmar Karas, Georgios Kyrtsos, Karsten Lucke, Evelyn Regner, Antonio Maria Rinaldi, Simone Schmiedtbauer, Ralf Seekatz, Michal Šimečka, Ivan Štefanec

GŁOSOWANIE KOŃCOWE W FORMIE GŁOSOWANIA IMIENNEGO W KOMISJI OPINIODAWCZEJ

51	+
PPE	Andrzej Halicki, Othmar Karas, Jeroen Lenaers, Lukas Mandl, Fulvio Martusciello, Nuno Melo, Nadine Morano, Peter Pollák, Emil Radev, Paulo Rangel, Karlo Ressler, Simone Schmiedtbauer, Ralf Seekatz, Sara Skyttedal, Ivan Štefanec, Tomas Tobé, Elissavet Vozemberg-Vrionidi, Javier Zarzalejos
RENEW	Abir Al-Sahlani, Malik Azmani, Gilles Boyer, Sophia in 't Veld, Georgios Kyrtsos, Maite Pagazaurtundúa, Michal Šimečka, Ramona Strugariu, Róża Thun und Hohenstein, Yana Toom
S&D	Marek Paweł Balt, Pietro Bartolo, Jonás Fernández, Hannes Heide, Evin Incir, Karsten Lucke, Javier Moreno Sánchez, Evelyn Regner, Isabel Santos, Birgit Sippel, Paul Tang, Elena Yoncheva
THE LEFT	Konstantinos Arvanitis, Malin Björk, Clare Daly, Miguel Urbán Crespo
VERTS/ALE	Patrick Breyer, Saskia Bricmont, Romeo Franz, Alice Kuhnke, Erik Marquardt, Terry Reintke, Diana Riba i Giner

1	-
NI	Milan Uhrík

4	0
ECR	Assita Kanko, Vincenzo Sofo
ID	Patricia Chagnon, Antonio Maria Rinaldi

Objaśnienie używanych znaków:
+ : za
- : przeciw
0 : wstrzymało się