Future Finance Poland

Warszawa, 20 marca 2025 r.

Szanowny Pan
Wiceminister Cyfryzacji
Dariusz Standerski

Ministerstwo Cyfryzacji
Królewska 27
00-060 Warszawa

sekretariat.dp@cyfra.gov.pl

Szanowny Panie Ministrze,

bardzo dziękujemy za możliwość wzięcia udziału w konsultacjach dotyczących projektu ustawy z dnia 18 lutego 2026 r. o zmianie ustawy o usługach zaufania oraz identyfikacji elektronicznej oraz niektórych innych ustaw (dalej "**Projekt ustawy**").

Projekt ustawy wprowadza szeroki pakiet zmian mających na celu dalsze wzmocnienie i unowocześnienie systemu identyfikacji elektronicznej oraz usług zaufania, przyczyniając się do zwiększenia bezpieczeństwa, interoperacyjności i dostępności usług cyfrowych w Polsce. Jednocześnie projekt ten wdraża przepisy Rozporządzenia Parlamentu Europejskiego i Rady (UE) 2024/1183 z dnia 11 kwietnia 2024 r. w sprawie zmiany rozporządzenia (UE) nr 910/2014 w odniesieniu do ustanowienia europejskich ram tożsamości cyfrowej (dalej "**eIDAS 2.0**"), harmonizując krajowy system identyfikacji elektronicznej z europejskimi standardami.

Proponowane regulacje rozszerzają zakres dotychczasowych przepisów, obejmując m.in. funkcjonowanie europejskiego portfela tożsamości cyfrowej, rozwój usług związanych z dopasowywaniem tożsamości oraz weryfikacją atrybutów, a także stworzenie rejestru stron ufających. Usprawniono procesy wydawania elektronicznych poświadczeń atrybutów oraz doprecyzowano zasady współpracy podmiotów odpowiedzialnych za źródła autentyczne. Zmiany umożliwiają obywatelom, przedsiębiorcom oraz podmiotom publicznym korzystanie z nowoczesnych i bezpiecznych narzędzi cyfrowych, zwiększając wygodę oraz pewność prawną w korzystaniu z usług online.

Całość proponowanych zmian tworzy nowoczesne ramy prawne, które sprzyjają innowacjom, umożliwiają sprawniejsze załatwianie spraw online oraz wspierają dalszy rozwój cyfrowych usług

publicznych. Jednocześnie regulacje te odpowiadają na rosnące potrzeby obywateli i przedsiębiorców w zakresie cyfrowej identyfikacji i bezpiecznej komunikacji z administracją, przyczyniając się do wzrostu zaufania do systemów elektronicznych.

Pomimo pozytywnej oceny całości projektu poniżej przedstawiamy kilka postulatów, które naszym zdaniem warto, aby znalazły odzwierciedlenie w regulacji. W celu uniknięcia wątpliwości pragniemy również wskazać, że w treści postulatów posługujemy się wymiennie pojęciami aplikacji, mObywatel Europa, EUDI Wallet i europejski portfel tożsamości cyfrowej jako pojęciami tożsamymi.

Wiceprezes Fundacji Future Finance Poland

Brak regulacji dotyczących przenoszenia oraz onboardingu użytkowników pomiędzy obecną a nową aplikacją

Projekt ustawy nie zawiera żadnych przepisów ani wytycznych odnoszących się do zasad przenoszenia użytkowników oraz ich danych pomiędzy aktualnie funkcjonującą wersją aplikacji ("**mObywatel**") a nową aplikacją opracowywaną na podstawie eIDAS 2.0 ("**mObywatel Europa**"). W szczególności brak jest jednoznacznych odpowiedzi na następujące kwestie:

1. **Czy migracja użytkowników nastąpi automatycznie**, z zachowaniem dotychczasowych uprawnień, uwierzytelnienia oraz dostępnych dokumentów, **czy też konieczne będzie ponowne przeprowadzenie całego lub częściowego procesu onboardingu** (np. ponowna weryfikacja tożsamości, nie uwzględniając przy tym kwestii środków identyfikacji elektronicznej na poziomie high)?
2. **Kiedy i w jakim trybie mObywatel Europa zastąpi aktualnie działającego mObywatela**, a także czy przewidywany jest okres równoległego funkcjonowania obu aplikacji, umożliwiający płynne przejście użytkowników.
3. **Co stanie się z danymi przechowywanymi w obecnej aplikacji mObywatel**– w szczególności czy zostaną one automatycznie przeniesione do nowej aplikacji mObywatel Europa, w jakim zakresie, w jakiej formie oraz przy zastosowaniu jakich zabezpieczeń.

Brak powyższych regulacji stwarza istotne ryzyko, że część użytkowników nie zrealizuje procesu migracji w sposób prawidłowy, co w efekcie może prowadzić do ich utraty jako aktywnych użytkowników. Tymczasem kluczowe z perspektywy ciągłości działania usług jest utrzymanie możliwie najszerszej i stabilnej bazy użytkowników.

Z tego względu zasadne jest uzupełnienie projektu o przepisy lub przynajmniej delegację ustawową, które wprost określą zasady migracji, tryb zastępowania aplikacji oraz obsługę danych użytkowników.

Ponadto projekt nie precyzuje, w jakim trybie nastąpi wycofanie dotychczasowej aplikacji ani jaki będzie los danych w niej zapisanych — czy zostaną one automatycznie przeniesione, zarchiwizowane, czy też usunięte. Brak jasnych wytycznych w tym zakresie może dodatkowo pogłębić ryzyko dezorientacji użytkowników oraz rozproszenia danych.

W tym kontekście warto również zadbać o odniesienia definicyjne w ustawie o aplikacji mObywatel do nowej aplikacji mObywatel Europa.

Umożliwienie przekazywania danych

Każdy użytkownik aplikacji ma w niej dostęp do swoich danych, a funkcjonalność i atrakcyjność aplikacji rośnie wraz z liczbą dostępnych w niej informacji. Aby korzystanie z aplikacji było jeszcze wygodniejsze i bardziej użyteczne, warto umożliwić podmiotom prywatnym wprowadzanie danych lub udostępnianie w niej usług w sposób prosty i zautomatyzowany.

W praktyce oznacza to, że prywatne podmioty korzystające z aplikacji mogłyby jednocześnie przekazywać do aplikacji własne informacje lub usługi za pośrednictwem odpowiedniego API. Takie podejście ułatwi obywatelom korzystanie z ich uprawnień oraz weryfikację danych, zgodnie z zasadą obustronnej wymiany informacji.

Minister odpowiedzialny za informatyzację mógłby zapewnić dostępność interfejsu API, który pozwoli podmiotom prywatnym na pełną integrację z aplikacją. Interfejs ten powinien obsługiwać zarówno pobieranie, jak i przekazywanie danych użytkowników, przy pełnym zachowaniu przepisów dotyczących ochrony danych osobowych i bezpieczeństwa informacji.

SCA

Zgodnie z obowiązującą ustawą o usługach płatniczych, odpowiedzialność za prawidłowe przeprowadzenie silnego uwierzytelnienia klienta (Strong Customer Authentication, SCA) spoczywa na dostawcy usługi płatniczej, który realizuje transakcję. Podmiot ten zobowiązany jest do zapewnienia, aby każda autoryzacja płatności spełniała wymogi bezpieczeństwa przewidziane w tejże ustawie, w tym m.in.: zastosowania co najmniej dwóch niezależnych elementów uwierzytelnienia (wiedza, posiadanie, cecha), zapewnienia integralności i poufności

danych w trakcie uwierzytelniania czy też ograniczenia ryzyka nadużyć i nieautoryzowanych transakcji. Brak dopełnienia tych obowiązków może skutkować odpowiedzialnością cywilną oraz sankcjami nadzorczymi ze strony Komisji Nadzoru Finansowego.

Jednocześnie Projekt ustawy nie precyzuje zasad odpowiedzialności w przypadku dokonywania SCA za pomocą EUDI Wallet. Brak jasnych regulacji w tym zakresie rodzi istotne ryzyko prawne i praktyczne: nie jest określone, kto odpowiada za prawidłowe uwierzytelnienie, w jaki sposób należy zapewnić bezpieczeństwo transakcji ani jakie konsekwencje ponosi dostawca usługi lub użytkownik w przypadku błędów lub nadużyć.

W związku z tym konieczne jest doprecyzowanie przepisów, które jednoznacznie wskażą odpowiedzialność stron i zasady przeprowadzania SCA w przypadku korzystania z EUDI Wallet, aby zapewnić bezpieczeństwo użytkowników i pewność prawną podmiotów świadczących usługi płatnicze.

Płatności elektroniczne

W art. 14g ust. 1 Projektu ustawy przewidziano, że w europejskim portfelu tożsamości cyfrowej, o którym mowa w art. 5a ust. 2 lit. a eIDAS 2.0, mogą być udostępniane różne usługi umożliwiające użytkownikowi europejskiego portfela tożsamości cyfrowej, w tym m.in. „dokonywanie płatności elektronicznych związanych z usługami online świadczonymi na rzecz użytkownika europejskiego portfela tożsamości cyfrowej, o którym mowa w art. 5a ust. 2 lit. a rozporządzenia 910/2014;".

Zwracamy uwagę, że eIDAS 2.0 nie przewiduje obsługi przez europejski portfel tożsamości cyfrowej „dokonywania płatności elektronicznych". Oznacza to, że Projekt ustawy w tym zakresie wykracza poza ramy eIDAS 2.0 i nie jest niezbędny do jego implementacji. Należy również zaznaczyć, że eIDAS 2.0 nie nakłada obowiązku obsługi takich płatności na uczestników rynku. Obowiązek dotyczy wyłącznie stosowania silnego uwierzytelniania użytkownika (zob. art. 5f ust. 2 eIDAS 2.0). Wprawdzie Projekt ustawy również nie nakłada obowiązku na inne podmioty obsługi takich płatności (jest tam mowa tylko o „możliwości" udostępniania usług, o których mowa w tym przepisie), jednak – dla przejrzystości tej regulacji – proponujemy odpowiednie doprecyzowanie w formie ust. 3 do tego artykułu:

3. Umożliwienie korzystania z usług, o których mowa w ust. 1 i 2, przez strony ufające lub inne podmioty, jest dobrowolne, chyba że co innego wynika z niniejszej ustawy lub z przepisów odrębnych.

Warto również dodać, że „dokonywanie płatności elektronicznych" jest co do zasady świadczeniem usług płatniczych. Należałoby zatem wyjaśnić, w jakim zakresie i na jakich zasadach usługi takie będą świadczone, oraz kwestie jak np. zakres odpowiedzialności dostawcy

europejskiego portfela tożsamości cyfrowej wobec użytkowników z tytułu nieautoryzowanych transakcji płatniczych. Ponieważ rynek usług płatniczych jest bardzo konkurencyjny, potrzebne jest również uzasadnienie, dlaczego projektodawca uważa, że państwo (Minister właściwy do spraw informatyzacji) powinno świadczyć takie usługi, być może wypierając dostawców sektora prywatnego z tego rynku. Sugerujemy również rozważenie, czy celem projektodawcy nie było raczej, aby dostawca portfela był kwalifikowany nie jako dostawca usług płatniczych, ale jako dostawca usług technicznych, wzorem portfeli Apple albo Google. Wówczas należałoby odpowiednio przeredagować ten przepis i zrezygnować z frazy „dokonywanie płatności elektronicznych".

Podpisy elektroniczne

W art. 14e ust. 1 Projektu ustawy przewidziano, że przy użyciu europejskiego portfela tożsamości cyfrowej możliwe będzie nieodpłatne składanie kwalifikowanych podpisów elektronicznych w celach innych niż profesjonalne. W związku z tym pojawiają się wątpliwości co do skutków prawnych użycia takiego podpisu w celach profesjonalnych, w tym czy podpis pozostaje wówczas ważny. Proponujemy więc doprecyzowanie, że cel podpisu nie wpływa na jego ważność ani skuteczność prawną, a odpowiedzialność za zgodność użycia podpisu z deklarowanym celem ponosi wyłącznie osoba składająca podpis. Strona ufająca nie powinna być zobowiązana do weryfikowania, czy podpis został użyty zgodnie z deklarowanym celem. Doprecyzowanie to jest niezbędne dla zapewnienia jednoznaczności przepisów i ma zapobiec sytuacjom, w których ważność kwalifikowanego podpisu mogłaby być podważana lub kwestionowana wyłącznie ze względu na deklarowany cel, chroniąc tym samym skuteczność prawną dokumentu, którym podpis został opatrzony.

Obowiązek akceptacji EUDI Wallet

Postulujemy wprowadzenie przepisu doprecyzowującego status numeru identyfikacyjnego EUDI Wallet w procesach identyfikacji tożsamości, w tym w procedurach przeciwdziałania praniu pieniędzy i finansowaniu terroryzmu (AML/KYC). Proponowana zmiana do Art. 6 ust. 2 Projektu ustawy, wprowadzająca art. 14a ust. 2, przewiduje dodanie przepisu w części dotyczącej danych identyfikujących osoby, w którym wskazuje się, że identyfikator przekazywany z europejskiego portfela tożsamości cyfrowej może być stosowany w rozumieniu numeru i serii dokumentu tożsamości w procesach weryfikacji tożsamości w sektorze finansowym. Nowy ustęp mógłby brzmieć następująco: „W procesach identyfikacji i weryfikacji tożsamości prowadzonych na podstawie przepisów odrębnych, w szczególności dotyczących przeciwdziałania praniu pieniędzy i finansowaniu terroryzmu, „numer danych identyfikujących daną osobę", o którym mowa w art. 14a ust. 2 pkt 4, przekazywany z europejskiego portfela tożsamości cyfrowej, może być traktowany jako numer dokumentu identyfikacyjnego osoby." Doprecyzowanie to jest niezbędne, ponieważ sektor finansowy potrzebuje jednoznacznej podstawy prawnej do wykorzystywania

identyfikatora z portfela w procedurach AML/KYC. Obecnie przepisy regulacji AML wymagają podczas identyfikacji pobrania numeru i serii dokumentu tożsamości, niezależnie od tego, czy identyfikacja przebiega na podstawie dokumentu tożsamości, czy środka identyfikacji elektronicznej.

Ponadto postuluje się doprecyzowanie Projektu ustawy w zakresie tzw. „pełnego zestawu danych", numeru PESEL oraz portfeli wydawanych w innych państwach UE, w taki sposób, aby brak PESEL nie uniemożliwiał przeprowadzenia identyfikacji. Art. 6 ust. 2 Projektu ustawy, wprowadzający art. 14a ust. 2, powinien obejmować następujące elementy: wprowadzenie definicji, że europejski portfel tożsamości cyfrowej w przepisach krajowych obejmuje także portfele wydane lub uznane przez inne państwa członkowskie UE, w zakresie uznawania wynikającym z eIDAS 2.0; doprecyzowanie, że europejski portfel cyfrowy zawiera Krajowy Numer Identyfikacyjny, o ile taki numer został ustanowiony w danym kraju; oraz wskazanie, że dla Europejskich Środków Identyfikacji Elektronicznej wydawanych w Polsce Krajowym Numerem Identyfikacyjnym, o którym mowa w art. 14a ust. 2 pkt 5, będzie numer PESEL. Takie doprecyzowanie eliminuje ryzyko interpretacji, w której brak numeru PESEL w portfelu uniemożliwia identyfikację, co jest szczególnie istotne w przypadku klientów bez PESEL, w tym cudzoziemców, oraz w kontekście portfeli transgranicznych przekazujących różne zestawy danych. Wyraźne ujęcie tych zasad w art. 14a ust. 2 zapewnia, że procesy onboardingowe i dostęp do usług pozostaną możliwe, a praktyka rynkowa w zakresie stosowania europejskich portfeli tożsamości cyfrowej będzie jednolita.

Proponowany mechanizm „selektywnego udostępniania danych" jest korzystny z perspektywy ochrony prywatności klientów, jednak może stanowić istotną barierę operacyjną dla wielu instytucji, ponieważ w praktyce skutkuje otrzymywaniem niekompletnych danych niezbędnych do przeprowadzenia procesów identyfikacji, zawarcia umowy lub realizacji transakcji. W związku z tym mechanizm powinien umożliwiać stronie ufającej, czyli instytucji, wymuszenie określonego profilu danych (pakietu), który jest niezbędny do realizacji danej usługi. Klient powinien mieć możliwość wyboru między udostępnieniem wszystkich danych wymaganych ustawowo a rezygnacją z korzystania z usługi, zamiast możliwości przesyłania niepełnych formularzy lub ograniczania zakresu zgód na przetwarzanie danych w odniesieniu do poszczególnych celów. Takie podejście pozwala zachować równowagę między ochroną prywatności a zapewnieniem prawidłowego funkcjonowania usług finansowych.

Art. 14a Projektu ustawy określa zakres danych identyfikujących osobę fizyczną, obejmujący m.in. "wizerunek twarzy użytkownika portfela". W praktyce oznacza to, że w procesie identyfikacji przy wzajemnej fizycznej obecności stron strona ufająca może porównać wizerunek twarzy pobrany z EUDI Wallet z osobą, która faktycznie stoi przed nią, co jest równoważne weryfikacji z dokumentu tożsamości. Warto podkreślić, że eIDAS 2.0 nie nakłada obowiązku akceptacji wszystkich atrybutów portfela, w tym wizerunku twarzy, w relacjach z instytucjami

przy identyfikacji użytkownika - polski projekt ustawy idzie w tym zakresie o krok dalej, umożliwiając w praktyce porównanie wizerunku z portfela z osobą fizycznie obecną, co w efekcie zrównuje PID z dokumentem tożsamości w procesach stacjonarnych. Jednocześnie projekt nie precyzuje, że akceptacja tej formy identyfikacji jest obligatoryjna w procesach onboardingowych, co może rodzić różne interpretacje po stronie instytucji finansowych. Doprecyzowanie art. 14a jest więc kluczowe dla zapewnienia zgodności procedur identyfikacyjnych oraz zachowania jednoznacznej praktyki rynkowej w zakresie stosowania europejskich portfeli tożsamości cyfrowej zarówno w procesach stacjonarnych, jak i zdalnych.

Rozdzielenie roli nadzorcy od wykonawcy

W projekcie ustawy konieczne jest wyraźne rozdzielenie roli nadzorcy od roli wykonawcy usług w zakresie funkcjonowania europejskiego portfela tożsamości cyfrowej. Obecnie projekt wskazuje ministra właściwego ds. cyfryzacji jako organ odpowiedzialny zarówno za nadzór nad wdrażaniem portfela, jak i za zapewnienie jego operacyjnego funkcjonowania. Takie połączenie funkcji może rodzić ryzyko konfliktu interesów i niejasności kompetencyjnych. W praktyce nadzór powinien obejmować monitorowanie zgodności działania portfela z przepisami prawa, natomiast funkcje wykonawcze — utrzymanie infrastruktury, udostępnianie danych i interfejsów API — powinny być realizowane przez niezależny podmiot lub wyspecjalizowany departament. Wyraźne oddzielenie tych ról pozwoli na większą przejrzystość procesów, wzmocni bezpieczeństwo operacyjne, ograniczy potencjalne konflikty interesów i zapewni, że nadzór będzie wykonywany w sposób obiektywny, a decyzje dotyczące funkcjonowania portfela nie będą obciążone bezpośrednim uczestnictwem ministra w procesie operacyjnym.

Katalog podmiotów publicznych

W projekcie ustawy przewidziano utworzenie katalogu podmiotów publicznych. Należy jednak zwrócić uwagę, że istnieje już taki katalog, co rodzi pytanie o zasadność tworzenia kolejnego odrębnego rejestru. Wprowadzenie nowego katalogu mogłoby skutkować niepotrzebnym powielaniem danych, zwiększeniem kosztów administracyjnych i komplikacją procedur aktualizacji.

EUDI Wallet a EBW

W pierwotnych założeniach projekt europejskiego portfela tożsamości cyfrowej (eUDI Wallet) miał obejmować wyłącznie osoby fizyczne, natomiast dla jednoosobowych działalności gospodarczych (JDG) i osób prawnych przewidziano odrębną aplikację EBW, która miała służyć do identyfikacji i uwierzytelniania podmiotów nieosobowych w kontaktach z administracją publiczną i instytucjami prywatnymi. W aktualnym Projekcie ustawy zakres EUDI Wallet został rozszerzony w sposób obejmujący także JDG i osoby prawne, co rodzi pytania o spójność

regulacyjną, praktyczne konsekwencje dla przyszłych aplikacji EBW oraz potencjalne ryzyka wynikające z konkurencji między portfelami. W praktyce podmioty gospodarcze mogą nie wiedzieć, który portfel powinny stosować, a instytucje przyjmujące dane mogą otrzymywać niejednolity zestaw informacji identyfikacyjnych.

Konieczne jest więc wyraźne wskazanie w Projekcie ustawy, czy stanowi ona też implementację regulacji unijnych dotyczących portfela biznesowego.

Dane statystyczne

Aktualnie brakuje informacji statystycznych dotyczących wykorzystywania usług zaufania oraz elektronicznej identyfikacji. Przez to rynek nie może być zwymiarowany ilościowo, co wpływa negatywnie na jego transparentność, określenie wagi dla całego ekosystemu cyfrowych usług komercyjnych i publicznych. Proponujemy aby w Projekcie ustawy wprowadzić zapisy zobowiązujące:

- kwalifikowanych dostawców usług zaufania do przekazywania do Ministra Cyfryzacji, informacji o wykorzystaniu poszczególnych usług zaufania za poprzedni kwartał np. do 15-ego miesiąca po końcu danego kwartału i publikacji przez Ministra Cyfryzacji zagregowanych danych w tym zakresie do końca danego miesiąca;
- dostawcę krajowego Europejskiego Portfela Tożsamości Cyfrowej do przekazywania do Ministra Cyfryzacji informacji o wykorzystaniu EUDI Wallet (w zakresie liczby użytkowników oraz transakcyjności), za poprzedni kwartał, np. do 15. miesiąca po końcu danego kwartału, i publikacji przez Ministra Cyfryzacji zagregowanych danych w tym zakresie do końca danego miesiąca.

Szczegółowe założenia do określenia statystyki w tym zakresie byłyby do uszczegółowienia w odpowiednim akcie wykonawczym do ustawy.