Uwagi do projektu ustawy o zmianie ustawy o usługach zaufania oraz identyfikacji elektronicznej oraz niektórych innych ustaw wdrażającego EIDAS 2.0

1) Dobrowolność uznawania Europejskiego Portfela Tożsamości Cyfrowej podczas wzajemnej fizycznej obecności stron

Należy jednoznacznie określić w przepisach, że uznawanie Europejskiego Portfela Tożsamości Cyfrowej (EPTC) w procesach identyfikacji prowadzonych w placówkach, tj. w sytuacji wzajemnej fizycznej obecności stron, **nie stanowi obowiązku dla podmiotów sektora prywatnego, w tym banków**.

Uzasadnienie

Projektowany art. 14d ustawy może być interpretowany jako wprowadzający obowiązek uznawania EPTC w procesach identyfikacji prowadzonych podczas fizycznej obsługi klienta. Tymczasem regulacje rozporządzenia eIDAS wskazują jednoznacznie, że europejski portfel tożsamości cyfrowej jest przede wszystkim **środkiem identyfikacji elektronicznej przeznaczonym do wykorzystania w usługach online**.

Choć rozporządzenie eIDAS nie wyklucza wykorzystania portfela w trybie offline, nie przewiduje w tym zakresie żadnego obowiązku jego akceptacji przez strony ufające. Zgodnie z konstrukcją systemu eIDAS, korzystanie z portfela przez prywatne strony ufające ma charakter **co do zasady dobrowolny**, a podmiot zainteresowany jego wykorzystaniem podlega dobrowolnemu procesowi rejestracji w odpowiednim systemie.

Wyjątki od tej zasady przewidziano jedynie w ściśle określonych sytuacjach wskazanych w art. 5f ust. 2 i 3 rozporządzenia eIDAS, w szczególności w odniesieniu do:

1. prywatnych dostawców usług zobowiązanych do stosowania silnego uwierzytelnienia użytkownika (SCA) w ramach usług online, z wyłączeniem mikroprzedsiębiorstw i małych przedsiębiorstw,
2. bardzo dużych platform internetowych.

W żadnym przypadku rozporządzenie eIDAS nie wprowadza obowiązku uznawania portfela w procesach identyfikacji prowadzonych w trybie offline.

Wprowadzenie takiego obowiązku na poziomie prawa krajowego oznaczałoby w praktyce odejście od zasady dobrowolności po stronie prywatnych stron ufających, która została wyraźnie wskazana w rozporządzeniu eIDAS, w szczególności w pkt 17 preambuły oraz w art. 5b ust. 1 tego rozporządzenia.

Należy również podkreślić, że **EPTC nie stanowi dokumentu tożsamości**, lecz środek identyfikacji elektronicznej. Zgodnie z art. 3 rozporządzenia eIDAS:

- pkt 2 definiuje środek identyfikacji elektronicznej jako materialną lub niematerialną jednostkę zawierającą dane identyfikujące osobę i wykorzystywaną do uwierzytelniania w usługach online lub – **w stosownych przypadkach** – offline,

- pkt 34 określa europejski portfel tożsamości cyfrowej jako **środek identyfikacji elektronicznej** umożliwiający przechowywanie, zarządzanie oraz udostępnianie danych identyfikujących osobę i elektronicznych poświadczeń atrybutów,
- pkt 57 definiuje tryb offline jako interakcję między użytkownikiem a stroną trzecią w fizycznej lokalizacji **przy użyciu technologii zbliżeniowych**, przy czym europejski portfel tożsamości cyfrowej nie musi mieć dostępu do systemów zdalnych za pośrednictwem sieci komunikacji elektronicznej do celów tej interakcji.

Jednocześnie art. 5a rozporządzenia eIDAS wskazuje, że portfel umożliwia uwierzytelnianie wobec stron ufających **w trybie online, a jedynie w stosownych przypadkach także offline**. Oznacza to, że zastosowanie portfela w środowisku offline ma charakter **wyjątkowy**, a nie powszechny.

Co istotne, wykorzystanie portfela w trybie offline powinno odbywać się przy użyciu technologii zbliżeniowych oraz z zachowaniem zasad selektywnego ujawniania danych. Samo okazanie wizualizacji danych z portfela wraz z wizerunkiem użytkownika nie spełnia tych wymogów technicznych.

Dodatkowo należy wskazać, że projektowany przepis wzorowany jest na rozwiązaniu funkcjonującym w ustawie o aplikacji mObywatel, w której obok środka identyfikacji elektronicznej mObywatel wprowadzono **nową kategorię krajowego dokumentu tożsamości – mDowód**. Europejski portfel tożsamości cyfrowej nie jest jednak dokumentem tożsamości i żadne przepisy prawa unijnego nie nadają mu takiego statusu ani nie upoważniają państw członkowskich do jego wprowadzenia.

Nałożenie obowiązku uznawania EPTC na wszystkie instytucje w Polsce – w tym również w odniesieniu do portfeli wydanych przez inne państwa członkowskie – na obecnym etapie wdrożenia tego rozwiązania wiązałoby się z istotnymi kosztami wdrożeniowymi przy jednoczesnym braku realnych korzyści operacyjnych. W przeciwieństwie do rozwiązania mDowód, które było krajowym systemem o szerokiej adopcji rynkowej już w momencie jego wprowadzenia, europejski portfel tożsamości cyfrowej znajduje się dopiero na wczesnym etapie implementacji.

Należy również zauważyć, że portfele wydawane przez inne państwa członkowskie mogą zawierać odmienny zestaw danych identyfikacyjnych, w tym w szczególności mogą nie zawierać wizerunku użytkownika. Może to dodatkowo utrudniać ich wykorzystanie w procesach identyfikacji prowadzonych w placówkach.

Jednocześnie brak obowiązku uznawania portfela w trybie offline nie powinien negatywnie wpłynąć na jego wykorzystanie w sektorze bankowym. Banki będą bowiem zobowiązane – zgodnie z rozporządzeniem eIDAS – do umożliwienia wykorzystania portfela w procesach silnego uwierzytelnienia użytkownika (SCA) najpóźniej od końca 2027 r.

Dodatkowo projekt nie rozstrzyga jednoznacznie, czy ewentualny obowiązek uznawania portfela miałby obejmować również portfele wydane przez inne państwa członkowskie.

W przypadku gdyby ustawodawca zdecydował się jednak na wprowadzenie obowiązku akceptacji portfela przez instytucje obowiązane, konieczne byłoby zapewnienie **odpowiednio długiego okresu dostosowawczego**. W szczególności należałoby rozważyć powiązanie takiego obowiązku z terminem wynikającym z art. 5f ust. 2 rozporządzenia eIDAS, tj. **24 grudnia 2027 r.**, i **wprowadzenie co najmniej rocznego vacatio legis** umożliwiającego dostosowanie systemów oraz procesów operacyjnych instytucji finansowych.

2) Środek identyfikacji elektronicznej jako identyfikator użyteczny w procesach AML - doprecyzowanie statusu

Należy wprowadzić przepis jednoznacznie wskazujący, że numer identyfikacyjny europejskiego środka identyfikacji elektronicznej może być wykorzystywany jako odpowiednik numeru dokumentu tożsamości w procesach identyfikacji i weryfikacji tożsamości.

W art. 6 ust. 2 projektu ustawy, wprowadzającym art. 14a ustawy o aplikacji mObywatel, zdaniem sektora zasadnym byłoby dodanie przepisu w części dotyczącej danych identyfikujących osobę, który wskazywałby, że identyfikator przekazywany z europejskiego portfela tożsamości cyfrowej może być wykorzystywany jako numer identyfikacyjny w procesach identyfikacji tożsamości prowadzonych przez podmioty sektora finansowego. Sugerujemy dodanie do projektu przepisu w brzmieniu: „W procesach identyfikacji i weryfikacji tożsamości prowadzonych na podstawie przepisów odrębnych, w szczególności dotyczących przeciwdziałania praniu pieniędzy oraz finansowaniu terroryzmu, numer danych identyfikujących 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."

Uzasadnienie

Sektor finansowy wnosi o zapewnienie jednoznacznej podstawy prawnej umożliwiającej wykorzystanie identyfikatora przekazywanego przez europejski portfel tożsamości cyfrowej w procedurach identyfikacji klienta prowadzonych na podstawie przepisów dotyczących przeciwdziałania praniu pieniędzy i finansowaniu terroryzmu (AML/CFT).

Zgodnie z art. 36 ustawy z dnia 1 marca 2018 r. o przeciwdziałaniu praniu pieniędzy oraz finansowaniu terroryzmu instytucje obowiązane są zobowiązane do ustalenia m.in. serii i numeru dokumentu tożsamości klienta. Obowiązek ten dotyczy procesów identyfikacji i weryfikacji tożsamości klienta niezależnie od tego, czy identyfikacja odbywa się na podstawie dokumentu tożsamości, czy przy wykorzystaniu środka identyfikacji elektronicznej.

Projekt ustawy nie rozstrzyga jednoznacznie, czy identyfikacja przeprowadzona przy wykorzystaniu europejskiego portfela tożsamości cyfrowej - w szczególności na wysokim poziomie bezpieczeństwa - spełnia wymogi identyfikacji i weryfikacji tożsamości określone w przepisach AML. Nie jest również jasne, czy elektroniczne poświadczenie atrybutów wydawane przez ministra właściwego do spraw informatyzacji, o którym mowa w art. 22g projektu ustawy, może być uznawane za wystarczające dla celów procedur KYC.

Brak jednoznacznych regulacji w tym zakresie może prowadzić do niepewności prawnej oraz utrudniać wykorzystanie portfela w procesach identyfikacji klientów przez instytucje finansowe.

Jednocześnie z uzasadnienia do projektu ustawy wynika, że zestaw metadanych odnoszących się do wydawanego zestawu danych identyfikujących osobę obejmuje m.in. numer danych identyfikujących osobę nadany przez dostawcę danych identyfikujących osobę. W praktyce numer ten może pełnić funkcję zbliżoną do numeru dokumentu identyfikacyjnego, podobnie jak numer dokumentu mObywatel nadawany po ustaleniu tożsamości użytkownika.

W związku z powyższym zasadne jest jednoznaczne przesądzenie w przepisach, że identyfikator przekazywany przez europejski portfel tożsamości cyfrowej może być traktowany jako odpowiednik numeru dokumentu tożsamości na potrzeby procesów identyfikacji prowadzonych przez instytucje obowiązane.

Jednocześnie projekt ustawy nie odnosi się wprost do relacji pomiędzy regulacjami dotyczącymi europejskiego portfela tożsamości cyfrowej a przepisami ustawy o przeciwdziałaniu praniu pieniędzy i finansowaniu terroryzmu. W związku z tym warto rozważyć również wprowadzenie przepisu interpretacyjnego lub odpowiedniej zmiany w ustawie AML, która jednoznacznie wskazywałaby, że identyfikacja przeprowadzona przy użyciu europejskiego środka identyfikacji elektronicznej na wysokim poziomie bezpieczeństwa spełnia wymogi identyfikacji i weryfikacji tożsamości klienta na potrzeby AML/CFT.

Dodatkowo projekt ustawy nie wyjaśnia w sposób wystarczający, w jaki sposób europejski portfel tożsamości cyfrowej będzie funkcjonował w relacji do infrastruktury krajowej identyfikacji elektronicznej, w szczególności do tzw. **Węzła Krajowego**. Dotychczasowe założenia dotyczące wdrożenia eIDAS 2 wskazywały, że portfel będzie funkcjonował jako środek identyfikacji elektronicznej niezależny od tej infrastruktury. W związku z tym zasadne jest doprecyzowanie, czy zgodnie z projektowanymi przepisami portfel będzie osadzony w Węźle Krajowym oraz czy strony ufające będą zobowiązane do integracji z tym systemem w celu korzystania z portfela.

3) Numer PESEL i portfele transgraniczne - doprecyzowanie zakresu danych identyfikujących

Zdaniem sektora należy doprecyzować przepisy projektu ustawy w celu:

1. jednoznacznego wskazania, że regulacje dotyczące europejskiego portfela tożsamości cyfrowej odnoszą się do wszystkich portfeli zapewnianych zgodnie z rozporządzeniem eIDAS, w tym portfeli wydawanych przez inne państwa członkowskie Unii Europejskiej;
2. wyeliminowania interpretacji, zgodnie z którą brak numeru PESEL w zestawie danych identyfikujących osobę przekazywanych przez portfel uniemożliwia przeprowadzenie identyfikacji;
3. doprecyzowania, że portfel zawiera krajowy numer identyfikacyjny właściwy dla państwa wydającego środek identyfikacji elektronicznej, przy czym w przypadku portfeli wydawanych w Polsce będzie nim numer PESEL.

Uzasadnienie

Z projektowanego art. 14d ust. 1 ustawy o aplikacji mObywatel wynika, że komplet danych identyfikujących osobę przekazywany z europejskiego portfela tożsamości cyfrowej ma umożliwiać spełnienie obowiązku stwierdzenia tożsamości lub obywatelstwa na podstawie dokumentu tożsamości. W związku z tym konieczne jest zapewnienie, aby zestaw danych dostępnych w portfelu był spójny z wymaganiami identyfikacyjnymi wynikającymi z innych przepisów prawa, w szczególności z regulacji dotyczących przeciwdziałania praniu pieniędzy i finansowaniu terroryzmu (AML/CFT).

Z projektowanego art. 14a ust. 2 wynika, że europejski portfel tożsamości cyfrowej zawiera zestaw danych identyfikujących osobę fizyczną obejmujący m.in. imię, nazwisko, datę i miejsce urodzenia, numer PESEL, obywatelstwo, płeć, nazwisko rodowe (jeżeli występuje w rejestrze PESEL) oraz wizerunek twarzy użytkownika portfela.

Jednocześnie należy uwzględnić, że portfele wydawane w innych państwach członkowskich mogą przekazywać odmienny zestaw danych identyfikacyjnych, w tym w szczególności mogą nie zawierać numeru PESEL. W praktyce sektor finansowy obsługuje znaczną liczbę klientów nieposiadających numeru PESEL, w tym cudzoziemców.

Brak jednoznacznego doprecyzowania przepisów może prowadzić do powstania interpretacji, zgodnie z którą brak numeru PESEL w zestawie danych przekazywanych przez portfel uniemożliwiałby przeprowadzenie identyfikacji. W konsekwencji mogłoby to utrudniać lub blokować procesy onboardingowe oraz dostęp do usług finansowych dla klientów korzystających z portfeli wydanych w innych państwach członkowskich.

Ponadto brak jednoznacznych regulacji w tym zakresie może prowadzić do niejednolitej praktyki rynkowej w zakresie wykorzystywania portfeli transgranicznych przez instytucje finansowe.

W związku z powyższym zasadne jest doprecyzowanie przepisów w taki sposób, aby jednoznacznie wskazywały, że europejski portfel tożsamości cyfrowej obejmuje portfele wydawane w innych państwach członkowskich UE oraz że portfel zawiera krajowy numer identyfikacyjny właściwy dla państwa wydającego środek identyfikacji elektronicznej, którym w przypadku portfeli wydawanych w Polsce jest numer PESEL.

4) Podpis kwalifikowany „do celów innych niż profesjonalne” - brak obowiązku weryfikacji celu po stronie banku/strony ufającej

Należy doprecyzować przepisy projektu w zakresie kwalifikowanego podpisu elektronicznego udostępnianego w ramach europejskiego portfela tożsamości cyfrowej w taki sposób, aby:

1. jednoznacznie wskazać, że oznaczenie podpisu kwalifikowanego jako wykorzystywanego „do celów innych niż profesjonalne” nie wpływa na jego ważność ani skuteczność prawną;
2. wyraźnie określić, że strona ufająca nie jest zobowiązana do weryfikowania celu, w jakim podpis został użyty;
3. wskazać, że odpowiedzialność za wykorzystanie podpisu zgodnie z deklarowanym celem spoczywa na osobie składającej podpis.

<u>Uzasadnienie</u>

Projekt ustawy przewiduje wprowadzenie możliwości nieodpłatnego składania kwalifikowanego podpisu elektronicznego przez użytkowników europejskiego portfela tożsamości cyfrowej, przy czym możliwość ta ma być ograniczona do celów „innych niż

profesjonalne”. Jednocześnie projekt nie określa skutków prawnych użycia takiego podpisu w sytuacji, gdy został on wykorzystany do celów profesjonalnych.

Z uzasadnienia projektu wynika, że ustawodawca nie przewiduje w tym zakresie żadnej sankcji prawnej. Powoduje to poważne wątpliwości interpretacyjne dotyczące skutków prawnych czynności prawnych dokonanych przy użyciu podpisu oznaczonego jako „nieprofesjonalny”, w szczególności w kontekście prawa cywilnego. Nie jest jasne, czy ewentualne wykorzystanie takiego podpisu do celów profesjonalnych mogłoby prowadzić do podważenia skuteczności prawnej czynności, której podpis dotyczy.

Brak jednoznacznej regulacji w tym zakresie rodzi również pytanie, czy ciężar oceny prawidłowości użycia podpisu ma zostać przeniesiony na strony ufające, które byłyby zobowiązane do badania celu jego wykorzystania. W praktyce oznaczałoby to przerzucenie na podmioty prywatne ryzyka prawnego związanego z oceną ważności podpisu oraz potencjalnych sporów dotyczących skuteczności oświadczeń woli.

Taki stan prawny mógłby prowadzić do istotnego ograniczenia pewności obrotu gospodarczego oraz zwiększenia ryzyka procesowego po stronie podmiotów korzystających z podpisów kwalifikowanych, w tym instytucji finansowych, które są jednymi z największych odbiorców podpisów elektronicznych.

Dodatkowe wątpliwości pojawiają się w kontekście transgranicznym, w szczególności w sytuacji, gdy użytkownik posługujący się portfelem wydanym przez inne państwo członkowskie dokona czynności prawnej ze stroną ufającą w Polsce. W takim przypadku nie jest jasne, czy strona ufająca miałaby obowiązek badania regulacji obowiązujących w państwie wydającym portfel w zakresie rozróżnienia podpisów profesjonalnych i nieprofesjonalnych.

Należy również podkreślić, że zgodnie z rozporządzeniem eIDAS kwalifikowany podpis elektroniczny jest równoważny podpisowi własnoręcznemu. Wprowadzenie dodatkowej kategorii podpisu kwalifikowanego o ograniczonym zakresie zastosowania może prowadzić do niejednoznaczności interpretacyjnych oraz zwiększenia ryzyk operacyjnych i prawnych dla podmiotów korzystających z tego rozwiązania.

Ponadto rozporządzenie eIDAS 2.0 nie nakłada na państwa członkowskie obowiązku wprowadzania rozróżnienia pomiędzy podpisem kwalifikowanym wykorzystywanym do celów profesjonalnych i nieprofesjonalnych. Regulacja taka została przewidziana jedynie jako możliwość pozostawiona do decyzji ustawodawcy krajowego. Wprowadzenie takiego rozróżnienia bez jednoczesnego jednoznacznego określenia skutków prawnych użycia podpisu może prowadzić do niepewności prawnej zarówno po stronie użytkowników portfela, jak i po stronie podmiotów przyjmujących podpisane dokumenty.

W związku z powyższym zasadne jest doprecyzowanie przepisów w taki sposób, aby jasno wskazywały, że oznaczenie podpisu jako wykorzystywanego do celów innych niż profesjonalne nie wpływa na jego ważność ani skuteczność prawną, a odpowiedzialność za zgodność wykorzystania podpisu z deklarowanym celem ponosi osoba składająca podpis.

5) Relacja europejskiego portfela tożsamości cyfrowej do obowiązku stosowania silnego uwierzytelnienia użytkownika (SCA)

Należy doprecyzować przepisy projektu ustawy w zakresie relacji pomiędzy wykorzystaniem europejskiego portfela tożsamości cyfrowej a obowiązkiem stosowania silnego uwierzytelnienia użytkownika (SCA) wynikającym z przepisów ustawy o usługach płatniczych. W szczególności konieczne jest:

1. jednoznaczne określenie, w jaki sposób wykorzystanie portfela może spełniać wymogi silnego uwierzytelnienia użytkownika w rozumieniu przepisów regulujących usługi płatnicze;

2. doprecyzowanie, czy uwierzytelnienie użytkownika w ramach portfela (np. z wykorzystaniem biometrii lub innych mechanizmów uwierzytelniania dostępnych w aplikacji) może być uznane za spełnienie wymogów SCA, czy też konieczne będzie zastosowanie dodatkowych elementów uwierzytelnienia po stronie dostawcy usług płatniczych;

3. określenie zasad odpowiedzialności w przypadku wykorzystania portfela do autoryzacji transakcji, które okażą się nieautoryzowane z uwagi na nieuprawnione użycie portfela przez osobę trzecią.

Uzasadnienie

Zgodnie z art. 32i ust. 1 ustawy o usługach płatniczych dostawca usług płatniczych jest zobowiązany do stosowania silnego uwierzytelnienia użytkownika w przypadku, gdy płatnik uzyskuje dostęp do swojego rachunku w trybie online, inicjuje elektroniczną transakcję płatniczą lub dokonuje za pomocą kanału zdalnego czynności, która może wiązać się z ryzykiem oszustwa lub innych nadużyć.

Projekt ustawy przewiduje, że europejski portfel tożsamości cyfrowej może umożliwiać m.in. dokonywanie płatności elektronicznych. Jednocześnie projekt nie zawiera szczegółowych regulacji określających sposób wykorzystania portfela w kontekście obowiązków związanych ze stosowaniem silnego uwierzytelnienia użytkownika przez dostawców usług płatniczych.

Powoduje to istotne wątpliwości interpretacyjne dotyczące praktycznego funkcjonowania portfela w środowisku usług płatniczych. W szczególności nie jest jasne, czy uwierzytelnienie użytkownika dokonywane w ramach portfela – przykładowo przy wykorzystaniu biometrii lub innych mechanizmów dostępnych w aplikacji – będzie mogło być uznane za spełnienie wymogów silnego uwierzytelnienia użytkownika w rozumieniu przepisów ustawy o usługach płatniczych, czy też konieczne będzie zastosowanie dodatkowych elementów uwierzytelnienia przez bank.

Dodatkowo projekt ustawy nie odnosi się do kwestii odpowiedzialności w sytuacji, w której portfel zostałby wykorzystany do autoryzacji transakcji płatniczej przez osobę nieuprawnioną. Z jednej strony ustawodawca w uzasadnieniu projektu wskazuje na ryzyka związane z kradzieżą tożsamości, z drugiej jednak projekt nie przewiduje mechanizmów odpowiedzialności w przypadku, gdy do nieautoryzowanej transakcji dojdzie w wyniku nieprawidłowego przypisania portfela do użytkownika lub jego przejęcia przez osobę trzecią.

Zgodnie z art. 46 ustawy o usługach płatniczych bank jest zobowiązany do zwrotu kwoty nieautoryzowanej transakcji płatniczej, nawet jeśli nie miał wpływu na proces wydania portfela ani na mechanizmy jego zabezpieczenia. W praktyce oznacza to przeniesienie na dostawców usług płatniczych pełnego ryzyka finansowego związanego z wykorzystaniem portfela w procesach autoryzacji transakcji.

W związku z powyższym konieczne jest doprecyzowanie przepisów projektu ustawy w taki sposób, aby jednoznacznie określały relację pomiędzy europejskim portfelem tożsamości cyfrowej a obowiązkami dostawców usług płatniczych w zakresie stosowania silnego uwierzytelnienia użytkownika, a także aby wskazywały zasady odpowiedzialności w przypadku nieautoryzowanego wykorzystania portfela.

6) Transgraniczne uznawanie europejskich portfeli tożsamości cyfrowej - konieczność doprecyzowania zasad stosowania

Mając na względzie wcześniejsze komentarze wnosimy o doprecyzowanie przepisów projektu ustawy w zakresie zasad uznawania europejskich portfeli tożsamości cyfrowej wydawanych przez inne państwa członkowskie UE. W szczególności konieczne jest określenie, w jaki sposób prywatne strony ufające, w tym instytucje finansowe, powinny w praktyce realizować obowiązek uznawania takich portfeli oraz jak mechanizm ten ma funkcjonować w procesach identyfikacji klientów.

Uzasadnienie

Projekt ustawy nie określa jednoznacznie zasad uznawania portfeli zapewnianych przez inne państwa członkowskie. Jednocześnie projektowany art. 22a ustawy o usługach zaufania oraz identyfikacji elektronicznej odnosi się do mechanizmu dopasowywania tożsamości w kontekście art. 11a ust. 1 rozporządzenia eIDAS, który zobowiązuje państwa członkowskie do zapewnienia możliwości jednoznacznego dopasowania tożsamości w usługach transgranicznych.

Przepisy powinny zatem w sposób jasny określać, jak w praktyce ma funkcjonować akceptacja portfeli wydawanych w innych państwach członkowskich, tak aby prywatne strony ufające mogły realizować swoje obowiązki w sposób zgodny z przepisami krajowymi, w szczególności w zakresie przeciwdziałania praniu pieniędzy i finansowaniu terroryzmu (AML/CFT).

7) Portfel dla osób prawnych - wątpliwości co do zakresu podmiotowego regulacji

Należy doprecyzować przepisy projektu ustawy w zakresie podmiotów uprawnionych do założenia europejskiego portfela tożsamości cyfrowej, tak aby jednoznacznie określić, czy możliwość ta obejmuje wyłącznie osoby prawne w rozumieniu prawa cywilnego, czy również jednostki organizacyjne nieposiadające osobowości prawnej, które uczestniczą w obrocie gospodarczym.

Uzasadnienie

Projekt ustawy w kilku miejscach posługuje się pojęciem „osoby prawnej” jako podmiotu uprawnionego do założenia portfela, w szczególności w art. 14c. Tymczasem w prawie polskim pojęcie osoby prawnej ma ściśle określone znaczenie normatywne wynikające z art. 33 kodeksu cywilnego. Zgodnie z tym przepisem osobami prawnymi są Skarb Państwa oraz jednostki organizacyjne, którym przepisy szczególne przyznają osobowość prawną.

W konsekwencji podmiotami tymi nie są m.in. spółki jawne, komandytowe czy partnerskie, które - choć uczestniczą w obrocie gospodarczym – nie posiadają osobowości prawnej i są określane w doktrynie jako jednostki organizacyjne nieposiadające osobowości prawnej.

Na tym tle pojawia się wątpliwość, czy podmioty tego rodzaju będą uprawnione do korzystania z portfela. Wątpliwość ta jest tym bardziej istotna, że w innym miejscu projektu ustawy (art. 14f ust. 1) ustawodawca posługuje się wprost pojęciem „jednostki organizacyjnej nieposiadającej osobowości prawnej”. Oznacza to, że projekt rozróżnia te kategorie podmiotów, jednak w kontekście możliwości założenia portfela odnosi się wyłącznie do osób prawnych.

W praktyce mogłoby to prowadzić do sytuacji, w której część podmiotów funkcjonujących w obrocie gospodarczym – takich jak spółki osobowe – nie miałaby możliwości korzystania z portfela. Taka interpretacja byłaby trudna do pogodzenia z założeniami rozporządzenia eIDAS, które nakazuje interpretować pojęcie osoby prawnej w sposób autonomiczny, obejmujący wszystkie podmioty uczestniczące w obrocie prawnym, które nie są osobami fizycznymi (motyw 68 rozporządzenia eIDAS).

W związku z powyższym zasadne jest rozważenie doprecyzowania przepisów projektu ustawy w taki sposób, aby jednoznacznie określić zakres podmiotów uprawnionych do zakładania europejskiego portfela tożsamości cyfrowej i uniknąć wątpliwości interpretacyjnych w tym zakresie.

8) Dodatkowe punktowe uwagi

1. Dane dotyczące osoby małoletniej oraz zakres umocowania opiekuna

Należy rozważyć rozszerzenie funkcjonalności portfela o możliwość przekazywania stronie ufającej danych identyfikujących osobę małoletnią przez osobę posiadającą wobec niej odpowiednie prawa, w zakresie zbliżonym do identyfikacji osoby pełnoletniej. Zasadne byłoby również umożliwienie przekazywania informacji o zakresie uprawnień przedstawiciela ustawowego wobec małoletniego, w tym ewentualnych ograniczeniach dotyczących dysponowania majątkiem dziecka. Dodatkowo warto rozważyć utworzenie wiarygodnego źródła lub rejestru pozwalającego na weryfikację tych uprawnień oraz doprecyzowanie zasad dostępu osób małoletnich do ich własnych europejskich portfeli tożsamości cyfrowej. Ma to istotne znaczenie z perspektywy ochrony małoletnich przed nadużyciami oraz prawidłowej weryfikacji umocowania opiekunów przez banki.

2. „Dokonywanie płatności elektronicznych” jako funkcja portfela

Projekt przewiduje możliwość udostępniania w portfelu usług polegających na „dokonywaniu płatności elektronicznych”, choć rozporządzenie eIDAS nie przewiduje takiej funkcjonalności.

W tym zakresie projekt wykracza zatem poza ramy niezbędnej implementacji eIDAS. Zasadne jest doprecyzowanie, że korzystanie z takich usług przez strony ufające i inne podmioty ma charakter dobrowolny, o ile obowiązek taki nie wynika z przepisów szczególnych.

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".

3. Relacja nowego portfela do dotychczasowych usług aplikacji mObywatel

Projekt nie określa jednoznacznie, na jakich zasadach miałoby dojść do wygaszenia lub dalszego funkcjonowania dotychczasowych usług aplikacji mObywatel, w tym dokumentu mObywatel, który banki są obecnie zobowiązane honorować jako narzędzie identyfikacji i weryfikacji tożsamości na podstawie art. 83 obowiązującej ustawy o aplikacji mObywatel. Wskazane jest doprecyzowanie tej relacji, tak aby nie powstawały wątpliwości co do dalszego obowiązywania obecnych obowiązków.

4. Zmienność wymogów technicznych wynikających z aktów wykonawczych UE

Projekt przewiduje wejście w życie głównych przepisów z dniem 24 grudnia 2026 r., podczas gdy część wymogów technicznych zależy od aktów wykonawczych Komisji Europejskiej, które nadal mogą ulegać zmianom albo nie zostały jeszcze ostatecznie przyjęte. Może to prowadzić do sytuacji, w której podmioty rynkowe poniosą koszty dostosowania do aktualnego stanu regulacyjnego, a następnie będą zmuszone do ponownych inwestycji. Zasadne byłoby rozważenie wprowadzenia mechanizmu umożliwiającego elastyczne dostosowywanie wymogów technicznych na poziomie wykonawczym, bez konieczności każdorazowej nowelizacji ustawy.

5. Informowanie stron ufających o incydentach bezpieczeństwa portfela

Projekt nakłada na ministra właściwego do spraw informatyzacji obowiązek informowania użytkowników portfela o naruszeniach bezpieczeństwa, nie reguluje jednak sposobu i terminów przekazywania takich informacji stronom ufającym, w tym bankom. Brak takiej regulacji może

istotnie utrudnić reakcję na incydenty bezpieczeństwa, zwłaszcza w przypadku naruszeń o charakterze masowym. Wskazane byłoby doprecyzowanie zasad niezwłocznego informowania właściwych organów nadzorczych oraz instytucji korzystających z portfela o incydentach mogących mieć wpływ na bezpieczeństwo procesów uwierzytelniania.

6. Odpowiedzialność za błędne dopasowanie tożsamości do rejestru PESEL

Projektowany art. 22a reguluje system scentralizowanego dopasowywania tożsamości do rejestru PESEL, nie określa jednak skutków błędnego dopasowania danych, w szczególności w przypadku tzw. false positive. Brak regulacji w tym zakresie rodzi ryzyka praktyczne dla stron ufających, które mogą podjąć decyzję na podstawie nieprawidłowo przypisanej tożsamości. Wymaga doprecyzowania kwestia odpowiedzialności za błędne wyniki systemu oraz ewentualnego trybu dochodzenia roszczeń przez podmioty, które poniosą z tego tytułu szkodę.

7. Bank jako punkt potwierdzający tożsamość

Projekt w art. 14b przewiduje możliwość pełnienia przez bank roli punktu potwierdzającego tożsamość użytkownika portfela na poziomie bezpieczeństwa wysokim, nie określając jednak modelu finansowania tej funkcji ani zasad odpowiedzialności za ewentualne błędy w procesie potwierdzania tożsamości. Z uwagi na koszty organizacyjne, techniczne i prawne związane z realizacją tej funkcji zasadne jest doprecyzowanie zasad finansowania oraz zakresu odpowiedzialności podmiotów uczestniczących w tym modelu. Brak regulacji tych elementów powoduje, że rola ta - choć formalnie fakultatywna - jest nieprzewidywalna finansowo i prawnie.

8. Właściwość organów nadzoru wobec stron ufających z sektora finansowego

Projekt wskazuje ministra właściwego do spraw informatyzacji jako organ nadzoru nad usługodawcami zaufania i dostawcami portfela, nie rozstrzyga jednak jednoznacznie, który organ byłby właściwy wobec banków działających jako strony ufające. Wskazane jest doprecyzowanie kompetencji poszczególnych organów, w szczególności KNF, UODO oraz ministra właściwego do spraw informatyzacji, tak aby zapewnić przejrzystość systemu nadzorczego.

9. Bezpieczeństwo wdrożenia a dostępność rozwiązania

Postulowane zwiększenie poziomu bezpieczeństwa, np. poprzez wykorzystanie NFC, elektronicznej warstwy dowodu osobistego czy kodu PIN, należy ocenić pozytywnie z perspektywy ograniczania ryzyk nadużyć. Jednocześnie należy uwzględnić, że bardziej rygorystyczne wymagania mogą ograniczyć dostępność rozwiązania dla części użytkowników, w szczególności osób starszych i osób zagrożonych wykluczeniem cyfrowym. Dodatkowo brak docelowej architektury rozwiązania utrudnia obecnie ocenę szczegółowych wymagań wdrożeniowych po stronie banków i dostosowanie aplikacji bankowych do nowej wersji mObywatela oraz innych europejskich portfeli tożsamości cyfrowej.

10. Brak ścieżki odwoławczej od odmowy wpisu do rejestru

W projektowanym art. 22b ust. 10 wpis do rejestru został określony jako czynność materialno-techniczna, przy czym projekt nie przewiduje ścieżki odwoławczej od odmowy dokonania wpisu. Zasadne jest rozważenie uzupełnienia regulacji w tym zakresie w celu zapewnienia przejrzystości proceduralnej i gwarancji ochrony praw podmiotów zainteresowanych wpisem.

11. Brak ścieżki odwoławczej od odmowy wydania elektronicznego poświadczenia atrybutów

Analogicznie, projekt nie określa trybu odwoławczego w przypadku odmowy wydania elektronicznego poświadczenia atrybutów. Wskazane byłoby doprecyzowanie tej kwestii, tak aby zapewnić podmiotom ubiegającym się o wydanie poświadczenia odpowiednie gwarancje proceduralne.

12. Uwagi redakcyjne i techniczne do projektu

W projekcie dostrzeżono również kilka kwestii o charakterze redakcyjnym i technicznym, które wymagają korekty.

- art. 6 pkt 2 ustawy nowelizującej wskazuje, że *„po art. 14 dodaje się art. 14a-14j w brzmieniu:”*. Nie znaleziono w projekcie art. 14i oraz 14j;

- w art. 6 po pkt 2 jest od razu pkt 5, nie znaleziono pkt 3 i 4;

- w art. 11 pkt 4 ustawy nowelizującej zawarto, jak się wydaje, błędne odwołanie do art. 6 pkt 5.;

- w art. 1 pkt 9 projektu ustawy (dodawany art. 22a ust. 2 pkt 2) występuje błędne odesłanie. Czy planowana jest jego korekta na etapie dalszych prac legislacyjnych?;

- w art. 6 pkt 2 projektu ustawy występuje nieprawidłowe wprowadzenie przepisów (dodaje się przepisy 14a–j), podczas gdy faktycznie projekt obejmuje przepisy 14a–h. Czy planowana jest korekta tej numeracji?;

- w art. 6 pkt 2 projektu ustawy występuje również błędna numeracja punktów (po punkcie 2 następuje punkt 5). Czy zostanie ona skorygowana w dalszym procesie legislacyjnym?.

Pytania interpretacyjne do projektu ustawy o zmianie ustawy o usługach zaufania oraz identyfikacji elektronicznej oraz niektórych innych ustaw (projekt z wykazu prac legislacyjnych Rady Ministrów – nr UC122)

I. Interpretacja przepisów dotyczących identyfikacji i weryfikacji tożsamości (art. 14d)

1. Jaka była intencja ustawodawcy przy formułowaniu art. 14d ustawy z dnia 26 maja 2023 r. o aplikacji mObywatel, w szczególności poprzez dodanie sformułowania „podczas wzajemnej fizycznej obecności stron"? Warto wskazać, że podobne sformułowanie pojawia się również w art. 2 pkt 8 tej ustawy i pozwala na wykorzystanie mDowodu w procesie identyfikacji i weryfikacji tożsamości wyłącznie w kontaktach bezpośrednich bank–klient, co ogranicza weryfikację tożsamości w oparciu o mDowód w trybie online.
2. Czy identyfikacja w oparciu o portfel tożsamości cyfrowej lub dane identyfikujące osobę fizyczną zawarte w portfelu ma całkowicie zastępować identyfikację dokonywaną na podstawie dowodu osobistego lub paszportu? Czy w praktyce okazanie portfela zwalnia z obowiązku wglądu w fizyczny dowód osobisty lub paszport?
3. W jakim zakresie bank jest zobligowany do stosowania portfela w procesach związanych z weryfikacją tożsamości? Czy obowiązek ten dotyczy wyłącznie ustalenia danych klienta i weryfikacji jego tożsamości, czy również całego procesu onboardingu, w tym przyjęcia wniosku o otwarcie produktu bankowego oraz podpisania umowy o produkt bankowy?
4. W odniesieniu do art. 14d ust. 1 ustawy prosimy o potwierdzenie, czy podmiot korzystający z portfela w celu identyfikacji osoby będzie musiał być zarejestrowany jako strona ufająca oraz zintegrowany z całym ekosystemem portfela, czy też przewidziany będzie uproszczony tryb korzystania z portfela.

II. Relacja portfela cyfrowego do wymogów AML i dokumentów tożsamości

5. W portfelu cyfrowym nie będą dostępne dane takie jak seria i numer dowodu osobistego oraz data jego ważności. Tymczasem banki są zobowiązane ustawą AML do ustalenia tych danych. Czy identyfikacja na podstawie portfela zwalniałaby bank z obowiązku ustalenia danych dokumentu tożsamości?
6. Czy zastosowanie portfela podczas weryfikacji tożsamości oznacza, że bank nie musi ustalać i weryfikować danych dokumentu tożsamości, tj. dowodu osobistego lub paszportu?
7. W uzasadnieniu do ustawy wskazano, że zestaw metadanych odnoszących się do wydawanego zestawu danych identyfikujących osobę obejmuje trzy elementy obowiązkowe (wynikające z rozporządzenia 2024/2977) oraz jeden opcjonalny:
    - datę i godzinę wygaśnięcia ważności danych identyfikujących osobę,
    - nazwę organu wydającego dane identyfikujące osobę (w przypadku portfela zapewnianego przez ministra właściwego ds. informatyzacji – ten minister),
    - dwuznakowy kod ISO 3166-1 dla RP,

- numer danych identyfikujących osobę nadany przez dostawcę danych identyfikujących osobę (element opcjonalny).

W praktyce numer danych identyfikujących osobę może pełnić funkcję zbliżoną do numeru dokumentu mObywatel nadawanego po ustaleniu tożsamości użytkownika. Czy można interpretować to w ten sposób, że numer danych identyfikujących osobę miałby być odpowiednikiem serii i numeru dokumentu tożsamości w rozumieniu art. 36 ustawy AML?

8. W odniesieniu do art. 6 ust. 4 pkt 4 projektu ustawy oraz uzasadnienia (str. 28), gdzie wskazano, że jedną z metadanych dotyczących zestawu danych identyfikujących osobę będzie numer danych identyfikujących o znaczeniu podobnym do numeru dokumentu mObywatel:
a) czy numer ten powinien być traktowany jak numer dokumentu tożsamości i tym samym być rejestrowany w systemach bankowych analogicznie jak inne dokumenty tożsamości;
b) czy będzie istniała możliwość jego zastrzeżenia lub odwołania (w odniesieniu do pojęcia „unieważnienia" użytego w ustawie) w aplikacji portfela.

9. W jaki sposób banki miałyby dochować obowiązku zapewnienia dowodu audytowego (wynikającego z regulacji AML) z przeprowadzonej identyfikacji osoby z wykorzystaniem portfela, biorąc pod uwagę brak informacji dotyczących rejestrów logów po stronie stron ufających? Czy w praktyce konieczne będzie tworzenie własnego dokumentu potwierdzającego identyfikację, analogicznie jak w przypadku wykorzystania aplikacji mObywatel?

10. W jaki sposób bank powinien postępować w przypadku rozbieżności pomiędzy danymi pozyskanymi z portfela a danymi znajdującymi się w jego własnych bazach KYC?

III. Funkcjonowanie portfela tożsamości cyfrowej i jego architektura

11. Dotychczasowe rozmowy dotyczące eIDAS 2 wskazywały, że portfel będzie środkiem identyfikacji elektronicznej funkcjonującym niezależnie od Węzła Krajowego. Czy prawidłowo rozumiemy, że według aktualnej ustawy portfel ostatecznie będzie osadzony w Węźle Krajowym, a strony ufające będą musiały do Węzła przystąpić, aby móc z niego korzystać?

12. Czy jeden użytkownik na jednym urządzeniu będzie mógł mieć zainstalowaną zarówno aplikację mObywatel, jak i portfel tożsamości cyfrowej? Czy jeden użytkownik będzie mógł posiadać kilka portfeli tożsamości cyfrowej, np. w konfiguracji polski portfel oraz portfel wydany w innym państwie?

13. W uzasadnieniu do projektu ustawy (str. 20–21) wskazano, że cyfrowy portfel będzie zapewniany w węźle krajowym. Czy wykorzystanie portfela jako środka uwierzytelniającego użytkownika za pośrednictwem węzła krajowego oraz w zakresie danych jak obecnie będzie wymagało rejestracji podmiotu jako strony ufającej, czy też stroną ufającą będzie wyłącznie minister właściwy do spraw informatyzacji?

14. W jaki sposób w przyszłości będzie można zastrzec numer PESEL w sytuacji, gdy eDowód nie ma być przeniesiony do portfela, a aplikacja mObywatel ma zostać docelowo wycofana?

15. Czy przepis dotyczący równoważności dokumentu publicznego z atrybutem oznacza obowiązek dla banków przyjmowania atrybutów pochodzących z portfela?

16. Czy prawidłowe jest rozumienie, że w obowiązujących przepisach nie ma ogólnego obowiązku uznawania portfela w innych procesach niż SCA i w szczególności brak jest odpowiednika art. 83 ustawy o aplikacji mObywatel?

17. Czy bank może odmówić akceptacji portfela do czasu uzyskania certyfikacji EUDIW, a jeśli tak – przez jaki maksymalny okres?

IV. Podpis kwalifikowany w portfelu i kwestie podpisów elektronicznych

18. W odniesieniu do art. 14e ust. 1 oraz art. 14f ust. 1 i 2, a także do uzasadnienia do projektu ustawy (str. 33–35), prosimy o doprecyzowanie zasad dotyczących bezpłatnego podpisu kwalifikowanego w portfelu, w szczególności:
a) w jaki sposób zostanie zdefiniowane wykorzystanie podpisu do celów nieprofesjonalnych, biorąc pod uwagę, że w projekcie ustawy wskazano zamiar określenia zakresu czynności profesjonalnych oraz czynności innych niż profesjonalne;
b) czy oznaczenie podpisu jako użytego w celach innych niż profesjonalne daje stronie ufającej jakiekolwiek możliwości odmowy przyjęcia lub zakwestionowania dokumentu podpisanego z wykorzystaniem tego podpisu oraz czy planowane jest wzmocnienie przepisów poprzez jednoznaczne wskazanie odpowiedzialności użytkownika za wykorzystanie rozwiązania.

19. W odniesieniu do art. 6 pkt 2 projektu ustawy (dodawany art. 14f) prosimy o doprecyzowanie, czy w rozumieniu ministerstwa podpis kwalifikowany wykorzystywany do celów prywatnych obejmuje również podpisywanie umów z bankiem przez osoby fizyczne nieprowadzące działalności gospodarczej.

20. Czy stosowanie mechanizmu silnego uwierzytelniania klienta (SCA) w przypadku osoby prawnej będzie wymagało użycia portfela osoby prawnej czy portfela osoby fizycznej działającej w imieniu tej osoby prawnej?

V. Ochrona danych osobowych i zgłoszenia do UODO

21. W uzasadnieniu do projektu ustawy (str. 11) wskazano możliwość zgłaszania przez użytkowników portfela nadużyć w zakresie ochrony danych osobowych bezpośrednio do organu ochrony danych osobowych. Czy przewidywana jest analiza potencjalnych skutków takiego rozwiązania, w szczególności:
a) ryzyka masowego napływu zgłoszeń do organu nadzorczego;
b) ryzyka mechanicznego akceptowania zgłoszeń przez użytkowników w sposób analogiczny do zgód na cookies;
c) potrzeby prowadzenia działań edukacyjnych wśród obywateli dotyczących znaczenia takich zgłoszeń.

22. W uzasadnieniu projektu ustawy (str. 11 akapit 2 oraz str. 25 akapit 2) opisano możliwość zgłaszania naruszeń do UODO bezpośrednio z poziomu aplikacji. W jaki sposób zostanie zaprojektowana ta usługa? Czy planowane jest wprowadzenie formularza wymagającego opisania problemu, czy też będzie to rozwiązanie w postaci uproszczonego „przycisku" do zgłoszenia skargi?

23. W uzasadnieniu projektu ustawy wskazano, że użytkownik portfela będzie mógł powiadomić organ ochrony danych o każdym nieuzasadnionym żądaniu danych przez stronę ufającą. W jaki sposób ma wyglądać takie powiadomienie kierowane do UODO oraz jakie skutki prawne będzie ono wywoływało?

VI. Proces legislacyjny, błędy redakcyjne i harmonogram regulacji

24. Od kiedy przepis art. 14d ustawy z dnia 26 maja 2023 r. o aplikacji mObywatel ma obowiązywać w praktyce? Czy banki będą zobowiązane do jego stosowania od końca 2026 r., czy dopiero od końca 2027 r.?

25. Dlaczego w ocenie skutków regulacji (OSR) nie została przedstawiona analiza kosztów wdrożenia nowych rozwiązań dla sektora prywatnego, w tym dla banków?

26. Jakie sankcje grożą bankowi, który nie zarejestruje się w rejestrze stron ufających w terminie wynikającym z art. 5f rozporządzenia eIDAS 2.0?

27. Art. 14h ustawy przewiduje wydanie przez Radę Ministrów rozporządzenia określającego zakres danych oraz wykaz rejestrów publicznych i systemów teleinformatycznych. Do kiedy planowane jest wydanie tego rozporządzenia?

28. W art. 14a ust. 2 pkt 4 wskazano, że europejski portfel tożsamości cyfrowej zawiera dane obejmujące miejsce urodzenia. W jakim formacie będzie zapisywana ta informacja - czy będzie to wyłącznie kraj, czy również miejscowość?

29. W art. 14b ust. 3 wskazano, że minister właściwy do spraw informatyzacji określi w drodze rozporządzenia wymagania dotyczące weryfikacji tożsamości. Do kiedy planowane jest wydanie tego rozporządzenia?