Szanowna Pani,

poniżej moje uwagi do projektu ustawy:

1. Niespójne daty ustawy o aplikacji mObywatel - w art. 22g ust. 1 pojawia się „ustawa z dnia 26 maja 2026 r. o aplikacji mObywatel”, a w innych miejscach jest „ustawa z dnia 26 maja 2023 r.”.

   Propozycja: ujednolicić do jednej poprawnej daty (w projekcie ustawy konsekwentnie używana jest data 26 maja 2023 r.);

2. Błędne odesłanie w art. 14f ust. 1 który definiuje „cel inny niż profesjonalny”, ale odwołuje się do art. 22e ust. 1, który dotyczy wniosków do katalogów KE, a nie podpisów w portfelu. To wygląda jak pomyłka numeracji - aczkolwiek może to celowy zamysł, stwierdziłam jednak, że lepiej to wskazać aby zmitygować ewentualne ryzyko "pustego" zapisu;
3. Niespójność w art. 14b ust. 2 (odesłanie do nieistniejącej litery) - w art. 14b ust. 2 jest: „punkt potwierdzający tożsamość, o którym mowa w ust. 1 pkt 2 lit. b”, ale w ust. 1 pkt 2 nie ma lit. b (pkt 2 to profil zaufany z dodatkową weryfikacją; litery nie występują);
4. W projekcie ustawy pojawia się dużo błędów językowych:

   - formy typu „europejski portfela” zamiast „europejski portfel” w art. 14a ust. 1, art. 14a ust. 7 pkt 1, art. 14a ust. 7 pkt 2, art. 14c ust. 1 pkt 1 + art. Art. 14c ust. w którym to nie ma błędu gramatycznego, ale jest niespójność stylistyczna — w innych miejscach mowa o „unieważnieniu danych w portfelu”, a tu „unieważnienie portfela osoby prawnej”. Warto ujednolicić pojęcia (portfel vs instancja vs dane) + w art. 14d ust. 1 jest błąd językowy i powinno być: „…jakie zawiera europejski portfel tożsamości cyfrowej…”

   -powtórzenia, „kopiuj-wklej” i błędy redakcyjne w art. 20ac ust. 2 pkt 1 lit. f podwójnie jest "dodaje się", w art. 14e ust. 12 pkt 4 jest zbędna kropka po średniku, w art. 1 pkt 6 lit. b (ustawa o mObywatel) występuje przecinek przed średnikiem

5. W rozdziale o atrybutach projekt bazuje na pojęciach z eIDAS, ale nie dopina praktycznie, kto w Polsce jest „odpowiedzialny” i jak przebiega delegowanie/porozumienia, zwłaszcza przy art. 22f–22h (wydawanie poświadczeń „w imieniu”)

   Propozycja dopisku (norma porządkująca relacje i odpowiedzialność): Dodać przepis w okolicach art. 22f–22h: „*Minister właściwy do spraw informatyzacji wydaje elektroniczne poświadczenia atrybutów w imieniu podmiotu odpowiedzialnego za źródło autentyczne wyłącznie na podstawie porozumienia określającego co najmniej: zakres atrybutów, podstawę prawną udostępniania danych, role administratora/podmiotu przetwarzającego (RODO), zasady odpowiedzialności, okresy retencji, tryb audytu i zasady reagowania na incydenty.*”

6. Rejestr stron ufających: wpis jest „czynnością materialno-techniczną” (art. 22b ust. 10), a w razie braków minister „zwraca wniosek (...) a wniosek nie podlega rozpoznaniu” (ust. 11). Ryzyko: w praktyce podmiot może zostać „zablokowany” bez formalnej decyzji, czyli bez klasycznej drogi odwoławczej. To często jest kwestionowane (prawo do zaskarżenia rozstrzygnięcia organu).

   Propozycja:

   a) Zostawić materialno-techniczną formę wpisu, ale odmowę ująć jako decyzję np. „*W przypadku stwierdzenia braków lub niezgodności danych, minister wzywa do usunięcia braków w terminie 7 dni. Po bezskutecznym upływie terminu minister odmawia wpisu (albo zmiany wpisu) w drodze decyzji administracyjnej.*”;

   b) Alternatywnie: utrzymać „zwrot”, ale np. dodać: „*Na czynności, o których mowa w ust. 11, przysługuje skarga do sądu administracyjnego.*”

7. W art. 10h ust. 2–3 (doręczenia elektroniczne) jest decyzja o cofnięciu dostępu „w przypadku wystąpienia ryzyka naruszenia bezpieczeństwa” i „podlega natychmiastowemu wykonaniu”. Ryzyko: pojęcie „ryzyka” jest nieostre, nie ma minimalnych przesłanek, stopniowania, czasu obowiązywania, ani trybu przywrócenia dostępu (a to realnie wpływa na działanie systemów). Należałoby to doprecyzować.
8. Art. 21aa daje użytkownikom wgląd w historię użycia (logi), i umożliwia pobranie dokumentu z PESEL i danymi użycia. **Ryzyko:** projekt nie mówi jak długo logi są przechowywane, czy obejmują np. identyfikatory sesji, IP, urządzenia, czy użytkownik może żądać sprostowania / ograniczenia oraz jak chroni się przed „ujawnieniem zbyt dużo” (np. w razie przejęcia konta).

   Propozycja dopisku: dodać ust. 5–7 w art. 21aa np.„*5. Dzienniki systemowe, o których mowa w ust. 1, obejmują wyłącznie dane niezbędne do zapewnienia rozliczalności i bezpieczeństwa uwierzytelnienia. 6. Okres przechowywania dzienników systemowych wynosi ... (np. 24 miesiące), chyba że dłuższe przechowywanie jest niezbędne dla celów postępowań wyjaśniających, bezpieczeństwa lub roszczeń.*
   7. Udostępnienie historii użycia wymaga zastosowania uwierzytelnienia wieloskładnikowego oraz mechanizmów ograniczających ryzyko nieuprawnionego dostępu.”

9. Art. 10a ust. 3 przewiduje ogromny katalog danych o podmiotach i osobach (kierujący, reprezentanci, administratorzy kont, telefony służbowe, maile, PESEL). Ryzyko: bez precyzyjnej polityki dostępu i rozdzielenia: „co jest publiczne”, „co jest dostępne tylko uprawnionym”, „co przez API”, można wejść w konflikt z zasadą minimalizacji oraz bezpieczeństwa (bo to jest w praktyce „super-rejestr” o wysokiej wartości dla atakujących).

   Propozycja dopisku: dodać w rozdziale o KPP (np. po art. 10a): „*Dane osobowe przetwarzane w KPP udostępnia się wyłącznie w zakresie niezbędnym do realizacji zadań publicznych oraz zapewnienia komunikacji i doręczeń elektronicznych. Minister określa poziomy dostępu do danych (publiczny / ograniczony / administracyjny) oraz*

zakres danych dostępnych przez interfejsy API, kierując się zasadą minimalizacji danych i bezpieczeństwa."

10. Art. 23 pkt 2 przewiduje, że minister po opiniach CSIRT udostępnia kod źródłowy „poszczególnych komponentów oprogramowania" portfela. Ryzyko: nie wiadomo, czy to udostępnienie jest publiczne, czy ograniczone, nie wiadomo, co z prawami autorskimi / licencją, nie wiadomo, czy są wyłączone elementy krytyczne (np. klucze, konfiguracje, mechanizmy antyfraud) oraz brak trybu i kryteriów zakresu.

    Propozycja doprecyzowania: dodać po pkt 2 zdanie/punkt: „*Udostępnienie kodu źródłowego nie obejmuje informacji, których ujawnienie mogłoby zagrozić bezpieczeństwu portfela, bezpieczeństwu państwa lub ciągłości świadczenia usług, w szczególności danych konfiguracyjnych, mechanizmów ochrony przed nadużyciami oraz komponentów zawierających informacje niejawne. Minister określa warunki licencji i tryb udostępniania*."

Pozdrawiam,