PREZES
URZĘDU OCHRONY
DANYCH OSOBOWYCH

Mirosław Wróblewski

Warszawa, 25-03-2026

DPNT.401.60.2026.WL.PM

Pan
Dariusz Standerski
Sekretarz Stanu
w Ministerstwie Cyfryzacji

Szanowny Panie Ministrze,

w odpowiedzi na pismo z 18 lutego 2026 r. znak: DP.MC.WLA.0211.35.2025, działając na podstawie art. 57 ust. 1 lit. c rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679[1] oraz art. 51 ustawy o ochronie danych osobowych[2], uprzejmie informuję, że do przedstawionego projektu **ustawy o zmianie ustawy o usługach zaufania oraz identyfikacji elektronicznej oraz niektórych innych ustaw (UC122)**, Prezes Urzędu Ochrony Danych Osobowych jako organ nadzorczy zgłasza następujące uwagi.

Uwagi ogólne i test prywatności

Projektowana ustawa dostosowująca polski porządek prawny do zmian wynikających z 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 (Dz. Urz. UE L 2024/1183 z 30.04.2024), dalej: eIDAS2, **przewiduje szereg zasadniczych zmian w funkcjonującym w Polsce systemie identyfikacji elektronicznej**. Będzie to przede wszystkim wprowadzenie **europejskiego portfela tożsamości cyfrowej** i związanego z nim **modelu uwierzytelniania się na potrzeby usług świadczonych przez sieć Internet**. Projektowana ustawa wpłynie również na **funkcjonowanie rejestrów publicznych** w

[1] 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. Urz. UE L 119 z 4.5.2016, str. 1 ze zm.).
[2] Ustawa z dnia 10 maja 2018 r. o ochronie danych osobowych (Dz. U. z 2019 r. poz. 1781).

związku z koniecznością **dostosowania polskiego sytemu prawnego do eIDAS2**. Dotyczyć to będzie zmian w węźle krajowym i w połączonym z nim systemie scentralizowanym. Zostanie utworzony również nowy rejestr – Katalog Podmiotów Publicznych, w którym będzie gromadzony szereg informacji o podmiotach realizujących zadania publiczne realizujących usługi online. Projektowana ustawa wpłynie również na **funkcjonowanie i rozpowszechnienie użycia kwalifikowanego podpisu elektronicznego** poprzez udostępnienie tego narzędzia jako nieodpłatnego obywatelom do użytku nieprofesjonalnego.

Wprowadzanie takich rozwiązań – ze względu na rodzaj przetwarzania, w szczególności z użyciem nowych technologii, którego charakter, zakres, kontekst i cele z dużym prawdopodobieństwem mogą powodować wysokie ryzyko naruszenia praw lub wolności osób fizycznych – implikuje konieczność przeprowadzenia testu prywatności i **oceny skutków dla ochrony danych** już w ramach przyjmowania podstawy prawnej przetwarzania, odpowiadającej wymogom art. 25 ust. 1 [3] i art. 35 (w szczególności ust. 1 [4] i ust. 10)[5].

Przeprowadzenie oceny skutków dla ochrony danych ułatwia zbadanie ryzyk związanych z projektowanymi zmianami oraz wykazanie zgodności projektowanych rozwiązań z zasadami dotyczącymi przetwarzania danych osobowych wynikającymi z art.

[3] Uwzględniając stan wiedzy technicznej, koszt wdrażania oraz charakter, zakres, kontekst i cele przetwarzania oraz ryzyko naruszenia praw lub wolności osób fizycznych o różnym prawdopodobieństwie wystąpienia i wadze zagrożenia wynikające z przetwarzania, administrator – zarówno przy określaniu sposobów przetwarzania, jak i w czasie samego przetwarzania –wdraża odpowiednie środki techniczne i organizacyjne, takie jak pseudonimizacja, zaprojektowane w celu skutecznej realizacji zasad ochrony danych, takich jak minimalizacja danych, oraz w celu nadania przetwarzaniu niezbędnych zabezpieczeń, tak by spełnić wymogi niniejszego rozporządzenia oraz chronić prawa osób, których dane dotyczą.

[4] Jeżeli dany rodzaj przetwarzania – w szczególności z użyciem nowych technologii – ze względu na swój charakter, zakres, kontekst i cele z dużym prawdopodobieństwem może powodować wysokie ryzyko naruszenia praw lub wolności osób fizycznych, administrator przed rozpoczęciem przetwarzania dokonuje oceny skutków planowanych operacji przetwarzania dla ochrony danych osobowych. Dla podobnych operacji przetwarzania danych wiążących się z podobnym wysokim ryzykiem można przeprowadzić pojedynczą ocenę.

[5] Ust. 1–7 nie mają zastosowania, jeżeli przetwarzanie na mocy art. 6 ust. 1 lit. c) lub e) ma podstawę prawną w prawie Unii lub w prawie państwa członkowskiego, któremu podlega administrator, i prawo takie reguluje daną operację przetwarzania lub zestaw operacji, a oceny skutków dla ochrony danych dokonano już w ramach oceny skutków regulacji w związku z przyjęciem tej podstawy prawnej – chyba że państwa członkowskie uznają za niezbędne, by przed podjęciem czynności przetwarzania dokonać oceny skutków dla ochrony danych.

5 rozporządzenia 2016/679[6] oraz spełnienia warunków przetwarzania danych osobowych określonych w art. 6 ust. 3 tego rozporządzenia, a także pozwala ocenić czy rozwiązania zawarte w projekcie przewidują jednocześnie odpowiednie zabezpieczenia praw i wolności osób, których dane dotyczą.

Przetwarzanie danych osobowych na potrzeby *ratio legis* regulacji powinno być wyważone – istotą jest pogodzenie **celów regulacji**, a zwłaszcza **planowanych sposobów przetwarzania danych**, określonych projektowanymi przepisami, z **poszanowaniem praw osób**, których danych dotyczą, oraz **ochrony ich danych**. Kształt regulacji powinien zapewniać stosowanie następujących zasad dotyczących przetwarzania danych osobowych: a) zgodność z prawem, rzetelność i przejrzystość, b) ograniczenie celu, c) minimalizacja danych, d) prawidłowość, e) ograniczenie przechowywania, f) integralność i poufność oraz rozliczalność (art. 5 rozporządzenia 2016/679). Rolą prawodawcy, twórcy przepisów kierowanych do wykonawców norm, jest przyjęcie takich przepisów krajowych, które uwzględniać będą w swej treści te zasady. W poszczególnych uwagach wskazane zostaną poniżej te aspekty.

Prezes UODO z uznaniem przyjmuje **wprowadzenie szeregu zmian w funkcjonującym obecnie systemie identyfikacji elektronicznej**. Dotyczy to przede wszystkim wprowadzenia **nowych profili zaufanych** w postaci profilu identyfikującego i opisującego podmiot publiczny oraz profilu identyfikującego i opisującego osobę fizyczną reprezentującą podmiot publiczny, co ograniczy używanie „prywatnych" profili zaufanych do celów służbowych. Za korzystne należy uznać również **zapewnienie użytkownikom środków identyfikacji elektronicznej możliwości zapoznania się z historią ich użycia zapisaną w logach systemu,** jak również wdrożenie wynikającego z eIDAS2 rozwiązania pozwalającego na **selektywne udostępnianie dostawcom usług atrybutów, takich jak wiek i płeć bez podawania dodatkowych danych**.

Projektowana ustawa zawiera jednak również **szereg mankamentów**, które częściowo powielają rozwiązania wielokrotnie krytykowane przez organ nadzorczy w procesach legislacyjnych dotyczących ustaw, za które odpowiedzialny jest minister właściwy do spraw informatyzacji. Dotyczy to przede wszystkim rozwiązań **blankietowych**

[6] Art. 5 ust. 1. Dane osobowe muszą być: a) przetwarzane zgodnie z prawem, rzetelnie i w sposób przejrzysty dla osoby, której dane dotyczą ("zgodność z prawem, rzetelność i przejrzystość"); b) zbierane w konkretnych, wyraźnych i prawnie uzasadnionych celach i nieprzetwarzane dalej w sposób niezgodny z tymi celami; dalsze przetwarzanie do celów archiwalnych w interesie publicznym, do celów badań naukowych lub historycznych lub do celów statystycznych nie jest uznawane w myśl art. 89 ust. 1 za niezgodne z pierwotnymi celami ("ograniczenie celu"); c) adekwatne, stosowne oraz ograniczone do tego, co niezbędne do celów, w których są przetwarzane ("minimalizacja danych"); d) prawidłowe i w razie potrzeby uaktualniane; należy podjąć wszelkie rozsądne działania, aby dane osobowe, które są nieprawidłowe w świetle celów ich przetwarzania, zostały niezwłocznie usunięte lub sprostowane ("prawidłowość"); e) przechowywane w formie umożliwiającej identyfikację osoby, której dane dotyczą, przez okres nie dłuższy, niż jest to niezbędne do celów, w których dane te są przetwarzane; dane osobowe można przechowywać przez okres dłuższy, o ile będą one przetwarzane wyłącznie do celów archiwalnych w interesie publicznym, do celów badań naukowych lub historycznych lub do celów statystycznych na mocy art. 89 ust. 1, z zastrzeżeniem że wdrożone zostaną odpowiednie środki techniczne i organizacyjne wymagane na mocy niniejszego rozporządzenia w celu ochrony praw i wolności osób, których dane dotyczą ("ograniczenie przechowywania"); f) przetwarzane w sposób zapewniający odpowiednie bezpieczeństwo danych osobowych, w tym ochronę przed niedozwolonym lub niezgodnym z prawem przetwarzaniem oraz przypadkową utratą, zniszczeniem lub uszkodzeniem, za pomocą odpowiednich środków technicznych lub organizacyjnych ("integralność i poufność"). 2. Administrator jest odpowiedzialny za przestrzeganie przepisów ust. 1 i musi być w stanie wykazać ich przestrzeganie ("rozliczalność").

i cedowania niezgodnie z rozporządzeniem 2016/679 odpowiedzialności administratora na inne podmioty.

W ocenie organu nadzorczego projektowana ustawa **nie ogranicza również w odpowiedni sposób używania numeru PESEL**. Ponownie podkreślenia zatem wymaga, że państwa członkowskie mogą określić szczególne warunki przetwarzania krajowego numeru identyfikacyjnego lub innego identyfikatora o zasięgu ogólnym zgodnie z art. 87 rozporządzenia 2016/679. Krajowego numeru identyfikacyjnego lub innego identyfikatora o zasięgu ogólnym używa się wyłącznie z zachowaniem odpowiednich zabezpieczeń praw i wolności osoby, której dane dotyczą, wymaganych przepisami rozporządzenia 2016/679. Procedowanie projektowanej ustawy jest doskonałą okazją do **ograniczenia użycia numeru PESEL w ramach posługiwania się środkami identyfikacji elektronicznej** oraz do **wprowadzenia przepisów gwarancyjnych, o których mowa w art. 87 rozporządzenia 2016/679**. Ujawniony w wielu miejscach numer PESEL ułatwia kradzież tożsamości, jak również profilowanie osoby bez jej wiedzy i zgody. Motyw 75 rozporządzenia 2016/679[7] wskazuje skutki dla praw i wolności osób, które należy brać pod uwagę w związku z nieuprawnionym ujawnianiem danych osobowych. Na zagrożenia te wpływa unikalność numeru PESEL i szereg dodatkowych informacji jakie ta dana za sobą niesie, tj. wiek czy płeć osoby.

Uwagi Prezesa Urzędu Ochrony Danych Osobowych w znacznej części dotyczą tego aspektu projektu i wskazują projektodawcy jakie rozwiązania powinny zostać podjęte w celu zminimalizowania tych ryzyk. **Konieczne jest zatem ponowne przeanalizowanie koncepcji oparcia europejskiego portfela tożsamości cyfrowej na numerze PESEL, jako danej, która ostatecznie będzie potwierdzać tożsamość użytkownika.** Kwestia ta powinna zostać poddana poszerzonej analizie **w ocenie skutków dla ochrony danych, o której przeprowadzenie organ ochrony danych osobowych w tej sprawie apeluje**.

W ocenie skutków dla ochrony danych projektowanej ustawy powinna zostać również przeanalizowana oraz oceniona z punktu widzenia zasady zgodności z prawem, rzetelności i przejrzystości, ograniczenia celu, minimalizacji danych oraz rozliczalności:

1. możliwość zagwarantowania maksymalnego poziomu prywatności użytkowników europejskiego portfela tożsamości cyfrowej, zapewnianego przez ministra

[7] Ryzyko naruszenia praw lub wolności osób, o różnym prawdopodobieństwie i wadze, może wynikać z przetwarzania danych osobowych mogącego prowadzić do uszczerbku fizycznego lub szkód majątkowych lub niemajątkowych, w szczególności: jeżeli przetwarzanie może poskutkować dyskryminacją, kradzieżą tożsamości lub oszustwem dotyczącym tożsamości, stratą finansową, naruszeniem dobrego imienia, naruszeniem poufności danych osobowych chronionych tajemnicą zawodową, nieuprawnionym odwróceniem pseudonimizacji lub wszelką inną znaczną szkodą gospodarczą lub społeczną; jeżeli osoby, których dane dotyczą, mogą zostać pozbawione przysługujących im praw i wolności lub możliwości sprawowania kontroli nad swoimi danymi osobowymi; jeżeli przetwarzane są dane osobowe ujawniające pochodzenie rasowe lub etniczne, poglądy polityczne, wyznanie lub przekonania światopoglądowe, lub przynależność do związków zawodowych oraz jeżeli przetwarzane są dane genetyczne, dane dotyczące zdrowia lub dane dotyczące seksualności lub wyroków skazujących i czynów zabronionych lub związanych z tym środków bezpieczeństwa; jeżeli oceniane są czynniki osobowe, w szczególności analizowane lub prognozowane aspekty dotyczące efektów pracy, sytuacji ekonomicznej, zdrowia, osobistych preferencji lub zainteresowań, wiarygodności lub zachowania, lokalizacji lub przemieszczania się - w celu tworzenia lub wykorzystywania profili osobistych; lub jeżeli przetwarzane są dane osobowe osób wymagających szczególnej opieki, w szczególności dzieci; jeżeli przetwarzanie dotyczy dużej ilości danych osobowych i wpływa na dużą liczbę osób, których dane dotyczą.

właściwego do spraw informatyzacji, poprzez stworzenie **zestawu danych identyfikacyjnych, unikalnych dla tego portfela**,
2. **charakter i prawne umocowanie usług zapewnianych przez ministra właściwego do spraw informatyzacji**, w szczególności dotyczących zgłaszania naruszeń ochrony danych osobowych;
3. zakres regulacji dla zapewnienia **kompleksowego i wyczerpującego uregulowania w projektowanej ustawie kompetencji podmiotów publicznych i zasad udostępniania przez nie danych** na potrzeby funkcjonowania europejskiego portfela tożsamości cyfrowej oraz zasady weryfikacji tożsamości użytkowników europejskiego portfela tożsamości cyfrowej.

Kwestie te zostały szczegółowo omówione w poszczególnych uwagach do projektowanej ustawy.

Organ nadzorczy zwraca również uprzejmie uwagę, że **ocena skutków regulacji projektowanej ustawy nie wskazuje Prezesa UODO wśród podmiotów, na które oddziałuje projekt, nie zakłada się również żadnych dodatkowych środków finansowych i organizacyjnych dla organu nadzorczego w związku wdrożeniem usługi zgłaszania naruszeń z użyciem europejskiego portfela tożsamości cyfrowej zapewnianego przez ministra właściwego do spraw informatyzacji.**

Uwagi szczegółowe

I. Uwagi do zmian w ustawie z dnia 5 września 2016 r. o usługach zaufania oraz identyfikacji elektronicznej.

1. Zgodnie z **art. 1 pkt 5** projektu ustawy, wprowadzającym zmiany w **art. 21a** ustawy z dnia 5 września 2016 r. o usługach zaufania oraz identyfikacji elektronicznej (Dz. U. z 2024 r. poz. 1725), zostaje uchylony **ust. 6 w art. 21a** (art. 1 pkt 5 lit. b projektu), stanowiący dotychczasowy zamknięty katalog danych osobowych osób, którym wydano środki identyfikacji elektronicznej, przetwarzane przez ministra właściwego do spraw informatyzacji. W obecnym stanie prawnym są to: imię (imiona), nazwisko, nazwisko rodowe, numer PESEL lub niepowtarzalny identyfikator środka identyfikacji elektronicznej, o którym mowa w przepisach wydanych na podstawie art. 12 ust. 8 rozporządzenia 910/2014, data urodzenia, miejsce urodzenia, płeć oraz adres zamieszkania. Dodawany **art. 1 pkt 5** projektu ustawy **ust. 6a w art. 21a** odwołuje się natomiast do: „1) danych identyfikujących osobę, o których mowa w załączniku do rozporządzenia wykonawczego Komisji (UE) 2015/1501 z dnia 8 września 2015 r. w sprawie ram interoperacyjności na podstawie art. 12 ust. 8 rozporządzenia Parlamentu Europejskiego i Rady (UE) nr 910/2014 w sprawie identyfikacji elektronicznej i usług zaufania w odniesieniu do transakcji elektronicznych na rynku wewnętrznym (Dz. Urz. UE L z 2015 r. Nr 235, str. 1, z późn. zm.), zwanego dalej „rozporządzeniem 2015/1501”, 2) danych identyfikujących osobę, o których mowa w załączniku do rozporządzenia wykonawczego Komisji (UE) 2024/2977 z dnia 28 listopada 2024 r. w sprawie ustanowienia zasad stosowania

rozporządzenia Parlamentu Europejskiego i Rady (UE) nr 910/2014 w odniesieniu do danych identyfikujących osobę i elektronicznych poświadczeń atrybutów wydawanych europejskim portfelom tożsamości cyfrowej (Dz. Urz. UE L z 2024 r. poz. 2977), zwanego dalej „rozporządzeniem 2024/2977",3) imion rodziców osób oraz numeru dokumentu potwierdzającego tożsamość osób, o których mowa w pkt 1 i 2. – w celu uwierzytelnienia z wykorzystaniem węzła krajowego.".

Po pierwsze, zgodnie z załącznikiem do **rozporządzenia 2015/1501**, do którego odwołuje się **art. 21a ust. 6a pkt 1,** „minimalny zestaw danych dotyczących osoby fizycznej zawiera wszystkie poniższe elementy obowiązkowe: a) obecnie używane nazwisko lub nazwiska; b) obecnie używane imię lub imiona; c) data urodzenia; d) niepowtarzalny identyfikator zbudowany przez wysyłające państwo członkowskie zgodnie ze specyfikacjami technicznymi do celów transgranicznej identyfikacji, który jest możliwie jak najtrwalszy. Minimalny zestaw danych dotyczących osoby fizycznej może zawierać co najmniej jeden z następujących elementów dodatkowych: a) imię lub imiona oraz nazwisko lub nazwiska rodowe; b) miejsce urodzenia; c) aktualny adres; d) płeć.". Po drugie, załącznik do rozporządzenia 2015/1501 zawiera minimalny zestaw danych, dotyczących osoby fizycznej, jest to więc katalog otwarty. Są to też dane dotyczące osoby fizycznej, nie wszystkie muszą być uznane automatycznie za identyfikujące tą osobę, jak zakłada projektodawca w art. 21a ust. 6a pkt 1 (nie wskazując jednocześnie, które dane dotyczące osoby ją identyfikują). Kolejno, zgodnie z lit. d załącznika niepowtarzalny identyfikator zbudowany przez wysyłające państwo członkowskie będzie się pokrywał większości przypadków z numerem PESEL, nie wynika to natomiast jednoznacznie z projektowanych przepisów. Chociażby w przypadku kwalifikowanych podpisów elektronicznych zgodnie z załącznikiem I do rozporządzenia 910/2014 kwalifikowany certyfikat zawiera co najmniej imię i nazwisko podpisującego lub jego pseudonim; jeżeli używany jest pseudonim, fakt ten jest jasno wskazany oraz kod identyfikacyjny certyfikatu, który musi być niepowtarzalny dla kwalifikowanego dostawcy usług zaufania.". Kod identyfikacyjny certyfikatu może więc być oparty na innym numerze z rejestru publicznego niż numer PESEL, w tym numerze dowodu osobistego lub paszportu. W obecnym stanie prawnym zgodnie z **art. 21a ust. 6 pkt 4** ustawy o usługach zaufania oraz identyfikacji elektronicznej minister właściwy do spraw informatyzacji przetwarza „numer PESEL lub niepowtarzalny identyfikator środka identyfikacji elektronicznej, o którym mowa w przepisach wydanych na podstawie art. 12 ust. 8 rozporządzenia 910/2014". Przepisami wydanymi na podstawie art. 12 ust. 8 rozporządzenia 910/2014, jest właśnie rozporządzenie 2015/1501, zaś w proponowanym stanie prawnym nie wyodrębnia się wprost numeru PESEL jako danej innej niż niepowtarzalny identyfikator zbudowany przez wysyłające państwo członkowskie zgodnie ze specyfikacjami technicznymi do celów transgranicznej identyfikacji, który jest możliwie jak najtrwalszy.

Powstaje więc pytanie – mając na uwadze szeroko opisywane w uzasadnieniu do projektowanej ustawy zalety wykorzystania numeru PESEL do jednoznacznej identyfikacji osoby posługującej się środkami identyfikacji elektronicznej (o czym szerzej w uwagach do zmian wprowadzanych w ustawie o aplikacji mObywatel) – **czy taka konstrukcja projektowanego przepisu wpłynie na możliwość posługiwania się kwalifikowanymi podpisami elektronicznymi niezawierającymi numeru PESEL w certyfikacie**. W

ocenie organu nadzorczego oparcie się w projektowanym przepisie na ogólnym odesłaniu do rozporządzenia 2015/1501 wpływa na niejednoznaczność projektowanych rozwiązań, i co za tym idzie nieprzejrzystość katalogu danych, który projektodawca chce oprzeć na załączniku do rozporządzenia 2015/1501, zamiast jak jest to obecnie uregulowane w uchylanym art. 21a ust. 6 enumeratywnym katalogu danych.

W przypadku załącznika do **rozporządzenia 2024/2977,** do którego odwołuje projektodawca w **art. 21a ust. 6a pkt 2**, oprócz obowiązkowych danych identyfikujących osobę fizyczną: nazwiska, imion, daty urodzenia, miejsca urodzenia obywatelstwa (tabela 1), znajduje się szereg opcjonalnych danych identyfikujących osobę (tabela 2). Będzie to chociażby **numer telefonu, adres e-mail użytkownika oraz jego wizerunek twarzy**. **Powstaje pytanie o adekwatność przetwarzania tych danych w kontekście celu przetwarzania tj. dla „uwierzytelnienia z wykorzystaniem węzła krajowego" zadeklarowanego w projektowanym art. 21a ust. 6a część wspólna**. Węzeł krajowy w rozumieniu **art. 21a ust. 1** ustawy o usługach zaufania oraz identyfikacji elektronicznej (niezmienianego w tym zakresie projektowaną ustawą) jest definiowany w następujący sposób: „Krajowy schemat identyfikacji elektronicznej obejmuje: 1) węzeł krajowy identyfikacji elektronicznej, zwany dalej „węzłem krajowym"; 2) przyłączone do węzła krajowego: a) systemy identyfikacji elektronicznej, w których wydawane są środki identyfikacji elektronicznej, b) systemy teleinformatyczne, w których udostępniane są usługi online; 3) węzeł wykorzystywany w procesie transgranicznego uwierzytelniania osób, o którym mowa w przepisach wydanych na podstawie art. 12 ust. 8 rozporządzenia 910/2014, zwany dalej „węzłem transgranicznym".".

W ocenie organu nadzorczego **cały szereg opcjonalnych danych identyfikujących osobę, o których mowa w załączniku do rozporządzenia 2024/2977 nie będzie konieczny do uwierzytelnienia z wykorzystaniem węzła krajowego**, zaś w przypadku węzła transgranicznego uwierzytelnienie osób odbywa się w oparciu o przepisy wydane na podstawie art. 12 ust. 8 rozporządzenia 910/2014, czyli rozporządzenie 2015/1501, o którym mowa w art. 21a ust. 6a pkt 1 projektu ustawy, czyli w sposób odrębny.

Powstaje również pytanie w jaki sposób, w obecnie obowiązującym w Polsce stanie prawnym uwierzytelnienie w węźle krajowym ma się odbywać przy pomocy danej w postaci płci użytkownika definiowanej w tabeli 2 załącznika do rozporządzenia 2024/2977: „Dopuszcza się jedną z następujących wartości: 0 = nieznana; 1 = mężczyzna; 2 = kobieta; 3 = inna; 4 = osoba interseksualna; 5 = różnorodna; 6 = otwarta; 9 = nie dotyczy; W odniesieniu do wartości 0, 1, 2 i 9 stosuje się normę ISO/IEC 5218.".

W motywie 12 rozporządzenia 2024/2977 prawodawca przyjął, że: „W celu zagwarantowania, że dane identyfikujące osobę reprezentują użytkownika portfela w sposób niepowtarzalny, państwa członkowskie powinny – oprócz obowiązkowych atrybutów zbioru danych identyfikujących osobę określonych w niniejszym rozporządzeniu – zapewnić atrybuty opcjonalne niezbędne do zapewnienia niepowtarzalnego charakteru zbioru danych identyfikujących osobę.". To więc do państwa członkowskiego należy zapewnienie atrybutów niezbędnych do identyfikacji użytkownika, **konieczne jest więc dokonanie refleksji w tym kierunku ze strony projektodawcy i ustalenie katalogu**

tych danych w prawie krajowym. Jak wskazano dalej, **konieczne będzie również ustalenie katalogu dokumentów potwierdzających tożsamość.**

Jednocześnie w **art. 21a ust. 6a pkt 3** wskazano odrębnie „imiona rodziców osób oraz numer dokumentu potwierdzającego tożsamość osób, o których mowa w pkt 1 i 2." Co do zasady osoba fizyczna nie powinna być identyfikowana za pomocą danych innych osób, w tym przypadku imion rodziców. Identyfikacja poprzez imiona rodziców jest swoistym reliktem, którego projektodawca nie powinien wprowadzać w nowych narzędziach służących do identyfikacji elektronicznej, tym bardziej, że cały szereg innych danych, o których mowa w **art. 21a ust. 6a** projektu ustawy pozawala na identyfikację osoby. **Należy zadać pytanie o adekwatność tych danych, do tej pory nie wymienionych w art. 21a ust. 6** ustawy o usługach zaufania oraz identyfikacji elektronicznej, oraz **nie wymaganych rozporządzaniem 910/2014 oraz aktami wykonawczymi do niego**. Sformułowanie „numer dokumentu potwierdzającego tożsamość osób, o których mowa w pkt 1 i 2", ma również charakter niejednoznaczny gdyż, przynajmniej w odniesieniu do obywateli Polski istnieje w powszechnie obowiązującym stanie prawnym ograniczona liczba dokumentów potwierdzających tożsamość. Tak sformułowany przepis może prowadzić do sytuacji, w której minister właściwy do spraw informatyzacji będzie przetwarzał dane z innych dokumentów niż chociażby dowód osobisty czy paszport, gdyż na ich podstawie również można stwierdzić tożsamość osoby, chociaż są wydawane w innych celach (np. prawo jazdy, legitymacja studencka). Uprawdopodabnia tą sytuację brzmienie **art. 22a ust. 5 pkt 2 lit. b** projektu: „W przypadku niedopasowania tożsamości do danych gromadzonych w rejestrze PESEL, za pomocą systemu scentralizowanego: (…) za zgodą użytkownika wysyłane są do strony ufającej: (…) numer dokumentu potwierdzającego tożsamość tego użytkownika podany przez tego użytkownika.". To od użytkownika będzie zatem zależało jaki numer dokumentu potwierdzającego tożsamość poda.

Konstytucyjna zasada legalizmu wymaga, aby przetwarzanie danych osobowych przez podmioty publiczne odbywało się na podstawie i w granicach przepisów prawa (art. 7 Konstytucji RP). Rolą projektodawcy jest natomiast precyzyjne wskazanie wykonawcom norm, jakie dane mają być przetwarzane, w jakim celu, w jaki sposób, przez jaki okres czasu oraz kto będzie za to przetwarzanie odpowiadał (art. 5 ust. 1 lit. a, b, c, e w zw. z art. 5 ust. 2 w zw. z art. 6 ust. 3 rozporządzenia 2016/679). Władze publiczne nie mogą zaś pozyskiwać, gromadzić i udostępniać innych informacji o obywatelach niż niezbędne w demokratycznym państwie prawnym, zaś zasady i tryb gromadzenia oraz udostępnienia informacji określa ustawa (art. 51 ust 2 i ust. 5 Konstytucji RP).

Wszystkie powyższe kwestie powinny zostać poddane pogłębionej analizie przez projektodawcę, w tym również w **ocenie skutków dla ochrony danych**, tak aby projektowane przepisy odpowiadały zasadzie zgodności z prawem, rzetelności i przejrzystości, ograniczenia celu, minimalizacji danych oraz rozliczalności.

2. Ww. uwaga odnosi się odpowiednio do **art. 1 pkt 9** projektu ustawy – projektowanego **art. 22a ust. 3** w odniesieniu do **zakresu danych przetwarzanych w systemie scentralizowanym.**

3. Zgodnie z **art. 1 pkt 6** projektu ustawy zostaje dodany **art. 21aa** ustawy o usługach zaufania oraz identyfikacji elektronicznej, który w ust. 1 zobowiązuje ministra właściwego do spraw informatyzacji do zapewnienia użytkownikom środków identyfikacji elektronicznej wydanych w systemie identyfikacji elektronicznej przyłączonym do węzła krajowego możliwości zapoznania się z historią ich użycia zapisaną w logach systemu, niezależnie od spełnienia wymogu zawartego w art. 5a ust. 4 lit. d rozporządzenia eIDAS2. Przepis ten bardzo korzystnie wpłynie na rozliczalność operacji wykonywanych przy użyciu środków identyfikacji elektronicznej.

W projekcie **brak jest jednak informacji przez jak długi okres dane o historii użycia środków identyfikacji elektronicznej**, o których mowa wyżej, **będą przechowywane**. Z uwagi na obowiązek poinformowania osoby, której dane dotyczą o okresie przechowywania danych jej dotyczących, a w przypadku gdy nie jest to możliwe, kryteriach ustalenia tego okresu, wynikający z art 13 ust. 2 lit. a rozporządzenia 2016/679, dodany **art. 21aa należy rozszerzyć o informację wskazującą okres przechowywania logów systemu, o których mowa w ust 1**.

Wyjaśnienie i doprecyzowanie tych kwestii jest konieczne z punktu widzenia zasady zgodności z prawem, rzetelności i przejrzystości, ograniczenia celu, minimalizacji danych, ograniczenia przechowywania oraz rozliczalności.

4. Zgodnie z **art. 1 pkt 6** projektu ustawy dodającym **art. 21aa ust. 4** w ustawie o usługach zaufania oraz identyfikacji elektronicznej: „Użytkownik może pobrać dokument elektroniczny zawierający imię, nazwisko, numer PESEL oraz dane, o których mowa w ust. 2, opatrzony zaawansowaną pieczęcią elektroniczną weryfikowaną za pomocą kwalifikowanego certyfikatu ministra właściwego do spraw informatyzacji.”.
Z projektowanego przepisu **nie wynika jaki jest cel wydawania tego dokumentu i co za tym idzie, jaki jest cel przetwarzania danych**. Jeżeli celem tym ma być potwierdzenie autentyczności danych zawartych w tym dokumencie za pomocą kwalifikowanego certyfikatu ministra właściwego do spraw informatyzacji, to powinno to być wprost ujęte w projektowanym przepisie, dla zachowania zasady zgodności z prawem, rzetelności i przejrzystości oraz ograniczenia celu.

5. Zgodnie z **art. 1 pkt 9** projektu ustawy dodającym **art. 22a ust. 1** i **2** w ustawie o usługach zaufania oraz identyfikacji elektronicznej: „Minister właściwy do spraw informatyzacji zapewnia funkcjonowanie systemu scentralizowanego, o którym mowa w art. 21a ust. 1 lit. c, umożliwiającego dopasowywanie tożsamości, o którym w art. 11a rozporządzenia 910/2014. 2. System scentralizowany zapewnia w szczególności: (…)”.
Projektowany przepis powinien określać wszystkie funkcjonalności systemu scentralizowanego, ze względu na zakres i cel przetwarzania danych w tym systemie.

Podstawowym celem funkcjonowania tego sytemu jest – zgodnie z art. 11a ust.1 rozporządzenia 910/2014 – zapewnienie przez państwo członkowskie UE jednoznacznego dopasowywania tożsamości osób fizycznych z użyciem notyfikowanych środków identyfikacji elektronicznej lub europejskich portfeli tożsamości cyfrowej. W związku z **planowanym połączeniem sytemu scentralizowanego z innymi systemami**

podmiotów publicznych, zgodnie z **art. 8** projektu ustawy „System teleinformatyczny podmiotu publicznego, w którym udostępniane są usługi online, uruchomiony przed dniem wejściem życie ustawy przyłącza się do systemu scentralizowanego, o którym mowa w art. 21a ust. 1 pkt 2 lit. c, ustawy zmienianej w art. 1, w terminie 6 miesięcy od dnia wejścia w życie ustawy.”. W pierwszej kolejności należy wskazać, że termin „przyłącza się” w świetle operacji na danych osobowych i przetwarzania danych jest nieprecyzyjny. Projektowane przepisy nie określają w jaki sposób przyłączanie systemów wpłynie na ich funkcjonalności, nie wiadomo również w jaki sposób ma się ono odbyć.

Konieczne jest również wprowadzenie zmian wynikowych (tzw. „lustrzanych”) w poszczególnych ustawach regulujących funkcjonowanie tych systemów teleinformatycznych, których część będzie miało charakter rejestrów publicznych. Wynika ta konieczność określenia w przepisach prawa zasad przetwarzania danych osobowych w zbiorach i rejestrach prowadzonych przez podmioty publiczne z motywu 31 rozporządzenia 2016/679[8] oraz orzecznictwa europejskiego, w szczególności wyroku Trybunału Sprawiedliwości z 1 października 2015 r. w sprawie C-201/14 Smaranda Bara i in. przeciwko Presedintele Casei Nationale de Asigurări de Sănătate i in[9]. Na ryzyka braku określenia wszelkich procesów związanych z przetwarzaniem danych w rejestrach publicznych organ ochrony danych osobowych zwracał uwagę wielokrotnie w postępowaniach legislacyjnych i wystąpieniach i uwagi te pozostają aktualne[10].

6. Uwaga w zakresie konieczności uregulowania w przepisach prawa planowanej operacji przetwarzania danych odnosi się odpowiednio do **art. 5 pkt 2** projektu ustawy – projektowanego **rozdziału 1a ustawy z dnia 18 listopada 2020 r. o doręczeniach elektronicznych** w zakresie łączenia informacji z systemów teleinformatycznych i rejestrów publicznych z Katalogiem Podmiotów Publicznych.

7. Zgodnie z **art. 1 pkt 9** projektu ustawy, dodającym **art. 22a ust. 2 pkt 2** w ustawie o usługach zaufania oraz identyfikacji elektronicznej, „system scentralizowany zapewnia w szczególności: (…) możliwość żądania przez stronę ufającą od osoby fizycznej podania dodatkowych danych, o których mowa w ust. 4 pkt 3, i przekazania tych danych przez osobę fizyczną celem jednoznacznego dopasowania tożsamości w przypadku, gdy dopasowanie tożsamości jest niejednoznaczne”. W projektowanym

[8] Organy publiczne, którym ujawnia się dane osobowe w związku z ich prawnym obowiązkiem sprawowania funkcji publicznej (takich jak organy podatkowe, organy celne, finansowe jednostki analityki finansowej, niezależne organy administracyjne czy organy rynków finansowych regulujące i nadzorujące rynki papierów wartościowych), nie powinny być traktowane jako odbiorcy, jeżeli otrzymane przez nie dane osobowe są im niezbędne do przeprowadzenia określonego postępowania w interesie ogólnym zgodnie z prawem Unii lub prawem państwa członkowskiego. Żądanie ujawnienia danych osobowych, z którym występują takie organy publiczne, powinno zawsze mieć formę pisemną, być uzasadnione, mieć charakter wyjątkowy, nie powinno dotyczyć całego zbioru danych ani prowadzić do połączenia zbiorów danych. Przetwarzając otrzymane dane osobowe, takie organy powinny przestrzegać mających zastosowanie przepisów o ochronie danych, zgodnie z celami przetwarzania.

[9] Wyrok TSUE z 1.10.2015 R., C-201/14, Smaranda Bara i in. v. Pretedintele Casei Nationale De Asigurări De Sănătate i in., Zotsis 2015, Nr 10, Poz. I-638.

[10] W sprawie modelu funkcjonowania rejestrów publicznych i praktyki łączenia w rejestrach publicznych danych osobowych pozyskiwanych z różnych baz danych, organ nadzorczy skierował do Ministra Cyfryzacji wystąpienie znak: DOL.413.11.2024.WL.OJ z 29 października 2025 r.

przepisie występuje odwołanie do ust. 4 pkt 3, którego **brak** w dodanym art. 22a. W art. 22a ust. 4 są pkt 1 i pkt 2 (brak jest pkt 3).

8. Zgodnie z **art. 1 pkt 9** projektu ustawy, dodającym **art. 22a ust. 4 pkt 1** i **2** w ustawie o usługach zaufania oraz identyfikacji elektronicznej: „W przypadku dopasowania tożsamości do danych gromadzonych w rejestrze PESEL, za pomocą systemu scentralizowanego: (…) 1) użytkownik usługi online informowany jest o dopasowaniu i możliwości wysłania ustalonego numeru PESEL do strony ufającej; 2) za zgodą użytkownika usługi online wysyłane są do strony ufającej dane identyfikujące osobę, o których mowa w ust. 3 pkt 1 lub 2, wraz z ustalonym numerem PESEL.”.

Konieczne jest ponowne przeanalizowanie koncepcji oparcia systemu scentralizowanego na numerze PESEL, jako danej która ostatecznie będzie potwierdzać tożsamość użytkownika europejskiego portfela tożsamości cyfrowej. Kwestia ta powinna zostać poddana analizie **w ocenie skutków dla ochrony danych**. W kontekście bezpośredniego powiązania konieczności utworzenia systemu scentralizowanego z wprowadzeniem europejskiego portfela tożsamości cyfrowej, za którego funkcjonowanie będzie odpowiedzialny minister właściwy do spraw informatyzacji zagadnienie to zostało szerzej omówione w uwagach do zmian w ustawie o aplikacji mObywatel.

9. Zgodnie z **art. 1 pkt 9** projektu ustawy, dodającym **art. 22a ust. 2 pkt 3** w ustawie o usługach zaufania oraz identyfikacji elektronicznej, system scentralizowany będzie zapewniał „możliwość zachowania wyników dopasowywania tożsamości, w szczególności numeru PESEL, w sposób umożliwiający uniknięcie ponownego dopasowywania tożsamości dla tej samej osoby wykorzystującej ten sam środek identyfikacji elektronicznej.”. **Projektodawca nie wskazuje maksymalnego okresu przechowywania takich powiązań oraz nie określa czy użytkownik będzie miał wpływ na tą funkcjonalność, w szczególności czy będzie mógł decydować o nieskorzystaniu z niej**. Doprecyzowanie tej regulacji jest konieczne dla zachowania zasady zgodności z prawem, rzetelności i przejrzystości oraz ograniczenia przechowywania.

10. Zgodnie z **art. 1 pkt 9** projektu ustawy, dodającym **art. 22a ust. 6** w ustawie o usługach zaufania oraz identyfikacji elektronicznej, dane identyfikujące osobę są wysyłane w formacie danych zgodnym z formatem danych wysyłanych przez węzeł krajowy. Projektowany przepis jest **niejasny**, gdyż **nie określa tego formatu danych, nie zawiera również odesłania do innych przepisów ustawy regulujących tą materię**. Doprecyzowanie tej regulacji jest konieczne dla zachowania zasady zgodności z prawem, rzetelności i przejrzystości.

11. Zgodnie z **art. 1 pkt 9** projektu ustawy, dodającym **art. 22b ust. 1 pkt 5** i **6** w ustawie o usługach zaufania oraz identyfikacji elektronicznej: „Minister właściwy do spraw informatyzacji prowadzi, przy użyciu systemu teleinformatycznego, rejestr stron ufających

europejskiemu portfelowi tożsamości cyfrowej, o którym mowa w art. 3 ust. 1 rozporządzenia 2025/848, oraz zapewnia utrzymanie i rozwój tego rejestru, w tym: (…) 5) określa zasady bezpieczeństwa przetwarzanych danych, w tym danych osobowych; 6) określa zasady zgłaszania naruszenia ochrony danych osobowych;". Jak stanowi zaś uzasadnienie do projektu ustawy, odnosząc się do projektowanego **art. 22b ust. 3** ustawy o usługach zaufania oraz identyfikacji elektronicznej: „Wpis do rejestru stron ufających będzie następował automatycznie, po zweryfikowaniu kompletności danych przekazanych za pomocą formularza elektronicznego, udostępnionego przez ministra właściwego do spraw informatyzacji lub w ramach wniosku, przekazanego za pośrednictwem kwalifikowanego dostawcy usług zaufania. Zakłada się bowiem, że zakres danych osobowych, jakich strona ufająca będzie żądać od użytkownika europejskiego portfela tożsamości cyfrowej, nie będzie urzędowo weryfikowany w postępowaniu administracyjnym przed dokonaniem wpisu do rejestru stron ufających, ponieważ będzie wyświetlony każdemu użytkownikowi portfela, korzystającemu z danej usługi. Oznacza to, że sami użytkownicy portfela **będą mieli możliwość zweryfikowania, czy żąda się od nich nadmiarowych danych i będą mogli poinformować o takim ewentualnym przypadku organ ochrony danych osobowych za pomocą usługi udostępnionej w każdym portfelu**. Taki samoregulujący się system zapewni minimalizację danych niezbędnych do świadczenia usług bez potrzeby biurokratyzowania kwestii dostępu do tych wyżej wspomnianych danych w kosztownym postępowaniu administracyjnym, które spowalniałoby proces rejestracji, a jednocześnie nie zapewniłoby w praktyce lepszej ochrony takich danych.".

Projektowany przepis **powiela wadliwe rozwiązania** dotyczące blankietowego ukształtowania uprawnienia ministra właściwego do spraw informatyzacji do dodawania usług w systemach, których jest administratorem, sygnalizowane przez organ nadzorczy przy procedowaniu ustawy z dnia 26 maja 2023 r. o aplikacji mObywatel[11]. Uprawnienia te powinny być natomiast oparte na akcie prawa powszechnie obowiązującego. W tym przypadku na blankietowe i zdecydowanie niewyczerpujące przepisy ustawy nałożone zostaną uprawnienia do kształtowania celów i sposobów przetwarzania w drodze uznaniowej i opartej na uznaniu decyzji ministra właściwego do spraw informatyzacji.

W oparciu o ogólne uprawnienie do kształtowania zasad bezpieczeństwa i zgłaszania naruszeń ochrony danych osobowych, na podstawie wyłącznie uzasadnienia do projektu ustawy, projektodawca zakłada wprowadzenie usługi zgłaszania Prezesowi UODO naruszeń ochrony danych osobowych w ramach portfela tożsamości cyfrowej. Dodatkowo – argumentując to koniecznością uniknięcia nadmiernego biurokratyzowania – decyduje, że zakres danych osobowych, jakich strona ufająca będzie żądać od użytkownika europejskiego portfela tożsamości cyfrowej, nie będzie urzędowo weryfikowany w postępowaniu administracyjnym przed dokonaniem wpisu do rejestru stron ufających. Tym samym **administrator rejestru stron ufających** – minister właściwy do spraw informatyzacji – **przerzuca na użytkownika portfela tożsamości cyfrowej swoją odpowiedzialność za zapewnienie zasad przetwarzania danych osobowych, zgodności z prawem, rzetelności i przejrzystości, ograniczenia**

[11] Opinia Prezesa UODO do projektu ustawy z 22 czerwca 2022 r. znak: DOL.401.276.2022.WL.PM.

celu i minimalizacji danych. Jest to sprzeczne z filozofią i standardami rozporządzenia 2016/679, w tym również z zasadą rozliczalności, która na administratora nakłada odpowiedzialność za przestrzeganie zasad przetwarzania danych osobowych i wymaga wykazania ich przestrzegania. Powyższy problem ma rozwiązać dodanie wygodnej dla użytkownika usługi zgłaszania naruszeń ochrony danych organowi nadzorczemu. Użytkownik, powinien w pierwszej kolejności móc oprzeć swoją decyzję o ewentualnym zgłoszeniu naruszenia, na jasnych i przejrzystych rozwiązaniach prawnych określających ramy tego przetwarzania, mając jednocześnie świadomość, że podmiot publiczny przy pomocy nadanych mu mocą powszechnie obowiązującego prawa narzędzi będzie w stanie wyeliminować oczywiste zagrożenia dla prywatności osoby – użytkownika. Przy takiej konstrukcji i brzmieniu komentowanych przepisów odpowiedzialność ta będzie przeniesiona na użytkownika i częściowo na organ nadzorczy, który będzie obsługiwał zgłoszenia naruszeń przekazanych mu przy pomocy usługi udostępnianej przez ministra właściwego do spraw informatyzacji. Nie wiadomo przy tym nawet w przybliżonym kształcie jak taka usługa ma wyglądać i czy organ nadzorczy będzie zobowiązany do wdrożenia odpowiednich rozwiązań technicznych umożliwiających obsługę takich naruszeń.

Powstaje również zasadnicze pytanie czy to co projektodawca określa mianem zgłoszenia naruszenia nie jest w istocie skargą w rozumieniu art. 77 rozporządzenia 2016/679, w której użytkownik zwraca się o zbadanie poszanowania przez administratora zasady zgodności z prawem, rzetelności i przejrzystości; zasady ograniczenia celu oraz minimalizacji danych. W utrwalonym orzecznictwie sądów powszechnych i administracyjnych, to administrator jest wskazywany jako pierwszy odbiorcą żądania osoby do wyjaśnienia procesów przetwarzania danych. To on w pierwszej kolejności odpowiada za wykazanie legalności procesów przetwarzania danych oraz realizację innych zasad wynikających z rozporządzenia 2016/679. Zgłaszanie naruszeń jest obowiązkiem administratora danych zgodnie z art. 33 rozporządzenia 2016/679, będzie więc realizowane odpowiednio przez stronę ufającą lub ministra właściwego do spraw informatyzacji jako podmiotu odpowiedzialnego za zapewnienie portfela tożsamości cyfrowej.

Ocena skutków regulacji projektowanej ustawy nie wskazuje organu nadzorczego wśród podmiotów, na które oddziałuje projekt, nie zakłada się również, żadnych dodatkowych środków finansowych i organizacyjnych dla organu nadzorczego w związku z planowanym wdrożeniem tej usługi – na co należy zwrócić szczególną uwagę i dokonać odpowiedniego uzupełnienia. Jeśli ustawodawca przewiduje taki mechanizm, to w ocenie skutków regulacji powinna znaleźć się także analiza potencjalnej ilości naruszeń, które mogą zostać zgłoszone organowi nadzorczemu w opisywanym trybie.

12. Uwaga odnosi się odpowiednio do **art. 5 pkt 2** projektu ustawy – projektowanego **art. 10a ust. 1 pkt 5 i 6 ustawy z dnia 18 listopada 2020 r. o doręczeniach elektronicznych**, w odniesieniu do uprawnienia ministra właściwego do spraw informatyzacji do uznaniowego określania zasad bezpieczeństwa przetwarzanych

danych, w tym danych osobowych oraz zasad zgłaszania naruszenia ochrony danych osobowych w tworzonym Katalogu Podmiotów Publicznych.

13. Zgodnie z **art. 1 pkt 9** projektu ustawy, dodającym **art. 22b ust. 15** i **16** w ustawie o usługach zaufania oraz identyfikacji elektronicznej: „15. Minister właściwy do spraw informatyzacji określi i udostępni w Biuletynie Informacji Publicznej na swojej stronie podmiotowej: 1) krajową politykę rejestracji w rejestrze stron ufających europejskim portfelom tożsamości cyfrowej, o której mowa w rozporządzeniu 2025/848; 2) krajową politykę certyfikacji i oświadczeń dotyczących praktyk certyfikacji w odniesieniu do certyfikatów dostępu strony ufającej portfelowi, o której mowa w rozporządzeniu 2025/848; 3) krajową politykę certyfikacji i oświadczeń dotyczących praktyk certyfikacji w odniesieniu do certyfikatów rejestracji strony ufającej portfelowi, o której mowa w rozporządzeniu 2025/848. 16. Podmioty wydające certyfikaty dostępu strony ufającej portfela oraz certyfikaty rejestracji strony ufającej portfela stosują się do krajowych polityk, o których mowa w ust. 15.”.

Polityki, o których mowa w projektowanym przepisie będą miały kluczowe znaczenie dla funkcjonowania europejskiego portfela tożsamości cyfrowej, a zatem powinny zostać ustalone w akcie prawa powszechnie obowiązującego, np. aktem wykonawczym do ustawy o usługach zaufania oraz identyfikacji elektronicznej, zgodnie z zasadą zgodności z prawem, rzetelności i przejrzystości.

14. Zgodnie z **art. 1 pkt 9** projektu ustawy, dodającym **art. 22c** w ustawie o usługach zaufania oraz identyfikacji elektronicznej: „1. Podmioty publiczne odpowiedzialne na poziomie krajowym za źródła autentyczne, o których mowa w załączniku VI do rozporządzenia 910/2014, zapewniają kwalifikowanym dostawcom usług zaufania, którzy dostarczają kwalifikowane elektroniczne poświadczenia atrybutów, możliwość weryfikacji tych atrybutów drogą elektroniczną, na żądanie użytkownika, zgodnie z art. 45e ust. 1 rozporządzenia 910/2014. 2. Podmioty inne niż podmioty publiczne odpowiedzialne na poziomie krajowym za źródła autentyczne, o których mowa w załączniku VI do rozporządzenia 910/2014, mogą zapewnić kwalifikowanym dostawcom usług zaufania, którzy dostarczają kwalifikowane elektroniczne poświadczenia atrybutów, możliwość weryfikacji tych atrybutów drogą elektroniczną, na żądanie użytkownika, zgodnie z art. 45e ust. 1 rozporządzenia 910/2014.”. Projektodawca zakłada, że niecelowe jest ustalanie podmiotów odpowiedzialnych za źródła autentyczne, argumentując to w następujący sposób w uzasadnieniu do projektu ustawy: „Wspomniane wyżej podmioty publiczne celowo nie są wymieniane wprost w projektowanych przepisach, z uwagi na to, że stale postępująca informatyzacja zadań publicznych powoduje tworzenie kolejnych publicznych źródeł autentycznych, które wcześniej nie istniały. Zakłada się, że odpowiednie podmioty publiczne udostępnią kwalifikowanym dostawcom usług zaufania zarządzane przez siebie źródła autentyczne – do weryfikacji danych na podstawie przepisów eIDAS – stąd też nie ma potrzeby dodawania takiego wymogu w przepisach sektorowych. Powodowałoby to bowiem niepotrzebną inflację prawa i dodatkowo niepewność w zakresie możliwości udostępnienia źródeł autentycznych, w przypadku, gdy nie byłoby specjalnego przepisu ustawowego wymagającego udostępnienia określonego źródła. **Mogłoby to w**

zasadniczy sposób utrudnić albo wręcz uniemożliwić wydawanie kwalifikowanych elektronicznych poświadczeń atrybutów, co byłoby niezgodne z ogólnymi celami europejskich ram tożsamości cyfrowej.”.

W ocenie organu nadzorczego projektowany przepis osiągnie odwrotny skutek, tj. utrudnić może wykorzystanie źródeł autentycznych, dodatkowo narażając poszczególne podmioty publiczne będące administratorami, na których mają się oprzeć elektroniczne poświadczania atrybutów, na odpowiedzialność wynikającą z rozporządzenia 2016/679, tj. **udostępnianie danych bez odpowiedniej podstawy prawnej**. Załącznik VI do rozporządzenia 910/2014 wymienia następujące atrybuty, które polegają na źródłach autentycznych w sektorze publicznym: „adres, wiek, płeć, stan cywilny, skład rodziny, narodowość lub obywatelstwo; wykształcenie, tytuły i licencje, kwalifikacje zawodowe, tytuły i licencje; pełnomocnictwa i upoważnienia do reprezentowania osób fizycznych lub prawnych, publicznoprawne zezwolenia i licencje, w odniesieniu do osób prawnych – dane finansowe i dane dotyczące przedsiębiorstwa.”. W ocenie organu nadzorczego nie ma przeszkód ku temu aby wskazać w projektowanej ustawie, które podmioty publiczne będą odpowiedzialne za poszczególne atrybuty. Mocą przywoływanej już zasady rozliczalności administrator ponosi odpowiedzialność za przestrzeganie zasad przetwarzania danych osobowych i obowiązany jest wykazać ich przestrzeganie. Na podstawie tak blankietowo ukształtowanego przepisu jak projektowany art. 22c nie da się ustalić jaki podmiot publiczny odpowiedzialny jest za dany atrybut, bo takie pojęcie nie występuje w obecnym porządku prawnym. W ocenie organu nadzorczego **sam fakt występowania określonych danych w rejestrach publicznych, których administratorem jest dany podmiot publiczny nie przesądza, że dane te mają być udostępnione kwalifikowanym dostawcom usług zaufania dla celu innego niż pierwotnie założony**. Założeniem projektodawcy jest jak się wydaje udostępnianie tych danych przez poszczególne podmioty publiczne niezależnie od ich roli w procesach przetwarzania danych, a przesądzać o tym ma sam fakt bycia w ich posiadaniu, gdyż **kryterium odpowiedzialności za źródła autentyczne, też nie zostało w projektowanej ustawie zdefiniowane w kontekście polskiego porządku prawnego**. W ocenie organu nadzorczego jest to fundamentalnie sprzeczne z konstytucyjną zasadą legalizmu, która wymaga, aby przetwarzanie danych osobowych przez podmioty publiczne odbywało się na podstawie i w granicach przepisów prawa. Jest to również sprzeczne z zasadą zgodności z prawem, rzetelności i przejrzystości, ograniczenia celu, minimalizacji danych oraz rozliczalności.

W omawianym przypadku **konieczne jest wprowadzenie zmian sektorowych dotyczących poszczególnych rejestrów publicznych i systemów teleinformatycznych** zgodnie z wcześniej przytoczonymi wyżej w niniejszej opinii motywem 31 rozporządzenia 2016/679 i wyrokiem w sprawie C-201/14.

15. Zgodnie z **art. 1 pkt 9** projektu ustawy, dodającym **art. 22i** w ustawie o usługach zaufania oraz identyfikacji elektronicznej: „Minister właściwy do spraw informatyzacji: 1) opracowuje i utrzymuje krajowy program certyfikacji, o którym mowa art. 3 rozporządzenia wykonawczego Komisji (UE) 2024/2981 z dnia 28 listopada 2024 r. ustanawiającego zasady stosowania rozporządzenia Parlamentu Europejskiego i Rady

(UE) nr 910/2014 w odniesieniu do certyfikacji europejskich portfeli tożsamości cyfrowej, w szczególności sporządza i utrzymuje program certyfikacji europejskiego portfela tożsamości cyfrowej, o którym mowa w ustawie z dnia 26 maja 2023 r. o aplikacji mObywatel; 2) wyznacza jednostką certyfikującą, o której mowa w art. 2 pkt 9 rozporządzenia Wykonawczego Komisji (UE) 2024/2981 z dnia 28 listopada 2024 r. ustanawiającego zasady stosowania rozporządzenia Parlamentu Europejskiego i Rady (UE) nr 910/2014 w odniesieniu do certyfikacji europejskich portfeli tożsamości cyfrowej; 3) pełni rolę organu nadzoru, o którym mowa w art. 46a rozporządzenia 910/2014, oraz przekazuje odpowiednie informacje do Komisji Europejskiej w tym zakresie.”.

Na podstawie projektowanego przepisu dojdzie do sytuacji, w której minister właściwy do spraw informatyzacji opracowuje i utrzymuje krajowy program certyfikacji w odniesieniu do europejskiego portfela tożsamości cyfrowej, za którego funkcjonowanie ma być sam odpowiedzialny. Pełni również nadzór nad ramami dla europejskiego portfela tożsamości cyfrowej którego sam ma być administratorem. Prawodawca, mocą art. 46a rozporządzenia nr 910/2014 wymaga, aby organy nadzoru nad ramami europejskiego portfela tożsamości cyfrowej posiadały uprawnienia i zasoby do wykonywania swoich zadań w sposób skuteczny, efektywny i niezależny. Gwarancje w postaci **art 22j** projektu ustawy, który stanową, że: „Zadania ministra właściwego do spraw informatyzacji, o których mowa w art. 14a ustawy z dnia 26 maja 2023 r. o aplikacji mObywatel, nie mogą być realizowane przez tę samą komórkę organizacyjną w urzędzie obsługującym tego ministra, która realizuje zadania, o których mowa w art. 22i, sprawuje nadzór nad dostawcami usług zaufania, o którym mowa w art. 27 ust. 1, lub sprawuje nadzór nad krajowym schematem identyfikacji elektronicznej, o którym mowa w art. 39a.” mogą być niewystarczające dla zapewnienia wspomnianej niezależności. **Zaproponowane rozwiązanie wydaje się nie spełniać zatem wymaganych w art. 46a warunków niezależności.**

16. Zgodnie z **art. 1 pkt 11** projektu ustawy, zmieniającym **art. 23 pkt 2** w ustawie o usługach zaufania oraz identyfikacji elektronicznej: „Minister właściwy do spraw informatyzacji: (…) po uzyskaniu opinii CSIRT GOV, CSIRT MON i CSIRT NASK, o których mowa w art. 2 pkt 1–3 ustawy z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa (Dz. U. z 2024 r. poz. 1077), udostępnia kod źródłowy poszczególnych komponentów oprogramowania europejskiego portfela tożsamości, o którym mowa w ustawie z dnia 26 maja 2023 r. o aplikacji mObywatel;”. Z projektowanego przepisu **nie wynika w jaki sposób poszczególne komponenty kodu źródłowego zostaną udostępnione** (np. repozytorium kodu) i czy w ramach udostępnienia będą one publikowane w biuletynie informacji publicznej lub stronie podmiotowej ministra właściwego do spraw informatyzacji. Wyjaśnienie i doprecyzowanie tej kwestii są konieczne z punktu widzenia zasady zgodności z prawem, rzetelności i przejrzystości.

17. Zgodnie z **art. 1 pkt 14** projektu ustawy, dodającym **art. 24a** w ustawie o usługach zaufania oraz identyfikacji elektronicznej: „Dostawca rozwiązania składa wniosek do ministra właściwego do spraw informatyzacji o uznanie rozwiązania jako europejskiego portfela tożsamości cyfrowej wydawanego niezależnie od jednego z państw członkowskich

Unii Europejskiej, o którym mowa w art. 5a ust. 2 lit. c rozporządzenia 910/2014.”. Organ nadzorczy zwraca uwagę, że użyte w projektowanym przepisie sformułowanie: „niezależnie od jednego z państw członkowskich Unii Europejskiej” jest **niejasne**. Z projektowanego przepisu nie wynika, czy oznacza to, niezależność dostawcy rozwiązania od któregokolwiek z państw członkowskich, czy jednego z państw członkowskich, czy też dostawca musi być związany w jakiś sposób z państwem członkowskim lub czy może to być dostawca niezależny od państwa członkowskiego. Wyjaśnienie i doprecyzowanie tej kwestii są konieczne zgodnie z zasadą zgodności z prawem, rzetelności i przejrzystości.

II. Uwagi do zmian w ustawie z dnia 17 lutego 2005 r. o informatyzacji działalności podmiotów realizujących zadania publiczne.

1. Organ nadzorczy z uznaniem przyjmuje wprowadzenie **art. 4 pkt 1** projektu ustawy, zmieniającego **art. 3 pkt 14** w ustawie o informatyzacji działalności podmiotów realizujących zadania publiczne (Dz. U. z 2025 r. poz. 1703), który **wprowadza nowe profile zaufane** w postaci **profilu identyfikującego i opisującego podmiot publiczny** oraz **profilu identyfikującego i opisującego osobę fizyczną reprezentującą podmiot publiczny**, co pozytywnie wpłynie na osoby, które do tej pory musiały posługiwać się prywatnym profilem zaufanym do celów służbowych.

Jednak, dla pełnego zachowania zasad przetwarzania danych osobowych określonych w rozporządzaniu 2016/679 **konieczne jest ponownie dokonanie analizy katalogu danych jakie będą przetwarzane w nowych profilach zaufanych, jak również zasad posługiwania się nimi, o czym niżej.**

2. Zgodnie z **art. 4 pkt 3** projektu ustawy, dodającym **art 20ac pkt 1a – 1d** w ustawie o informatyzacji działalności podmiotów realizujących zadania publiczne, określony zostanie zakres danych przetwarzanych przez ministra właściwego do spraw informatyzacji w związku z obsługą odpowiednio: 1a podmiotu publicznego, któremu wydano profil zaufany, 1b osoby fizycznej, której wydano profil zaufany osoby reprezentującej podmiot publiczny, 1c administratora profilu zaufanego wydanego podmiotowi publicznemu. Wśród danych osób, o których mowa w punktach 1b i 1c pomimo, że są to osoby pełniące określone funkcje (osoby reprezentującej podmiot publiczny, osoby pełniącej funkcję administratora profilu zaufanego podmiotu publicznego) w podmiotach publicznych i w ramach danego podmiotu publicznego w sposób jednoznaczny identyfikowane poprzez imię, nazwisko, pełnioną funkcję oraz nazwę reprezentowanego podmiotu, wymagany jest dodatkowo numer PESEL. Należy dodatkowo zwrócić uwagę, że zgodnie z projektowanym **20ad ust. 1b** profil zaufany osoby fizycznej reprezentującej podmiot publiczny nie będzie zawierał numeru PESEL. Wyjaśnienie i doprecyzowanie tej kwestii jest konieczne dla zachowania zasady zgodności z prawem, rzetelności i przejrzystości, ograniczenia celu, minimalizacji danych, poufności i integralności oraz rozliczalności.

3. Zgodnie z **art. 4 pkt 4 lit. b** projektu ustawy, dodającym **art 20ad ust. 1b** w ustawie o informatyzacji działalności podmiotów realizujących zadania publiczne, profil

zaufany osoby fizycznej reprezentującej podmiot publiczny będzie zawierał imię (imiona), nazwisko¸ nazwisko, datę urodzenia, nazwę reprezentowanego podmiotu publicznego zgodną z KPP oraz numer KPP reprezentowanego podmiotu publicznego. Organ nadzorczy z uznaniem przyjmuje, że zakres tych danych nie będzie zawierał numeru PESEL.

Wśród wymienionych wyżej danych nie powinna pojawiać się również data urodzenia, gdyż w środowisku określonego podmiotu publicznego, z uwagi na zajmowaną funkcję osoby reprezentującej dany podmiot publiczny data urodzenia nie jest niezbędna do jednoznacznej identyfikacji osoby reprezentującej dany podmiot. Uzasadnionym byłoby **wprowadzenie wewnętrznego identyfikatora, w żaden sposób niepowiązanego z danymi osoby fizycznej, oznaczającego ją w ramach danego podmiot publicznego**, w tym dla osób takich jak pracownicy administracji publicznej, upoważnieni do wydawania decyzji administracyjnych, czy też elektronicznego pospisywania pism, zaś w żaden inny sposób nie umocowani do reprezentacji danego podmiotu publicznego. Wyjaśnienie i doprecyzowanie tych kwestii są konieczne dla zachowania zasady zgodności z prawem, rzetelności i przejrzystości, ograniczenia celu oraz minimalizacji danych.

4. Zgodnie z **art. 4 pkt 4 lit. d** projektu ustawy, dodającym **art 20ad ust. 2a** w ustawie o informatyzacji działalności podmiotów realizujących zadania publiczne: „W procedurze potwierdzania profilu zaufanego osoby fizycznej reprezentującej podmiot publiczny dane, o których mowa w ust. 1b, są pobierane automatycznie z danych zawartych w profilu zaufanym osoby fizycznej wskazywanej w sposób, o którym mowa w art. 20cd, oraz z profilu zaufanego podmiotu publicznego, za pomocą którego potwierdzono profil zaufany osoby fizycznej reprezentującej podmiot publiczny.”

Wprowadzona zmiana wprawdzie ułatwia zakładanie i potwierdzanie profilu poprzez kopiowanie danych, ale sprawia, że **w tym celu wymagane jest przetwarzanie numeru PESEL, co jak wskazano wcześniej w ocenie organu nadzorczego jest nieadekwatne**.

5. Zgodnie z **art. 4 pkt 6** projektu ustawy, dodającym **art 20cc i art. 22cd** w ustawie o informatyzacji działalności podmiotów realizujących zadania publiczne we wnioskach o wydanie profilu zaufanego podmiotu publicznego wymagane jest podanie poza imieniem i nazwiskiem pracownika wskazanego do zarządzania profilem (administrowania) również jego numer PESEL. Ponadto, zgodnie z art. 20cc ust. 5 projektu „Profil zaufany podmiotu publicznego jest powiązany z profilami zaufanymi osób fizycznych, wskazanych jako administratorzy we wniosku, o którym mowa w ust. 1, lub w sposób, o którym mowa w ust. 4, i jest wykorzystywany przy użyciu ich profili zaufanych, z wykorzystaniem mechanizmów uwierzytelniania polegających na profilu osobistym lub kwalifikowanym certyfikacie podpisu elektronicznego”.

W wyniku przyjęcia projektowanego rozwiązania dojdzie do **łączenia danych związanych z aktywnością zawodową z danymi o charakterze osobistym**. Jest to niezgodne z zasadami dotyczącymi przetwarzania danych osobowych: zgodności z prawem, rzetelności i przejrzystości, ograniczenia celu oraz minimalizacji danych.

III. Uwagi do zmian w ustawie z dnia 18 listopada 2020 r. o doręczeniach elektronicznych.

Zgodnie z **art. 5 pkt 2** projektu ustawy, dodającym **rozdział 1a** w ustawie z dnia 18 listopada 2020 r. o doręczeniach elektronicznych (Dz. U. z 2026 r. poz. 3), wprowadza się przepisy określające stworzenie i utrzymanie przez ministra właściwego do spraw informatyzacji rejestru publicznego – Katalogu Podmiotów Publicznych (KPP) zawierającego szereg bardzo szczegółowych informacji o podmiotach publicznych i niepublicznych realizujących zadania publiczne. Z projektowanego **art. 10a ust. 2** ustawy o doręczeniach elektronicznych wynika, że: „Prowadzenie Katalogu Podmiotów Publicznych ma na celu gromadzenie kompletnych, aktualnych i ustandaryzowanych danych o podmiotach publicznych i podmiotach niepublicznych realizujących zadania publiczne.”, czyli celem utworzenia katalogu jest samo istnienie katalogu. W uzasadnieniu do projektu wskazano, że utworzony KPP będzie istotnym źródłem danych, bez którego nie będzie możliwa realizacja niektórych procesów przewidzianych w projektowanej ustawie (na przykład rejestracja podmiotów w rejestrze stron ufających, wydawanie profilu zaufanego podmiotu publicznego oraz wydawanie europejskiego portfela tożsamości cyfrowej osoby prawnej). Uzasadnienie to **nie wydaje się być wystarczające,** mając na uwadze istniejące już rejestry takie jak Krajowy Rejestr Sądowy czy Centralna Ewidencja i Informacja o Działalności Gospodarczej, oraz nadawane podmiotom identyfikatory takie jak NIP, czy REGON.

Dodatkowo, zgodnie z projektowanym **art. 10a ust. 4** ustawy o doręczeniach elektronicznych: „Podmioty publiczne oraz podmioty niepubliczne realizujące zadania publiczne zamieszczają w katalogu podmiotów publicznych informacje dotyczące ich organizacji i funkcjonowania oraz aktualizują je nie później niż w terminie 5 dni roboczych od dnia zmiany tych informacji.” **bez dookreślenia jakich danych ten proces ma dotyczyć**.

Jednocześnie, na podstawie **art. 10c** ustawy o doręczeniach elektronicznych KPP będzie opierało się na procesie aktualizacji danych w oparciu o rejestry publiczne i na podstawie danych, w których posiadaniu jest minister właściwy do spraw informatyzacji pochodzących z systemów teleinformatycznych prowadzonych przez tego ministra. N**astąpi więc zmiana celu przetwarzania danych w tych systemach teleinformatycznych i rejestrach, bez jednoczesnej zmiany zasad przetwarzania w tych systemach i rejestrach, co prowadzić będzie do naruszenia zasady legalizmu i konstytucyjnej zasady praworządności.**

IV. Uwagi do zmian w ustawie z dnia 26 maja 2023 r. o aplikacji mObywatel.

1. Zgodnie z **art. 6 pkt 1** projektu ustawy, dodającym **art. 1 pkt 5 i 6** w ustawie z dnia 26 maja 2023 r. o aplikacji mObywatel (Dz. U. z 2024 r. poz. 1275 i 1717 oraz z 2025 r. poz. 1019) ustawa będzie określać: „6) sposób zapewnienia i funkcjonowania europejskiego portfela tożsamości cyfrowej, o którym mowa w art. 5a ust. 2 lit. a rozporządzenia Parlamentu Europejskiego i Rady (UE) nr 910/2014 z dnia 23 lipca 2014 r. w sprawie identyfikacji elektronicznej i usług zaufania w odniesieniu do transakcji

elektronicznych na rynku wewnętrznym oraz uchylającego dyrektywę 1999/93/WE, zwanego dalej „rozporządzeniem 910/2014”; 7) warunki i sposób pobierania przez użytkownika europejskiego portfela tożsamości cyfrowej, o którym mowa w art. 5a ust. 2 lit. a rozporządzenia 910/2014, danych dotyczących tego użytkownika, pochodzących z rejestrów publicznych, rejestrów niepublicznych lub systemów teleinformatycznych podmiotów publicznych lub podmiotów niepublicznych;”.

Europejski portfel tożsamości cyfrowej został zdefiniowany w art. 2 pkt 42 rozporządzenia 910/2024, zaś art. 5a ust 2 lit. a tego rozporządzenia określa sposób w jaki może zostać zapewnione funkcjonowanie europejskiego portfela tożsamości cyfrowej. Jeżeli zatem powodem, dla którego projektodawca zdecydował się na definiowanie europejskiego portfela tożsamości cyfrowej w sposób, który ma zapewnić, że podmiotem odpowiedzialnym za jego funkcjonowanie jest minister właściwy do spraw informatyzacji, to należy to uregulować poprzez wskazanie, że chodzi o europejski portfel tożsamości cyfrowej, o którym mowa w art. 2 pkt 42 rozporządzenia 910/2014, którego funkcjonowanie zapewni minister właściwy do spraw informatyzacji.

2. Uwaga odnosi się analogicznie do wszystkich odwołań do art 5a ust 2 lit a rozporządzenia 910/2014 w projektowanej ustawie.

3. Zgodnie z **art. 6 pkt 2** projektu ustawy, dodającym **art. 14a ust. 2** w ustawie z dnia 26 maja 2023 r. o aplikacji mObywatel: „Europejski portfel tożsamości cyfrowej, o którym mowa w art. 5a ust. 2 lit. a rozporządzenia 910/2014, zawiera zestaw danych identyfikujących osobę fizyczną, obejmujący: 1) imię (imiona); 2) nazwisko; 3) datę urodzenia; 4) miejsce urodzenia; 5) numer PESEL; 6) obywatelstwo; 7) płeć; 8) nazwisko rodowe jeżeli występuje w rejestrze PESEL; 9) wizerunek twarzy użytkownika portfela.”.

W kontekście innych uregulowań projektowanej ustawy powstaje zasadnicze pytanie o **adekwatność danych i celowość przetwarzania tak ukształtowanego katalogu danych**.

Po pierwsze, dane takie jak płeć; nazwisko rodowe czy wizerunek twarzy użytkownika portfela nie będą tej osoby identyfikować bez powiązania z innymi danymi, takimi jak jej imię nazwisko i numer PESEL, jeżeli osoba ta wcześniej nie uwierzytelni się u dostawcy danej usługi. Jak wskazano na str. 25 uzasadnienia: „Ponadto, należy podkreślić, że w przypadku, gdy w usłudze online nie jest niezbędny numer PESEL, mechanizmy portfela będą pozwalały na to, aby numer PESEL nie był przekazywany. Europejskie portfele tożsamości cyfrowej mają umożliwiać selektywne udostępnianie danych, czyli działać inaczej niż inne środki identyfikacji elektronicznej wydawane w ramach publicznego systemu identyfikacji elektronicznej (tj. profilu zaufanego, profilu osobistego i profilu mObywatel), dla których zestaw danych identyfikujących osobę fizyczną jest ustalony i stały. Podobnie będzie w przypadku nazwiska rodowego i płci jako elementów znajdujących się w krajowym zestawie danych identyfikujących osobę. Przekazywanie tych danych przez użytkownika portfela stronie ufającej będzie możliwe, tylko wtedy, gdy strona ta zarejestruje się w rejestrze stron ufających europejskiemu portfelowi tożsamości cyfrowej i wskaże odrębnie każdą usługę, w której zamierza takie dane wykorzystywać.”.

Organ nadzorczy z **uznaniem przyjmuje przyjęcie rozwiązań umożliwiających selektywne udostępnianie danych** (w szczególności w postaci wieku i płci osoby), powstaje jednak pytanie **jak rozwiązanie to ma się do zakładanego przez projektodawcę pobierania atrybutów z rejestrów publicznych**. Zgodnie z projektowanym **art. 14h** ustawy o aplikacji mObywatel: „Rada Ministrów określi, w drodze rozporządzenia, zakres danych i wykaz rejestrów publicznych oraz systemów teleinformatycznych, z których użytkownik europejskiego portfela tożsamości cyfrowej, o którym mowa w art. 5a ust. 2 lit. a rozporządzenia 910/2014, może pobrać dane, oraz podmiotów publicznych prowadzących te rejestry publiczne i systemy teleinformatyczne, mając na uwadze adekwatność zakresu tych danych do potrzeb związanych z usługami świadczonymi w ramach europejskiego portfela tożsamości cyfrowej, o którym mowa w art. 5a ust. 2 lit. a rozporządzenia 910/2014, oraz uwarunkowania pozwalające na zapewnienie możliwości pobierania tych danych.”. Tym samym, dane takie jak wiek, nazwisko rodowe, czy płeć osoby, o ile zdecyduje się na takie rozwiązanie Rada Ministrów, będą mogły być pobierane z rejestrów publicznych i udostępniane przez użytkowników dla skorzystania z poszczególnych usług. Powstaje zatem pytanie, **dlaczego projektodawca nie przyjął rozwiązania opierającego identyfikację osób jedynie na danych ograniczonych do imienia i nazwiska oraz unikalnego numeru powiązanego z europejskim portfelem tożsamości cyfrowej**. Skoro minister informatyzacji udostępni zgodnie z art. 5a ust. 2 lit. a rozporządzenia 910/2014, w imieniu Polski jako państwa członkowskiego UE europejski portfel tożsamości cyfrowej i będzie odpowiedzialny za jego funkcjonowanie na podstawie przepisów projektowanej ustawy, to może zgodnie z tabelą 2 rozporządzenia 2024/2977 zapewnić daną w postaci **personal_administrative_number** czyli „Wartość przypisaną osobie fizycznej, która jest niepowtarzalna wśród wszystkich osobistych numerów administracyjnych wydanych przez dostawcę danych identyfikujących osobę. W przypadku gdy państwa członkowskie zdecydują się na włączenie tego atrybutu, mają obowiązek opisać w swoich systemach identyfikacji elektronicznej, w ramach których wydawane są dane identyfikujące osobę, politykę, którą stosują do wartości tego atrybutu, w tym, w stosownych przypadkach, szczególne warunki przetwarzania tej wartości.”. W ocenie organu nadzorczego mógłby to być numer przypisany użytkownikowi portfela (niepowiązany z jego cechami charakterystycznymi jak wiek czy płeć jak ma to miejsce w przypadku numeru PESEL).

Skoro i tak zakłada się, możliwość pobierania danych z rejestrów publicznych przez użytkownika portfela, to w ocenie organu nadzorczego nie ma przeszkód ku temu, aby zapewnić maksymalny poziom prywatności użytkowników portfela przez stworzenie przez ministra właściwego do spraw informatyzacji zestawu danych identyfikacyjnych, unikalnych dla tego portfela, w tym jego numeru będącego w pewnym sensie „numerem seryjnym dokumentu”.

Kwestia ta powinna zostać również przeanalizowana **w ocenie skutków dla ochrony danych projektowanej ustawy** oraz oceniona z punktu widzenia z zasady zgodności z prawem, rzetelności i przejrzystości, ograniczenia celu, minimalizacji danych oraz rozliczalności.

4. Zgodnie z **art. 6 pkt 2** projektu ustawy, dodającym **art. 14b ust. 3** w ustawie z dnia 26 maja 2023 r. o aplikacji mObywatel: „Minister właściwy do spraw informatyzacji określi w drodze rozporządzenia wymagania dotyczące weryfikacji tożsamości, o której mowa w ust. 1 pkt 2, oraz warunki organizacyjno-techniczne jakie musi spełniać punkt potwierdzający tożsamość, o którym mowa w ust. 1 pkt 2 lit. b, uwzględniając wymogi określone w rozporządzeniu 2015/1502.”.

Kwestia **zasad weryfikacji tożsamości powinna zostać określona kompleksowo w projektowanej ustawie** w szczególności, że w omawianym przypadku będzie dotyczyć sposobu, o którym mowa w art. 14b ust. 1 pkt 2, tj. weryfikacji za pomocą profilu zaufanego, z dodatkową weryfikacją tożsamości spełniającą wymagania określone w przepisach wykonawczych wydanych na podstawie art. 5a ust. 24 rozporządzenia 910/2014, co jak wskazano w uzasadnieniu do projektu ustawy oznaczać będzie „(…) wykorzystanie zdalnej weryfikacji tożsamości – w szczególności polegającej na porównaniu danych elektronicznych znajdujących się w okazywanych zdalnie dokumentach tożsamości z warstwą elektroniczną, z wizerunkiem wnioskodawcy przekazywanym za pomocą audiowizualnego połączenia nawiązanego z podmiotem profesjonalnie weryfikującym tożsamość”. Omawiany przypadek będzie dotyczył **przetwarzania z użyciem nowych technologii**. Nie jest to wskazane bezpośrednio przez projektodawcę w uzasadnieniu do projektu ustawy, natomiast w ocenie organu nadzorczego, może istnieć ryzyko przetwarzania danych biometrycznych w postaci wizerunku twarzy (czyli danych szczególnej kategorii w rozumieniu art. 9 ust. 1 rozporządzenia 2016/679) przez podmiot profesjonalnie weryfikujący tożsamość, jeśli spełniać to będzie kryterium wysokiego poziomu bezpieczeństwa.

W odniesieniu do sposobu, o którym mowa w ust. 1 pkt 2 lit. b (na marginesie organ nadzorczy wskazuje, że odesłanie jest błędne – przepis powinien odsyłać do ust. 2 pkt 2 lit. b), czyli banku krajowego oraz niektórych organów gminy, które mogą pełnić tą funkcję za zgodą ministra właściwego do spraw informatyzacji, to organ nadzorczy wskazuje, że weryfikacja tożsamości, w kontekście możliwości posługiwania się narzędziem takim jak europejski portfel tożsamości cyfrowej, jest kwestią na tyle istotną, że przedmiotowa materia nie może zostać przeniesiona do aktu wykonawczego, tym bardziej, że w omawianym przypadku dojdzie do powierzenia realizacji zadania publicznego podmiotom prawa prywatnego – bankom krajowym.

Projektodawca nie uzasadnił wyczerpująco dlaczego, aż tak rozbudowana sieć punktów potwierdzających jest konieczna dla realizacji założeń rozporządzenia 910/2014, tym bardziej, że oprócz szeregu zdalnych metod weryfikacji tożsamości, funkcję tę będzie pełnił wojewoda (art. 14b ust. 2 pkt 1).

Wyjaśnienie tych kwestii jest konieczne dla zachowania zasady zgodności z prawem, rzetelności i przejrzystości oraz ograniczenia celu.

5. Zgodnie z **art. 6 pkt 2** projektu ustawy, dodającym **art. 14c ust. 2 pkt 3** w ustawie z dnia 26 maja 2023 r. o aplikacji mObywatel we wniosku o utworzenie konta użytkownika reprezentującego osobę prawną wśród danych identyfikujących tę osobę **wymagane jest podanie numeru PESEL pomimo, że numer PESEL nie jest**

niezbędny do jednoznacznej identyfikacji osoby fizycznej w obrębie jednostki organizacyjnej będącej osobą prawną.

W odniesieniu do zakresu danych we wniosku o utworzenie konta użytkownika europejskiego portfela tożsamości cyfrowej dla osoby prawnej **przetwarzanie numeru PESEL jest nadmiarowe**, co wynika również z faktu, że zgodnie z projektowanym **art. 20ac ust. 2 pkt 1b** ustawy o informatyzacji działalności podmiotów realizujących zadania publiczne w profilu zaufanym osoby fizycznej reprezentującej podmiot publiczny nie występuje numer PESEL.

6. Zgodnie z **art. 6 pkt 2** projektu ustawy, dodającym **art. 14e ust. 1** w ustawie z dnia 26 maja 2023 r. o aplikacji mObywatel: „Minister właściwy do spraw informatyzacji udostępnia przy użyciu europejskiego portfela tożsamości cyfrowej, o którym mowa w art. 5a ust. 2 lit. a rozporządzenia 910/2014, usługę, która umożliwia użytkownikom europejskiego portfela tożsamości cyfrowej, o którym mowa w art. 5a ust. 2 lit. a rozporządzenia 910/2014, nieodpłatne składanie kwalifikowanych podpisów elektronicznych, zgodnie z art. 5a ust. 5 lit. g rozporządzenia 910/2014, w celach innych niż profesjonalne.”. Zgodnie zaś z **art. 14e ust. 11 i 12** „11. Kwalifikowani dostawcy usług zaufania świadczą usługę, o której mowa w ust. 1, zgodnie z wytycznymi świadczenia tej usługi udostępnionymi przez ministra właściwego do spraw informatyzacji w Biuletynie Informacji Publicznej na jego stronie podmiotowej. 12. Wytyczne świadczenia usługi, o której mowa w ust. 1, określają: 1) sposób weryfikacji tożsamości użytkowników; 2) obsługiwane formaty podpisów; 3) szczególne wymagania dotyczące wydawanych certyfikatów kwalifikowanego podpisu elektronicznego; 4) sposób oznaczania podpisanych dokumentów elektronicznych informacją o opatrzeniu nieodpłatnym kwalifikowanym podpisem elektronicznym, złożonym w celach innych niż profesjonalne.”.

Zaprezentowany model nieodpłatnego składania kwalifikowanych podpisów elektronicznych z użyciem portfela tożsamości cyfrowej, o którym mowa w art. 5a ust. 2 lit. a rozporządzenia 910/2014 budzi zasadnicze wątpliwości organu nadzorczego.

Jedną z kluczowych kwestii podnoszonych w wystąpieniach organu nadzorczego do Ministra Cyfryzacji w związku z funkcjonowaniem w Polsce podpisów elektronicznych[12] było wypracowanie rozwiązań, które **zapobiegną ujawnianiu numeru PESEL jako „swoistego śladu cyfrowego” pozostawianego na podpisywanych cyfrowo dokumentach**.

Biorąc pod uwagę zestaw danych identyfikujących użytkownika portfela określonych w projektowanym **art. 14a ust. 2** ustawy o aplikacji mObywatel, tj. imię (imiona); 2) nazwisko; 3) datę urodzenia; 4) miejsce urodzenia; 5) numer PESEL; 6) obywatelstwo; 7) płeć; 8) nazwisko rodowe jeżeli występuje w rejestrze PESEL; 9) wizerunek twarzy użytkownika portfela oraz fakt, że szczególne wymagania dotyczące wydawanych certyfikatów kwalifikowanego podpisu elektronicznego nie są określone w projektowanej ustawie, ani nawet akcie wykonawczym do niej, a jedynie Biuletynie Informacji Publicznej ministra właściwego do spraw informatyzacji, **powstaje pytanie czy użytkownik**

[12] Wystąpienie znak ZSPU.023.97.2019 z 14 czerwca 2019 r. oraz wystąpienie znak: DOL.413.3.2024 z 12 września 2024 r.

nieodpłatnego kwalifikowanego podpisu elektronicznego będzie mógł używać tego podpisu, tak aby w jego certyfikacie nie było numeru PESEL.

W ocenie organu nadzorczego, jest to wysoce wątpliwe, biorąc pod uwagę blankietowość projektowanych rozwiązań, oraz brak w **art. 14a ust. 2** ustawy o aplikacji mObywatel, danej (oprócz numeru PESEL), która zapewniałaby jednoznaczną identyfikację osoby w powiązaniu z imieniem i nazwiskiem. Zgodnie z zgodnie z projektowanym **art. 14f** ustawy o aplikacji mObywatel „Przez cel składania kwalifikowanego podpisu elektronicznego inny niż profesjonalny, o którym mowa w art. 22e ust. 1, rozumie się składanie tego podpisu w celu oświadczenia woli w swoim imieniu lub imieniu innej osoby fizycznej w celu załatwienia sprawy prywatnej, niezwiązanej z wykonywanym zawodem, prowadzoną działalnością gospodarczą lub działalnością osoby prawnej albo jednostki organizacyjnej nieposiadającej osobowości prawnej, który składający to oświadczenia reprezentuje.”.

Powiązanie więc tego podpisu z sferą życia prywatnego jednostki oraz jego nieodpłatność tym bardziej skłania do umożliwienia oparcia certyfikatu tego rozwiązania na identyfikatorze innym niż PESEL, co jest możliwe w przypadku komercyjnie dostępnych kwalifikowanych podpisów elektronicznych. Byłoby to wtedy narzędzie, którym mogłyby posługiwać się osoby, które nie chcą ujawniać swojego numeru PESEL poprzez użycie podpisu zaufanego i podpisu osobistego.

W ocenie organu nadzorczego rozwiązaniem najbardziej korzystnym byłoby **pozostawienie użytkownikowi wyboru jakie dane mają znaleźć się w certyfikacie kwalifikowanego podpisu elektronicznego zapewnianego przez ministra do spraw informatyzacji** (oczywiście w ramach wymogów rozporządzenia 910/2014). Projektodawca powinien precyzyjnie uregulować tą kwestię w ustawie określając **zamknięty katalog takich identyfikatorów, np. numer PESEL, numer paszportu, numer dowodu osobistego lub jeśli na takie rozwiązanie zdecyduje się projektodawca, numer powiązany z portfelem tożsamości cyfrowej**, o którym mowa w uwadze do art. 14a ust. 2 projektu ustawy.

Kwestia ta powinna zostać przeanalizowana **w ocenie skutków dla ochrony danych projektowanej ustawy** oraz oceniona z punktu widzenia z zasady zgodności z prawem, rzetelności i przejrzystości, ograniczenia celu, minimalizacji danych oraz rozliczalności. Jest to konieczne również dla zapewnienia ochrony numeru PESEL zgodnie z art. 87 rozporządzenia 2016/679.

7. Zgodnie z **art. 6 pkt 2** projektu ustawy, dodającym **art. 14f ust. 2** w ustawie z dnia 26 maja 2023 r. o aplikacji mObywatel: „Dokumenty elektroniczne opatrzone nieodpłatnym kwalifikowanym podpisem elektronicznym w celu innym niż profesjonalny oznacza się w sposób umożliwiający stwierdzenie użycia takiego podpisu”.

Projektowany przepis jest **niejasny**, nie wynika z niego **w jaki sposób należy oznaczać podpisany, czy przeznaczony do podpisu dokument, tak aby wiadomo było, że wykonany on jest w celu innym niż profesjonalny**. Wyjaśnienie tej kwestii jest konieczne z punktu widzenia zasady zgodności z prawem, rzetelności i przejrzystości i pewności obrotu prawnego.

8. Zgodnie z **art. 6 pkt 2** projektu ustawy, dodającym **art. 14h** w ustawie z dnia 26 maja 2023 r. o aplikacji mObywatel: „Rada Ministrów określi, w drodze rozporządzenia, zakres danych i wykaz rejestrów publicznych oraz systemów teleinformatycznych, z których użytkownik europejskiego portfela tożsamości cyfrowej, o którym mowa w art. 5a ust. 2 lit. a rozporządzenia 910/2014, może pobrać dane, oraz podmiotów publicznych prowadzących te rejestry publiczne i systemy teleinformatyczne, mając na uwadze adekwatność zakresu tych danych do potrzeb związanych z usługami świadczonymi w ramach europejskiego portfela tożsamości cyfrowej, o którym mowa w art. 5a ust. 2 lit. a rozporządzenia 910/2014, oraz uwarunkowania pozwalające na zapewnienie możliwości pobierania tych danych.”.

Należy rozważyć, czy materia, która miałaby być określona aktem wykonawczym, o którym mowa w projektowanym przepisie, nie powinna znaleźć się w ustawie. Zarówno zakres danych, jak i wykaz rejestrów powiązanych z europejskim portfelem tożsamości cyfrowej, zapewnianym przez ministra właściwego do spraw informatyzacji nie powinny być raczej ustalane rozporządzeniem, z uwagi na zasady konstytucyjne, w tym zasady praworządności, autonomii informacyjnej jednostki oraz ograniczania praw konstytucyjnych. Projektowane rozwiązanie ma charakter blankietowy i przez to dodatkowo wpływa negatywnie na przejrzystość wcześniej komentowanych przepisów projektu, dotyczących funkcjonowania europejskiego portfela tożsamości cyfrowej, zapewnianego przez ministra właściwego do spraw informatyzacji. Dotyczy to zakresu danych przetwarzanych w węźle krajowym, w związku z funkcjonowaniem tego portfela, zakresu danych identyfikacyjnych użytkownika oraz funkcjonalności jakie ma on zapewniać europejski portfel tożsamości cyfrowej, w szczególności w zakresie udostępniania atrybutów i funkcjonowania nieodpłatnego kwalifikowanego podpisu elektronicznego. Reasumując, konstrukcja projektowanego przepisu budzi wątpliwości co do zgodności z zasadami zgodności z prawem, rzetelności i przejrzystości, ograniczenia celu oraz zasadą minimalizacji danych.

Pragnę jednocześnie podkreślić, że uwagi organu nadzorczego przedstawiane w toku prac legislacyjnych mają charakter eksperckich wskazówek dla Projektodawcy, który podejmuje decyzję co do ostatecznego kształtu przyjmowanych przepisów i odpowiada za zapewnienie ich zgodności z przepisami o ochronie danych osobowych.

Łączę wyrazy szacunku,

Mirosław Wróblewski

Prezes Urzędu Ochrony Danych Osobowych

/ - dokument w postaci elektronicznej podpisany kwalifikowanym podpisem elektronicznym/