

| Tabela uwag zgłoszonych w ramach opiniowania do projektu ustawy o zmianie ustawy o usługach zaufania oraz identyfikacji elektronicznej oraz niektórych innych ustaw (UC122) | | | | |
|---|---|------------------------|---|--|
| Lp. | Jednostka redakcyjna, do której wnoszone są uwagi | Podmiot wnoszący uwagi | Zgłoszone uwagi | Stanowisko |
| 1. | Art. 1 pkt 5 w zakresie zmian w art. 21a | Prezes UODO | <p>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</p> | <p>Uwaga wyjaśniona</p> <p>Zmiany w art. 21a w zakresie przyłączenia systemu scentralizowanego do węzła krajowego identyfikacji elektronicznej wynikają z tego, że skoro istnieje rozwiązanie techniczno- organizacyjne, w ramach którego zapewniane jest już uwierzytelnianie transgraniczne z użyciem notyfikowanych środków identyfikacji elektronicznej, a jednocześnie zgodnie z art. 11a 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 (Dz. Urz. UE L 257 z 28.08.2014, str. 73,z późn. zm.), zwanego dalej „rozporządzeniem eIDAS”, działając jako strony ufające w odniesieniu do usług transgranicznych, państwa członkowskie zapewniają jednoznaczne dopasowywanie tożsamości osób fizycznych z użyciem notyfikowanych środków identyfikacji elektronicznej lub europejskich portfeli tożsamości cyfrowej, to oczywistym rozwiązaniem jest, aby wykorzystany został istniejący potencjał techniczno-organizacyjny.</p> <p>Celem systemu scentralizowanego jest jednoznaczne dopasowanie tożsamości w rozumieniu art. 3 pkt 55 oraz art. 11a rozporządzenie eIDAS jak również przepisów rozporządzenia wykonawczego Komisji (UE) 2025/846 z dnia 6 maja 2025 r. ustanawiającego zasady stosowania rozporządzenia Parlamentu Europejskiego i Rady (UE) nr 910/2014 w odniesieniu do transgranicznego dopasowywania tożsamości osób fizycznych (Dz. U. UE. L. z 2025 r. poz. 846), zwanego dalej „rozporządzeniem 2025/846”.</p> <p>Należy zaznaczyć że „dopasowywanie tożsamości” zgodnie z art. 3 pkt 55 rozporządzenia eIDAS oznacza proces, w którym dane identyfikujące osobę lub środki identyfikacji elektronicznej są dopasowywane lub przyporządkowywane do istniejącego konta należącego do tej samej osoby.</p> |

| | | | |
|--|--|--|---|
| | | <p>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) pieczęć.”. 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 tę 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</p> | <p>Projektowana ustawa nie dotyczy zakresu danych, które znajdują się w certyfikacie podpisów kwalifikowanych. Zmiana usuwająca obecny przepis art. 21a ust. 6 wymieniający wprost minimalny zakres danych wymieniony w rozporządzeniu wykonawczym 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.), zwanym dalej „rozporządzeniem 2015/1501”, i zastępująca go przepisem poszerzającym ten zakres danych o dane wskazane 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”, oraz imiona rodziców osób oraz numer dokumentu potwierdzającego tożsamość wynika z konieczności formalnego wskazania zakresu danych, jaki minister będzie faktycznie przetwarzał w związku z koniecznością realizacji dwóch zadań:</p> <ul style="list-style-type: none">- uwierzytelniania za pośrednictwem węzła,- zapewnienia dopasowania tożsamości. <p>Zakres danych wskazanych w załączniku do rozporządzenia 2024/2977 określa dane obligatoryjne oraz opcjonalne, jakie państwa członkowskie mogą ustanowić dla minimalnego zakresu danych identyfikacji osobę w europejskim portfelu tożsamości cyfrowej, co za tym idzie system scentralizowany, o którym mowa w art. 1 pkt 5 projektu ustawy (art. 21a projektowanej ustawy). Podobnie jak w przypadku rozporządzenia 1501/2015 jest to zakres ściśle określony. Uznano jednak, że nie ma powodu „przepisywać” tych zakresów do ustawy, tym bardziej że rozporządzenia wykonawcze mogą być nowelizowane.</p> <p>Nawet jeżeli system scentralizowany nie będzie potrzebował w zakresie danych identyfikujących osobę oznaczenia płci określonego zgodnie z szerokimi możliwościami określonymi w rozporządzeniu 2024/2977 albo numeru telefonu komórkowego, ale użytkownik portfela zagranicznego mimo to będzie usiłował przekazać takie dane w zestawie danych identyfikujących osobę, to nawet odrzucenie takich danych będzie oznaczało ich przetwarzanie. Należy podkreślić,</p> |
|--|--|--|---|

| | | | |
|--|--|--|---|
| | | <p>identyfikacji elektronicznej (o czym szerzej w uwagach do zmian wprowadzanych w ustawie o aplikacji mObywatel).</p> <p>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.</p> <p>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.</p> <p>Powstaje również pytanie w jaki sposób, w obecnie obowiązującym w</p> | <p>że zakresy danych wskazane w projekcie ustawy wskazują na dane identyfikujące osobę, jakie zostały wskazane w art. 2 ust. 3 i 4 rozporządzenia 2025/846. Tamże wskazuje się, że odpowiednio należy polegać na danych, o których mowa w rozporządzeniu wykonawczym (UE) 2024/2977, wraz z wszelkimi opcjonalnymi danymi, które są potrzebne do zapewnienia niepowtarzalności przedstawionego zbioru danych, w tym, w stosownych przypadkach, z dodatkowymi informacjami lub procedurami uzupełniającymi lub zestawie danych dotyczących osoby fizycznej określonymi w pkt 1 załącznika do rozporządzenia 2015/1501, w tym, w stosownych przypadkach, dodatkowymi informacjami lub procedurami uzupełniającymi.</p> <p>W związku z tym, jeżeli dopasowanie jest dokładne i jednoznaczne na podstawie ww. danych wraz zaproponowaną procedurą uzupełniającą dopasowanie uważa się za skuteczne.</p> <p>Podsumowując – celem scentralizowanego systemu dopasowania tożsamości jest:</p> <ul style="list-style-type: none"> a) wstępne ustalenie czy osoba fizyczna używająca zagranicznego środka identyfikacji elektronicznej (czyli jednoznacznie zidentyfikowana czego gwarantem jest państwo członkowskie UE) miała nadany nr PESEL i jaki to numer, co pozwoli na jednoznaczną jej identyfikację w Polsce bez potrzeby weryfikacji dokumentów tożsamości, b) przesłanie danych (za zgodą tej osoby) do końcowej strony ufającej z ustalonym nr PESEL lub w przypadku niedopasowania do rejestru PESEL – danych identyfikujących osobę przekazywanych transgranicznie. <p>Celem tych przepisów nie jest weryfikacja w każdym przypadku serii i numeru dokumentu tożsamości, daty ważności dokumentu oraz miejsca i kraju urodzenia.</p> <p>Odnosząc się do uwagi dotyczącej dodatkowej identyfikacji za pomocą imion rodziców należy wyjaśnić, że jest to wyłącznie dodatkowa identyfikacja celem dopasowania do danych w rejestrze PESEL i dotyczy danych osoby, której tożsamość już została zidentyfikowana, ale nie ma pewności, czy jest to ta sama osoba, której dane zostały wpisane do ewidencji ludności. Rezygnacja z tej opcji może utrudnić lub nawet uniemożliwić licznym przedstawicielom Polonii skorzystanie z usług online w Polsce, którzy zapomnieli przez lata spędzone poza ojczyzną, jaki mieli nadany nr PESEL.</p> <p>W tym miejscu należy ponownie podkreślić, że mimo, iż zestawy danych identyfikujących osobę, o których mowa w rozporządzeniach</p> |
|--|--|--|---|

| | | | | |
|--|--|--|--|--|
| | | | <p>Polsce stanie prawnym uwierzytelnienie w węzle 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.”.</p> <p>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 pozwala 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 rozporządzeniem 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). Uprawdopodobnia tą sytuację</p> | <p>1501/2015 oraz 2024/2977, jednoznacznie identyfikują osobę, to nie chodzi tylko o tę identyfikację. Nawet bowiem, jeżeli środek identyfikacji elektronicznej użyty w systemie dopasowywania tożsamości będzie zawierał imię, nazwisko, datę urodzenia i miejsce urodzenia zgodne z danymi w rejestrze PESEL, nie będzie można z całkowitą pewnością ustalić, czy jest to jedna i ta sama osoba. Podanie imienia rodzica nie służy zatem identyfikacji osoby fizycznej, gdyż ta została już dokonana, ale wyłącznie do dopasowania do danych w ewidencji ludności, w której imiona rodziców to dane obowiązkowo przechowywane.</p> |
|--|--|--|--|--|

| | | | | |
|----|--|--------------------------|---|---|
| | | | 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. | |
| 2. | Art. 1 pkt 6 w zakresie art. 21aa | Rada do Spraw Cyfryzacji | <p>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).</p> <p>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.</p> <p>7. Udostępnienie historii użycia wymaga zastosowania uwierzytelnienia wieloskładnikowego oraz mechanizmów ograniczających ryzyko nieuprawnionego dostępu.”</p> | <p>Uwaga wyjaśniona</p> <p>W przypadku braku wskazania w przepisach sektorowych zastosowanie znajdują przepisy § 20 rozporządzenia Rady Ministrów z dnia 21 maja 2024 r. w sprawie Krajowych Ram Interoperacyjności, minimalnych wymagań dla rejestrów publicznych i wymiany informacji w postaci elektronicznej oraz minimalnych wymagań dla systemów teleinformatycznych (Dz. U. poz. 773).</p> <p>Projektowane przepisy wyraźnie wskazują w art. 21aa ust. 3, że dane, o których mowa w ust. 2, udostępniane są wyłącznie użytkownikowi, którego dane dotyczą, po uwierzytelnieniu z wykorzystaniem środka identyfikacji elektronicznej wydanego w systemie identyfikacji elektronicznej przyłączonym do węzła krajowego identyfikacji elektronicznej, zapewniającego wysoki poziom bezpieczeństwa, a zatem zapewniany będzie najwyższy możliwy poziom bezpieczeństwa. Użytkownik nie może żądać ani sprostowania ani ograniczenia zbieranie logów, gdyż obowiązki te wynikają z odrębnych przepisów. Automatycznie zbierane logi systemowe nie mają znaczenia dla przestępców w przypadku hipotetycznego przejęcia przez nich środka identyfikacji elektronicznej (że zapoznają się z logami), tylko dla potencjalnych poszkodowanych, którzy będą chcieli się dowiedzieć w jakich interakcjach były używane przejęte przez przestępców środki identyfikacji elektronicznej.</p> |
| 3. | Art. 1 pkt 6 w zakresie art. 21aa | Prezes UODO | 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. | <p>Uwaga wyjaśniona</p> <p>W przypadku braku wskazania w przepisach sektorowych zastosowanie znajdują przepisy § 20 rozporządzenia Rady Ministrów z dnia 21 maja 2024 r. w sprawie Krajowych Ram Interoperacyjności, minimalnych wymagań dla rejestrów publicznych i wymiany informacji w postaci elektronicznej oraz minimalnych wymagań dla systemów teleinformatycznych (Dz. U. poz. 773).</p> |
| 4. | Art. 1 pkt 6 w zakresie art. 21aa ust. 4 | Prezes UODO | 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 | <p>Uwaga wyjaśniona</p> <p>Jest to funkcjonalność usługi, z której może, ale nie musi skorzystać użytkownik. Opatrzanie dokumentu zaawansowaną pieczęcią</p> |

| | | | | |
|----|---|-------------|--|---|
| | | | 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. | elektroniczną weryfikowaną za pomocą kwalifikowanego certyfikatu ministra właściwego do spraw informatyzacji co do zasady służy do potwierdzenia i zachowania integralności danych zawartych w dokumencie. |
| 5. | Art. 1 pkt 9 w zakresie art. 22a ust. 1 i 2 | Prezes UODO | <p>1. Projektowany przepis powinien określać wszystkie funkcjonalności systemu scentralizowanego, ze względu na zakres i cel przetwarzania danych w tym systemie.</p> <p>2. Konieczne jest również wprowadzenie zmian wynikowych (tzw. „lustrzanych”) w poszczególnych ustawach regulujących funkcjonowanie tych systemów teleinformatycznych, których część będzie miało charakter rejestrów publicznych.</p> | <p>Uwaga wyjaśniona</p> <p>Celem systemu scentralizowanego jest jednoznaczne dopasowanie tożsamości w rozumieniu art. 3 pkt 55 oraz art. 11a rozporządzenie eIDAS jak również przepisów rozporządzenia wykonawcze Komisji (UE) 2025/846 z dnia 6 maja 2025 r. ustanawiające zasady stosowania rozporządzenia Parlamentu Europejskiego i Rady (UE) nr 910/2014 w odniesieniu do transgranicznego dopasowywania tożsamości osób fizycznych (Dz. U. UE. L. z 2025 r. poz. 846)</p> <p>Należy zaznaczyć, że "dopasowywanie tożsamości" zgodnie z art. 3 pkt 55 eIDAS oznacza proces, w którym dane identyfikujące osobę lub środki identyfikacji elektronicznej są dopasowywane lub przyporządkowywane do istniejącego konta należącego do tej samej osoby. Przepis ustawy precyzuje wszystkie procesy i zakres danych. Uwaga niezrozumiała, co do zasady użytkownikom transgranicznym należy zapewnić dostęp do usług publicznych za pomocą notyfikowanych środków identyfikacji elektronicznej oraz europejskich portfeli tożsamości cyfrowej.</p> |
| 6. | Art. 1 pkt 9 w zakresie art. 22a ust. 2 pkt 2 | Prezes UODO | W projektowanym 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). | <p>Uwaga uwzględniona</p> <p>W art. 22a ust. 2 pkt 2 poprawiono na odwołanie.</p> |
| 7. | Art. 1 pkt 9 w zakresie art. 22a ust. 2 pkt 3 | Prezes UODO | 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. | <p>Uwaga wyjaśniona</p> <p>Maksymalny okres przechowywania wyników dopasowania tożsamości realizowanego na podstawie rozporządzenia wykonawczego Komisji (UE) 2025/846 został ustalony w art. 5 ust. 3 tego rozporządzenia.</p> <p>Zgodnie z art. 11a rozporządzenia eIDAS „Działając jako strony ufające w odniesieniu do usług transgranicznych, państwa członkowskie zapewniają jednoznaczne dopasowywanie tożsamości osób fizycznych z użyciem notyfikowanych środków identyfikacji elektronicznej lub europejskich portfeli tożsamości cyfrowej”, czyli dopasowywanie tożsamości jest obowiązkiem nałożonym na państwa członkowskie który zgodnie z art. 2 ust. 1 rozporządzenie wykonawczego Komisji (UE) 2025/846 dotyczy usług online oferowanych przez podmiot sektora publicznego lub w jego imieniu.</p> <p>Każdy użytkownik europejskiego portfela tożsamości cyfrowej będzie informowany o stronie ufającej jakiej ma przekazać dane w oparciu o</p> |

| | | | | |
|-----|--|-------------|--|--|
| | | | | <p>certyfi­kat dostę­pu i cer­tyfi­kat re­jes­tracji stronu ufają­cej portfe­la – w przy­padku sys­te­mu do­pa­so­wy­wa­nia toż­sa­mo­ści rów­nie­ż. Bę­dzie za­tem wie­dział komu prze­ka­zu­je da­ne i bę­dzie mógł ich nie prze­ka­zać. W ta­kiej sy­tuacji nie skor­zy­sta z usłu­gi on­line.</p> |
| 8. | Art. 1 pkt 9 w za­kresie art. 22a ust. 4 pkt 1 i 2 | Prezes UODO | <p>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.</p> | <p>Uwaga wyjaśniona</p> <p>Nie można zgodzić się z tezą, że system scentralizowany jest oparty na nr PESEL. Opiera się on na danych uzyskiwanych z notyfikowanych środków identyfikacji elektronicznej europejskich portfeli tożsamości cyfrowej i rejestrze PESEL którego nr PESEL jest tylko częścią. Numer PESEL nie będzie ostatecznie potwierdzać tożsamości użytkownika europejskiego portfela tożsamości cyfrowej w systemie scentralizowanym, gdyż tożsamość ta będzie potwierdzana środkami identyfikacji elektronicznej, które co do zasady nr PESEL nie zawierają. Cel wstępnej weryfikacji danych w rejestrze PESEL został wyjaśniony w uzasadnieniu.</p> <p>Zgodnie z postulatem ocena skutków dla ochrony danych projektowanej ustawy została przeprowadzona.</p> |
| 9. | Art. 1 pkt 9 w za­kresie art. 22a ust. 6 | Prezes UODO | <p>Projektowany przepis jest niejasny, gdyż nie określa tego formatu danych, nie zawiera również odesłania do innych przepisów ustawy regulujących tą materię.</p> | <p>Uwaga wyjaśniona</p> <p>Węzeł krajowy identyfikacji elektronicznej jest zintegrowany z węzłem transgranicznym, o którym mowa w art. 12 ust. 8 rozporządzenia 910/2014, więc formaty danych muszą być zgodne ze specyfikacją “eIDAS eID Profile” ogłoszoną pod adresem https://ec.europa.eu/digital-building-blocks/sites/spaces/DIGITAL/pages/467109280/eIDAS+eID+Profile udostępniona przez Komisję Europejską zgodnie z rozporządzeniem wykonawczym Komisji (UE) 2015/1501</p> |
| 10. | Art. 1 pkt 9 w za­kresie art. 22b ust. 1 pkt 5 i 6 oraz OSR | Prezes UODO | <p>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. 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.</p> <p>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</p> | <p>Uwaga wyjaśniona</p> <p>Przyjęte rozwiązanie wynikają z przepisów europejskich. Wszystkie europejskie portfele tożsamości cyfrowej będą w taki sam sposób technicznie zorganizowane, jeżeli chodzi o ich podstawowe funkcje –zgodnie z rozporządzeniem wykonawczym Komisji (UE) 2024/2979 z dnia 28 listopada 2024 r. ustanawiające zasady stosowania rozporządzenia Parlamentu Europejskiego i Rady (UE) nr 910/2014 w odniesieniu do integralności i podstawowych funkcji europejskich portfeli tożsamości cyfrowej (Dz. U. UE. L. z 2024 r. poz. 2979). W związku z powyższym zgodnie z Rozporządzeniem Parlamentu Europejskiego i Rady (UE) 2016/679 oraz – w stosownych przypadkach – dyrektywa 2002/58/WE Parlamentu Europejskiego i Rady mają zastosowanie do wszystkich czynności przetwarzania danych osobowych na podstawie rozporządzenia (UE) nr 910/2014.</p> |

| | | | |
|--|--|---|--|
| | | <p>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 celu i minimalizacji danych. (...)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. (...)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.</p> <p>Ocena skutków regulacji projektowanej ustawy nie wskazuje organu nadzorczego wśród podmiotów, na które oddziałuje projekt, nie zakłada się również, żadnych dodatkowych środków finansowych i</p> | <p>Zarówno konstrukcja rejestru stron ufających, jak i procedura zgłaszania naruszeń danych osobowych przez użytkowników europejskich portfeli tożsamości cyfrowej zostały uregulowane na poziomie unijnym odpowiednio w art. 5b rozporządzenia eIDAS oraz z rozporządzeniu wykonawczym (UE) 2025/848 z dnia 6 maja 2025 r. ustanawiające zasady stosowania rozporządzenia Parlamentu Europejskiego i Rady (UE) nr 910/2014 w odniesieniu do rejestracji stron ufających portfela (Dz. U. UE. L. z 2025 r. poz. 848).</p> <p>W odniesieniu do uzyskiwania wpisu do rejestru stron ufających, zgodnie z motywem 17 rozporządzenia Parlamentu Europejskiego i Rady (UE) nr 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. U. UE. L. z 2024 r. poz. 1183): "Aby zapewnić jej upowszechnienie wśród usługodawców, rejestracja powinna być efektywna kosztowo oraz proporcjonalna względem odnośnych zagrożeń. W tym kontekście rejestracja powinna przewidywać stosowanie zautomatyzowanych procedur, w tym poleganie na istniejących rejestrach i korzystanie z nich przez państwa członkowskie, oraz nie powinna wiązać się z procesem uzyskiwania wstępnego zezwolenia." Legislacja unijna wykluczył zatem prowadzenie postępowania administracyjnego przed uzyskaniem wpisu do rejestru stron ufających.</p> <p>Obowiązek zapewnienia użytkownikom europejskich portfeli tożsamości cyfrowych wygodnej usługi zgłaszania naruszeń ochrony danych osobowych przez strony ufające organowi nadzorczemu wynika z art. 5a ust. 4 lit. d pkt (iii) oraz ust. 5 lit. a pkt (x) rozporządzenia 910/2014.</p> <p>OSR została odpowiednio zmieniona.</p> |
|--|--|---|--|

| | | | | |
|-----|---|--------------------------|--|---|
| | | | 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 nadzorcemu w opisywanym trybie. | |
| 11. | Art. 1 pkt 9 w zakresie art. 22b ust. 10 | Rada do Spraw Cyfryzacji | <p>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).</p> <p>Propozycja:</p> <p>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.”;</p> <p>b) Alternatywnie: utrzymać „zwrot”, ale np. dodać: „Na czynności, o których mowa w ust. 11, przysługuje skarga do sądu administracyjnego.”</p> | <p>Uwaga nieuwzględniona</p> <p>Zgodnie z art. 5b ust. 2 zdanie pierwsze rozporządzenia eIDAS „Proces rejestracji musi być efektywny kosztowo i proporcjonalny względem zagrożeń.”</p> <p>Dlatego też zakłada się, że „wpis do rejestru następuje po zweryfikowaniu kompletności danych zawartych we wniosku”.</p> <p>Oznacza to, że wpis nie podlega żadnej ocenie merytorycznej – jeżeli jest kompletny, a dane są zgodne z odpowiednimi rejestrami, wpis jest realizowany. Jeżeli jest niekompletny, to znaczy, że zawiera braki formalne.</p> |
| 12. | Art. 1 pkt 9 w zakresie art. 22b ust. 15 i 16 | Prezes UODO | 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. | <p>Uwaga nieuwzględniona</p> <p>Polityki są dokumentem technicznym ustalającym zasady bezpieczeństwa i w związku z tym wymagane jest, aby można je było na bieżąco aktualizować. W przypadku zamieszczenia ich w aktach wykonawczych do ustawy, możliwość ich aktualizacji byłaby nadmiernie ograniczona.</p> |
| 13. | Art. 1 pkt 9 w zakresie art. 22c | Prezes UODO | 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 poświadczenia 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 | <p>Uwaga wyjaśniona</p> <p>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 szczególnego przepisu ustawowego wymagającego udostępnienia określonego źródła. Mogłoby to w zasadniczy sposób utrudnić albo wręcz uniemożliwić</p> |

| | | | | |
|-----|--------------------------------------|--------------------------|--|--|
| | | | <p>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.</p> <p>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.</p> | <p>wydawanie kwalifikowanych elektronicznych poświadczeń atrybutów, co byłoby niezgodne z ogólnymi celami europejskich ram tożsamości cyfrowej.</p> <p>Warto wyjaśnić również, że zgodnie z projektowanym art. 22c ust. 1 podmioty publiczne odpowiedzialne na poziomie krajowym za źródła autentyczne (...) zapewniają kwalifikowanym dostawcom usług zaufania (...) możliwość weryfikacji tych atrybutów drogą elektroniczną, na żądanie użytkownika, zgodnie z art. art. 45e ust. 1 eIDAS2.</p> <p>Oznacza to, że każdy podmiot publiczny będący źródłem autentycznym (zarówno w zakresie atrybutów wskazanych w załączniku VI do rozporządzenia eIDAS2, jak i innych atrybutów wynikających z prawa krajowego) będzie zobowiązany do Udostępnienia elektronicznego punktu weryfikacji – umożliwiającego kwalifikowanym dostawcom usług zaufania sprawdzenie autentyczności atrybutu użytkownika – zgodnie z przepisem art. 9 ust. 1–5 rozporządzenia 2025/1569, tj.: umożliwiającego złożenie elektronicznego wniosku o weryfikację atrybutu, dostępnego w sposób zautomatyzowany, działającego w oparciu o środki elektroniczne nadające się do automatycznego przetwarzania.</p> <p>Zapewnienia mechanizmu odpowiedzi w formie binarnej („tak/nie”) – bez ujawniania wartości atrybutu – z obowiązkowym wskazaniem podmiotu publicznego będącego źródłem autentycznym, zgodnie z art. 9 ust. 4 rozporządzenia 2025/1569.</p> |
| 14. | Art. 1 pkt 9 w zakresie art. 22f–22h | Rada do Spraw Cyfryzacji | <p>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”).</p> <p>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, rolę administratora/podmiotu przetwarzającego (RODO), zasady odpowiedzialności, okresy retencji, tryb audytu i zasady reagowania na incydenty.”</p> | <p>Uwaga częściowo uwzględniona</p> <p>Z projektowanego art. 22h ustawy o usługach zaufania oraz identyfikacji elektronicznej wynika, że minister właściwy do spraw informatyzacji wydaje elektroniczne poświadczenia atrybutów na wniosek podmiotu odpowiedzialnego za źródła autentyczne lub dostawcy usługi online wpisanego do rejestru stron ufających europejskiemu portfelowi tożsamości cyfrowej. Zgodnie z art. 22h ust. 2 pkt 2 lit. a wniosek taki ma zawierać między innymi „odniesienie do przepisów, norm lub wytycznych, jeżeli mają zastosowanie”.</p> <p>Tym niemniej w związku z tą uwagą dodano przepisy jednoznacznie wskazujące w jakie formalne wymogi muszą spełnić podmioty publiczne odpowiedzialne za źródła autentyczne, aby mogły same</p> |

| | | | | |
|-----|---|--------------------------|--|--|
| | | | | wydawać elektroniczne poświadczenia atrybutów w oparciu o źródła, którymi zarządzają. |
| 15. | Art. 1 pkt 9 w zakresie art. 22g ust. 1 | Rada do Spraw Cyfryzacji | 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.); | Uwaga uwzględniona Wprowadzono odpowiednie zmiany. |
| 16. | Art. 1 pkt 11 w zakresie art. 23 pkt 2 | Prezes UODO | 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. | Uwaga uwzględniona Wprowadzono zmiany w art. 23 pkt 2 dodano informację, że minister udostępnia kod źródłowy w Biuletynie Informacji Publicznej na swojej stronie podmiotowej. |
| 17. | Art. 1 pkt 11 w zakresie art. 23 pkt 2 | Rada do Spraw Cyfryzacji | 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.” | Uwaga zostanie częściowo uwzględniona (zdanie pierwsze) Określanie warunków licencji w związku z przepisem art. 5a ust. 3 eIDAS nie jest potrzebne. Kod źródłowy komponentów oprogramowania użytkowego europejskich portfeli tożsamości cyfrowej musi być objęty licencją otwartego oprogramowania. Państwa członkowskie mogą postanowić, że z należyte uzasadnionych powodów nie ujawnia się kodu źródłowego poszczególnych komponentów innych niż zainstalowane na urządzeniach użytkownika |
| 18. | Art. 1 pkt 14 w zakresie art. 24a | Prezes UODO | 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 któregośkolwiek 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. | Uwaga wyjaśniona/uwzględniona Sformułowanie wynika z art. 5a ust. 2 rozporządzenia 910/2014, zgodnie z którym europejskie portfele tożsamości cyfrowej muszą być zapewniane w co najmniej jeden z następujących sposobów: a) bezpośrednio przez państwo członkowskie; b) na podstawie upoważnienia od państwa członkowskiego; c) niezależnie od państwa członkowskiego, lecz uznawane przez to państwo członkowskie. Przepis został zmodyfikowany przez wskazanie, że dostawca rozwiązania składa wnioski do ministra właściwego do spraw informatyzacji o uznanie rozwiązania jako europejskiego portfela tożsamości cyfrowej, o którym mowa w art. 5a ust. 2 lit. c rozporządzenia 910/2014. |
| 19. | Art. 2 | GUS | W art. 2 projekt zakłada zmiany w ustawie z dnia 29 czerwca 1995 r. o statystyce publicznej (Dz. U. z 2024 r. poz. 1799 oraz z 2025 r. poz. 1792) | Uwaga uwzględniona |

| | | | | |
|--|--|--|--|--|
| | | | <p>poprzez:</p> <p>1) dodanie do art. 42 ustawy o statystyce publicznej ust. 7a: „7a. Złożenie wniosku o zmianę cech objętych wpisem oraz wniosku o skreślenie z rejestru podmiotów dla podmiotów, o których mowa w art. 10a ust. 3 ustawy z dnia 18 listopada 2020 r. o doręczeniach elektronicznych (Dz. U. z 2026 r. poz. 3), może nastąpić również na podstawie przepisów ustawy z dnia 18 listopada 2020 r. o doręczeniach elektronicznych.”.</p> <p>Należy zwrócić uwagę, że 31 grudnia 2025 r. weszła w życie ustawa z dnia 21 listopada 2025 r. o zmianie ustawy o statystyce publicznej oraz niektórych innych ustaw, która wprowadziła zmiany m.in. w zakresie dotyczącym rejestru REGON. Obecnie właściwe jest sformułowanie „rejestr REGON” zamiast „rejestr podmiotów”.</p> <p>Wskazanie w projektowanym art. 42 ust. 7a na art. 10a ust. 3 wydaje się nadmiarowe (w art. 10a ust. 3 pkt 2-3 wskazane są dane nieobjęte wpisem do rejestru REGON).</p> <p>Wskazanie to powinno odnosić się do definicji podmiotu publicznego zawartego w ustawie o doręczeniach elektronicznych, doprecyzowanej o podmioty niepubliczne realizujące zadania publiczne.</p> <p>Ponadto projektowany ust. 7a wyznacza możliwość złożenia wniosku o zmianę cech objętych wpisem oraz wniosku o skreślenie z rejestru dla podmiotów publicznych i podmiotów niepublicznych realizujących zadania publiczne.</p> <p>Wynika z tego, że wpis do rejestru REGON przedmiotowych podmiotów następował by nadal w trybach wskazanych w ustawie o statystyce publicznej, a aktualizacja cech podlegających wpisowi do Katalogu Podmiotów Publicznych (KPP)/wykreślenie wpisu z rejestru REGON następowało by na podstawie danych przekazywanych z KPP.</p> <p>Należy jednak zauważyć, że część podmiotów/cech, podlegających wpisowi do rejestru REGON i KPP, jest zgodnie z obowiązującymi przepisami wpisywana do rejestru REGON na podstawie danych przekazanych z KRS/RSPO/CRP KEP – w związku z czym należałoby wyłączyć możliwość dokonywania aktualizacji/skreśleń w oparciu o dane KPP w przypadkach uregulowanych w art. 42 ust. 3a, ust. 6a, ust. 7, ust. 11, ust. 14.</p> <p>Projekt powinien precyzyjnie określać tryb oraz zakres cech aktualizowanych przez podmioty publiczne i niepubliczne realizujących zadania publiczne w rejestrze REGON za pośrednictwem KPP. W szczególności w sposób jednoznaczny powinien wskazywać, która ścieżka aktualizacji - przez rejestr REGON czy przez KPP - znajduje zastosowanie w</p> | <p>Przepis art. 42 ust. 7a i 8a został wykreślony w związku z rezygnacją z mechanizmu zmiany danych w REGON z poziomu KPP.</p> |
|--|--|--|--|--|

| | | | | |
|-----|---|-------------|---|--|
| | | | <p>danym przypadku.</p> <p>Podmioty wpisane do KRS składają do rejestru REGON jedynie wnioski dotyczące ich jednostek lokalnych - w odniesieniu do podmiotu wpisanego do KRS, wpis/zmiana/skreślenie następuje na podstawie danych przekazanych z KRS oraz danych uzupełniających przekazanych z CRP KEP. W przypadku gdy podmiotem realizującym zadania publiczne jest podmiot wpisany do KRS – wpis/zmiana w zakresie cech wskazanych ustawą o statystyce publicznej następuje na podstawie danych z KRS. Dane uzupełniające natomiast – na podstawie danych z CRP KEP (podmioty zobowiązane są składać NIP-8).</p> <p>2) dodanie do art. 42 ust. 8a:</p> <p>„8a. Przepisu ust. 7 i 7a nie stosuje się również, jeżeli zmiana dotyczy jedynie cech objętych wpisem, niebędących przedmiotem wpisu w Katalogu Podmiotów Publicznych, o którym mowa w art. 10a ust. 3 ustawy z dnia 18 listopada 2020 r. o doręczeniach elektronicznych.”.</p> <p>Wskazanie na ust. 7 wymaga wyjaśnienia - wskazujemy, że ust. 7 stanowi o trybie wpisu zmiany/skreślenia podmiotów wpisanych w CEIDG (w tym przypadku do rejestru REGON wpływa pełny zakres danych i informacji) i RSPO (w przypadku RSPO obowiązuje ust. 8 umożliwiający podmiotom wpisanym do RSPO złożenie wniosku do rejestru REGON w zakresie informacji niebędących przedmiotem wpisu w RSPO).</p> | |
| 20. | Art. 3 pkt 4 lit. b w zakresie art 20ad ust. 1b | Prezes UODO | <p>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 podmiotu 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.</p> | <p>Uwaga uwzględniona</p> <p>Z katalogu danych, które zawierać będzie profil zaufany osoby fizycznej reprezentującej podmiot publiczny (art. 20ad ust. 1b ustawy o informatyzacji działalności podmiotów realizujących zadania publiczne), usunięto datę urodzenia. Dla zapewnienia jednoznacznej identyfikacji zdecydowano się na dodanie do tego katalogu identyfikatora profilu osoby fizycznej powiązanego z tym profilem zaufanym.</p> <p>Dla zachowania spójności ustawy w przepisach określających, jakie dane osobowe przetwarza minister w związku z zapewnianiem nowych środków identyfikacji również dodano tę daną (art. 20ac ust. 2 pkt 1b i 1c ww. ustawy).</p> |
| 21. | Art. 4 pkt 1 w zakresie art. 3 pkt 14 | Prezes UODO | <p>(...) dla pełnego zachowania zasad przetwarzania danych osobowych określonych w rozporządzeniu 2016/679 konieczne jest ponownie dokonanie analizy katalogu danych jakie będą przetwarzane w nowych profilach zaufanych, jak również zasad posługiwania się nimi</p> | <p>Uwaga uwzględniona</p> <p>Analiza została przeprowadzona, a jej wyniki uwzględnione w ocenie skutków dla ochrony danych projektowanej ustawy.</p> |
| 22. | Art. 4 pkt 3 w zakresie art 20ac pkt 1a – 1d | Prezes UODO | <p>Wśród danych osób, o których mowa w punktach 1b i 1c pomimo, że są to osoby pełniące określone funkcje (osoby reprezentujące podmiot publiczny, osoby pełniące funkcję administratora profilu zaufanego</p> | <p>Uwaga wyjaśniona</p> <p>Profil zaufany jest środkiem identyfikacji elektronicznej, co za tym idzie podlega w tym zakresie przepisom rozporządzenia</p> |

| | | | | |
|-----|---|-------------|--|--|
| | | | <p>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.</p> | <p>wykonawczego Komisji (UE) 2015/1502 z dnia 8 września 2015 r. w sprawie ustanowienia minimalnych specyfikacji technicznych i procedur dotyczących poziomów zaufania w zakresie środków identyfikacji elektronicznej na podstawie art. 8 ust. 3 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. U. UE. L. z 2015 r. Nr 235, str. 7, z późn. zm.).</p> <p>W tym akcie prawnym w części 2.1.4 załącznika wskazuje się wymagania dotyczące powiązanie między środkami identyfikacji elektronicznej osób fizycznych i prawnych jakie powinny mieć miejsce „w stosownych przypadkach”. Takim właśnie stosownym przypadkiem będzie powiązanie, o którym mowa w projektowanych nowych przepisach.</p> <p>Zatem nr PESEL jest daną przewarzaną w systemie, ale nie będzie przekazywany do dostawcy usługi.</p> <p>Wykorzystywanie numeru PESEL w ramach profilu zaufanego jest przemyślanym i celowym działaniem. Należy bowiem wskazać, że na gruncie polskiego prawa numer PESEL to podstawowy i najważniejszy identyfikator osoby fizycznej, który uregulowany został w ustawie o ewidencji ludności. Identyfikator ten stanowi element szeregu dokumentów tożsamości oraz dokumentów dotyczących sytuacji prawnej lub praw przysługujących ich posiadaczowi. Zgodnie minimalnymi wymaganiami dla systemów teleinformatycznych, szerzej opisanymi w dalszej części niniejszego stanowiska, podmioty publiczne mają obowiązek stosowania numeru PESEL jako identyfikatora osoby fizycznej w prowadzonych przez siebie rejestrach publicznych. W kontekście powyższego należy wskazać, że numer PESEL jest najbardziej powszechnym i skutecznym identyfikatorem, który poza unikalną identyfikacją osoby fizycznej pozwala także na powiązanie identyfikowanej osoby z szeregiem dotyczących jej dokumentów oraz opisujących tę osobę danych, które przetwarzane są w rejestrach publicznych.</p> |
| 23. | Art. 4 pkt 4 lit. d w zakresie art 20ad ust. 2a | Prezes UODO | <p>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.</p> | <p>Uwaga wyjaśniona</p> <p>Szerokie uzasadnienie i wyjaśnienie zakresu przetwarzania numeru PESEL do celów wydawania profili zaufanych osób fizycznych reprezentującej osobę prawną zostały zawarte powyżej (uwaga do art. 4 pkt 3).</p> |

| | | | | |
|-----|--|-------------|---|---|
| 24. | Art. 4 pkt 6 w zakresie art 20cc i art. 22cd | Prezes UODO | W wyniku przyjęcia projektowanego rozwiązania dojdzie do łączenia danych związanych z aktywnością zawodową z danymi o charakterze osobistym. Jest to niezgodne z: zgodności z prawem, rzetelności i przejrzystości, ograniczenia celu oraz minimalizacji danych. | <p>Uwaga wyjaśniona</p> <p>W profilu zaufanym osoby fizycznej reprezentującej osobę prawną zawarte są dane niezbędne do jednoznacznej identyfikacji tej osoby fizycznej i prawnej oraz informacje niezbędne do bezpiecznego uwierzytelnienia w usłudze online osoby posługującej się tym środkiem identyfikacji elektronicznej.</p> <p>Zgodnie z pkt 2.1.4 załącznika do rozporządzenia wykonawczego Komisji (UE) 2015/1502 wskazuje się wymagania dotyczące powiązanie między środkami identyfikacji elektronicznej osób fizycznych i prawnych jakie powinny mieć miejsce „w stosownych przypadkach”. Zatem owiązanie środków identyfikacji elektronicznej osób fizycznych i prawnych nie jest niezgodne zasadami dotyczącymi przetwarzania danych osobowych.</p> <p>Nie jest również jasne, w jakim zakresie połączenie tych danych miałyby naruszać wymienione w uwadze zasady.</p> |
| 25. | Art. 5 | GUS | Odnośnie do krajowego rejestru urzędowego podziału terytorialnego kraju (TERYT), w art. 5 wprowadzającym zmiany w ustawie o doręczeniach elektronicznych, w zakresie projektowanego art. 10c – przepis ten stanowi, że Minister właściwy do spraw informatyzacji może wprowadzać, wycofywać lub aktualizować dane, o których mowa w art. 10a ust. 3 pkt 1 lit. a, g-i, n, o, t, u, x, y oraz z, o podmiotach publicznych oraz o podmiotach niepublicznych realizujących zadania publiczne na podstawie danych pochodzących z rejestrów publicznych lub na podstawie danych, w których posiadaniu jest minister właściwy do spraw informatyzacji pochodzących z systemów teleinformatycznych prowadzonych przez tego ministra, a także prostować oczywiste błędy i omyłki pisarskie. Z uwagi na planowane gromadzenie w Katalogu Podmiotów Publicznych danych pochodzących z rejestru TERYT (identyfikatory i nazwy obiektów) proponujemy uwzględnienie tych danych wśród danych możliwych do aktualizacji przez Ministra właściwego ds. informatyzacji (lit. p, q, r – w przypadku uwzględnienia uwagi GUS lp. 1). Identyfikatory i nazwy jednostek podziału terytorialnego, miejscowości i ulic podlegają bieżącej aktualizacji w rejestrze TERYT, a informacja o dokonanych zmianach w postaci plików aktualizacyjnych jest udostępniana poprzez usługę sieciową; ponadto zgodnie z rozporządzeniem w sprawie rejestru TERYT organy prowadzące urzędowe rejestry i systemy informacyjne administracji publicznej są obowiązane do wprowadzania zmian w identyfikatorach po ich każdorazowej aktualizacji w tym rejestrze, obowiązek ten został również uwzględniony w aktualnie procedowanej ustawie zmieniającej ustawę o statystyce publicznej. | <p>Uwaga uwzględniona</p> <p>Wprowadzono zmiany w art. 10c.</p> |

| | | | | |
|-----|--------|-----|---|---|
| | | | <p>Analogiczna uwaga została zgłoszona przez GUS do projektu ustawy o zmianie ustawy o doręczeniach elektronicznych oraz niektórych innych ustaw (projekt z dnia 21.08.2025 r.). W odniesieniu do zgłoszonej przez GUS uwagi Ministerstwo Cyfryzacji wskazało, że dane z rejestru TERYT będą pobierane „na bieżąco” przez ministra właściwego do spraw informatyzacji na podstawie art. 10b projektowanej ustawy i nie ma konieczności zmiany art. 10c w opisanym zakresie. Wskazane działanie wydaje się jednak niewystarczające, gdyż pominięcie w tym przepisie danych z rejestru TERYT jako danych podlegających aktualizacji wskazuje, że pobieranie danych „na bieżąco” będzie dotyczyć tylko pozyskiwania plików pełnych służących do aktualizacji słowników w KPP, które będą wykorzystywane tylko do bieżącej rejestracji podmiotów, a nie aktualizacji danych adresowych podmiotów już zarejestrowanych w tym katalogu, w przypadku wprowadzenia zmian w rejestrze TERYT.</p> | |
| 26. | Art. 5 | GUS | <p>W art. 5 projekt zakłada zmiany w ustawie z dnia 18 listopada 2020 r. o doręczeniach elektronicznych (Dz. U. z 2026 r. poz. 3):</p> <p>1) art. 10a ust. 3 (zakres przedmiotowy KPP).</p> <p>Rozważenia wymaga kwestia zakresu przedmiotowego KPP w odniesieniu do cech, które mają być pobierane z rejestru REGON na podstawie art. 10b pkt 1 – z uwzględnieniem zmian wprowadzonych ustawą z dnia 21 listopada 2025 r. o zmianie ustawy o statystyce publicznej oraz niektórych innych ustaw.</p> <p>2) art. 10b zawiera wskazanie:</p> <p>Do Katalogu Podmiotów Publicznych, po utworzeniu konta podmiotu, przekazywane są automatycznie, za pośrednictwem interfejsu programistycznego aplikacji danego systemu, następujące dane podmiotów publicznych oraz podmiotów niepublicznych realizujących zadania publiczne [...].</p> <p>Proponowana powyżej treść wymaga doprecyzowania/wyjaśnienia - biorąc pod uwagę art. 10a pkt 4 zgodnie z którym to podmioty zamieszczają i aktualizują dane w KPP oraz art. 27b zgodnie z którym Prezes Głównego Urzędu Statystycznego udostępnia ministrowi właściwemu do spraw informatyzacji w drodze teletransmisji danych dane, o których mowa w art. 10b pkt 1, zawarte w rejestrze REGON - należy wskazać na jakim etapie dane będą pobierane z rejestru REGON. Przy czym w rejestrze REGON brak jest znacznika określającego jednoznacznie podmiot publiczny, a tym bardziej podmiot realizujący zadania publiczne. Oznacza to, że KPP będzie „odpytywał” rejestr REGON o konkretne podmioty.</p> <p>W zależności od przyjętych ostatecznych rozwiązań, rozważyć można</p> | <p>Uwaga uwzględniona</p> <p>Zakres został dostosowany do obecnego brzmienia przepisów ustawy o statystyce publicznej.</p> <p>lit b - uwaga uwzględniona - usunięto "tytuł",</p> <p>lit. c - uwaga wyjaśniona - zrezygnowano z mechanizmu przekazywania danych do REGON z poziomu KPP,</p> <p>lit. d - uwaga uwzględniona przepis został doprecyzowany poprzez dodanie "podstawowa i szczegółna",</p> <p>lit. e - uwaga uwzględniona,</p> <p>lit. i - uwaga uwzględniona,</p> <p>lit. k - uwaga uwzględniona,</p> <p>lit. l - uwaga uwzględniona</p> <p>lit. m - uwaga uwzględniona</p> <p>lit. n - uwaga uwzględniona</p> <p>3. KPP nie będzie przekazywał danych do REGON. Usunięto przepisy w zmianie ustawy o doręczeniach elektronicznych (art. 10g w brzmieniu przekazanym do opiniowania) oraz w zmianie ustawy o statystyce publicznej (dodawane w 42 ust. 7a i 8a w brzmieniu przekazanym do opiniowania).</p> <p>4. Uwaga uwzględniona przez wykreślenie projektowanych w art. 42 ustawy o statystyce publicznej ust. 7a i 8a.</p> <p>5. Wprowadzono zmiany w art. 10f w celu uwzględnienia uwagi.</p> |

| | | | | |
|--|--|--|---|--|
| | | | <p>dodanie informacji o wpisie do KPP do zakresu przedmiotowego rejestru REGON.</p> <p>W nawiązaniu do poszczególnych jednostek redakcyjnych art. 10b pkt 1 należy wskazać, jak niżej:</p> <ul style="list-style-type: none"> - lit. b: w rejestrze REGON nie jest wpisywany tytuł komornika sądowego. Proponuje się rozważenie umocowania w ustawie o komornikach sądowych zgodnie z którym Krajowa Rada Komornicza zapewniała by na potrzeby KAP dostęp do list oraz wykazu, o których mowa w art. 217–219 przedmiotowej ustawy, za pośrednictwem systemu teleinformatycznego w celu automatycznej weryfikacji komorników, zastępców komorników i asesorów komorniczych, - lit. c: forma własności jest wpisywana do rejestru REGON na podstawie procentowego udziału własności w ogólnej wartości kapitału, Skarbu Państwa, państwowych osób prawnych, jednostek samorządu terytorialnego lub samorządowych osób prawnych, krajowych osób fizycznych, pozostałych krajowych jednostek prywatnych, osób zagranicznych w ogólnej wartości kapitału. W związku z tym dla zmiany tej informacji, jeśli miałyby następować za pośrednictwem KPP konieczne jest wskazanie udziałów, - lit. d: do rejestru REGON jest wpisywana forma prawna – podstawowa i szczególna. Wobec tego zasadne wydaje się pobieranie form prawnych i szczególnych form prawnych stosownie do katalogów zawartych w rozporządzeniu Rady Ministrów z dnia 30 listopada 2015 r. w sprawie sposobu i metodologii prowadzenia i aktualizacji krajowego rejestru urzędowego podmiotów gospodarki narodowej, wzorów wniosków, ankiet i zaświadczeń (Dz. U. poz. 2009, z późn. zm.) – odpowiednio w § 7 pkt 1 i § 7 pkt 2, - lit. e: w zakres rejestru REGON wchodzi numer identyfikacji podatkowej (NIP) oraz informacje o jego unieważnieniu lub uchyleniu, - lit. i: data zakończenia działalności może nie być wypełniona w rejestrze REGON. Proponuje się rozważenie dodania daty wykreślenia z ewidencji/rejestru, - lit. k: wykonywana działalność, w tym przedmiot przeważającej działalności są wpisywane według Polskiej Klasyfikacji Działalności. Wskazuje się na konieczność kodowania wg PKD i dokonywania zmian w przypadku zmian zachodzących w tej klasyfikacji – ostatnia zmiana klasyfikacji została wprowadzona rozporządzeniem Rady Ministrów z dnia 18 grudnia 2024 r. w sprawie Polskiej Klasyfikacji Działalności (PKD) (Dz. U. z 2024 r. poz. 1936). - lit. l: numer telefonu i faksu siedziby – ponownie należy wskazać na | |
|--|--|--|---|--|

| | | | | |
|--|--|--|---|--|
| | | | <p>konieczność dostosowania terminologii (z „rejestru podmiotów” na „rejestr REGON”). Wskazać należy także na zasadność dostosowania projektu do zmian w ustawie o statystyce publicznej, które wejdą w życie 17 grudnia 2026 r. (od tego dnia obowiązywał będzie art. 42 ust. 3 pkt 10 w brzmieniu „numer telefonu i faksu, adres poczty elektronicznej i strony internetowej oraz adres do doręczeń elektronicznych, o ile podmiot takie posiada.”).</p> <p>- lit. m: do rejestru REGON wpisywana jest nazwa organu rejestrowego lub ewidencyjnego, nazwa rejestru (w tym rejestr przedsiębiorców oraz stowarzyszeń, innych organizacji społecznych i zawodowych, fundacji oraz samodzielnych publicznych zakładów opieki zdrowotnej (KRS)) i nadany przez ten organ numer, o ile został nadany. Wskazanie „w tym numer KRS oraz numer identyfikacyjny szkoły, placówki lub centra, o którym mowa w art. 9c ust. 2b ustawy z dnia 7 września 1991 r. o systemie oświaty” jest w naszej ocenie zbędne, wskazane informacje są powiązane z organem rejestrowym i rodzajem rejestru.</p> <p>Ponadto zakres został rozszerzony o typ podmiotu będącego jednostką sektora finansów publicznych – jednostka budżetowa albo samorządowy zakład budżetowy, w przypadku jednostki lokalnej o dane kontaktowe.</p> <p>- lit. n: informacje o jednostkach lokalnych tych podmiotów w zakresie określonym w lit. b, f, g, h, i, j, k, m. Zakres informacji o j. lokalnych został rozszerzony z terminem wejścia w życie 17.12.2026 r., w związku z czym proponujemy rozważenie rozszerzenia katalogu informacji o jednostkach lokalnych w KPP. Wskazany zakres wymaga zatem ponownego zredagowania wobec obecnie obowiązującej treści art. 42 ust. 3 ustawy o statystyce publicznej wynikającej z rozszerzenia zakresu przedmiotowego rejestru REGON nowelizacją.</p> <p>3) Art. 10c. zawiera wskazanie:</p> <p>Minister właściwy do spraw informatyzacji może wprowadzać, wycofywać lub aktualizować dane, o których mowa w art. 10a ust. 3 pkt 1 lit. a, g–i, n, o, t, u, x, y, oraz z, o podmiotach publicznych oraz o podmiotach niepublicznych realizujących zadania publiczne na podstawie danych pochodzących z rejestrów publicznych lub na podstawie danych, w których posiadaniu jest minister właściwy do spraw informatyzacji pochodzących z systemów teleinformatycznych prowadzonych przez tego ministra, a także prostować oczywiste błędy i omyłki pisarskie</p> <p>Prosimy o wyjaśnienie, czy taka zmiana zostanie przekazana do rejestru REGON. Przepis budzi także wątpliwość w przypadku gdy sprostowaniu podlegać będą informacje dla których referencyjne są dane KRS, RSPO, CRP-KEP.</p> | |
|--|--|--|---|--|

| | | | | |
|-----|--------|-----|--|---|
| | | | <p>4) Zgodnie z art. 10g ust. 1: Jeżeli zmiana danych w Katalogu Podmiotów Publicznych dotyczy danych objętych wpisem do rejestru REGON, wprowadzone do Katalogu Podmiotów Publicznych przez podmiot zobowiązany aktualne dane podmiotu publicznego lub podmiotu niepublicznego realizującego zadania publiczne są przekazywane z Katalogu Podmiotów Publicznych do rejestru REGON. Wprowadzenie aktualnych danych do Katalogu Podmiotów Publicznych przez podmiot zobowiązany jest równoznaczne ze złożeniem wniosku o zmianę cech objętych wpisem w rejestrze REGON albo wniosku o skreślenie podmiotu publicznego lub podmiotu niepublicznego realizującego zadania publiczne z rejestru REGON. Ponownie należy zauważyć, że część podmiotów/cech, podlegających wpisowi do rejestru REGON i KPP jest zgodnie z obowiązującymi przepisami wpisywana do rejestru REGON na podstawie danych przekazanych z KRS/RSPO/CRP KEP – w związku z czym należałoby wyłączyć możliwość dokonywania aktualizacji/skreśleń w oparciu o dane KPP w przypadkach uregulowanych w art. 42 ust 3a, 6a, 7, 11, 14. Projekt powinien precyzyjnie określać zakres cech aktualizowanych przez podmioty publiczne i niepubliczne realizujących zadania publiczne w rejestrze REGON za pośrednictwem KPP.</p> <p>5) Zgodnie z art. 10f: Art. 10f. Dane, o których mowa w art. 10a w ust. 3 pkt 1 lit. a, g, h, i, n, o, t, u, v, y oraz z, pkt 2 i 3, do Katalogu Podmiotów Publicznych wprowadzają podmioty publiczne oraz podmioty niepubliczne realizujące zadania publiczne w terminie 5 dni roboczych od dnia utworzenia konta w Katalogu Podmiotów Publicznych oraz aktualizują te dane w terminie 5 dni roboczych od dnia zmiany tych danych. Prosimy o wyjaśnienie w kontekście projektowanego rozwiązania, zgodnie z którym dane są pobierane z rejestru REGON.</p> | |
| 27. | Art. 5 | GUS | <p>Odnosnie do krajowego rejestru urzędowego podziału terytorialnego kraju (TERYT), w art. 5 wprowadzającym zmiany w ustawie o doręczeniach elektronicznych, w zakresie projektowanego art. 10b pkt 2 – uwaga analogiczna jak w uwaga do art. 10a ust. 3 pkt 1 lit. r; proponuje się ujednolicenie przepisów art. 10b z art. 10a w następujący sposób: „2) z krajowego rejestru urzędowego podziału terytorialnego kraju, o którym mowa w art. 47 ustawy z dnia 29 czerwca 1995 r. o statystyce publicznej:</p> <p>„... s) t) u)</p> | <p>Uwaga uwzględniona Przepis został przeredagowany zgodnie z treścią uwagi.</p> |

| | | | | |
|-----|--------|-----|--|---|
| | | | v) w) x) y) z) aa) bb) cc) dd) ee) ff) gg) a) identyfikatory i nazwy jednostek podziału terytorialnego, b) identyfikatory i nazwy miejscowości, c) nazwy ulic i ich identyfikatory,...". | |
| 28. | Art. 5 | GUS | <p>Odnosnie do krajowego rejestru urzędowego podziału terytorialnego kraju (TERYT), w art. 5 wprowadzającym zmiany w ustawie o doręczeniach elektronicznych, w zakresie projektowanego art. 10b – zgodnie z wprowadzeniem do przepisu, do Katalogu Podmiotów Publicznych, przekazywane są automatycznie (za pośrednictwem interfejsu programistycznego aplikacji danego systemu) dane podmiotów publicznych oraz podmiotów niepublicznych realizujących zadania publiczne pochodzące z kilku źródeł, w tym z rejestru TERYT; należy jednak zaznaczyć, że w ramach rejestru TERYT nie są gromadzone dane o jakichkolwiek podmiotach, co sugeruje obecne brzmienie przepisu, a jedynie identyfikatory i nazwy, które mogą być użyte do opisu tych podmiotów, stąd do rozważenia pozostaje czy wprowadzenie do przepisu nie powinno zostać przeredagowane w taki sposób, aby jego brzmienie nie wskazywało na niezgodny ze stanem faktycznym zakres rejestru TERYT.</p> <p>Powyższa uwaga została zgłoszona przez GUS do projektu ustawy o zmianie ustawy o doręczeniach elektronicznych oraz niektórych innych ustaw (projekt z dnia 21.08.2025 r.). Zgodnie z odniesieniem do zgłoszonej przez GUS uwagi wprowadzenie do wyliczenia w art. 10b miało zostać przeredagowane i otrzymać brzmienie:</p> <p>„Do Katalogu Podmiotów Publicznych, po utworzeniu konta podmiotu, przekazywane są automatycznie, za pośrednictwem interfejsu programistycznego aplikacji danego systemu, następujące dane dotyczące podmiotów publicznych oraz podmiotów niepublicznych realizujących zadania publiczne:” – przeredagowanie dotyczyło dopisania w przepisie</p> | <p>Uwaga uwzględniona</p> <p>Przepis przeredagowany zgodnie z treścią uwagi.</p> |

| | | | | |
|-----|--------------|--------------------------|--|--|
| | | | wyrazu „dotyczące”. W nowym projekcie ustawy o zmianie ustawy o doręczeniach elektronicznych oraz niektórych innych ustaw (projekt z dnia 19.02.2026 r.) oraz w opiniowanym projekcie o zmianie ustawy o usługach zaufania oraz identyfikacji elektronicznej oraz niektórych innych ustaw, nowe brzmienie wprowadzenia do wyliczenia nie zostało jednak uwzględnione. Tym samym w obydwu wymienionych projektach rejestr TERYT pozostaje wskazanym jako jedno ze źródeł danych podmiotów publicznych i podmiotów niepublicznych realizujących zadania publiczne, pomimo iż nie gromadzi danych o tych podmiotach. | |
| 29. | Art. 5 pkt 2 | Rada do Spraw Cyfryzacji | 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 rozdzielania: „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.” | Uwaga wyjaśniona Zasady udostępniania danych są uregulowane w art. 10g i ograniczają się tylko do danych określonych w art. 10a ust. 3 pkt 1, które są danymi powszechnie dostępnymi pobieranymi z rejestrów publicznych. W związku z tym nie jest potrzebna dodatkowa zmiana zgłoszona w uwadze. |
| 30. | Art. 5 pkt 2 | Rada do Spraw Cyfryzacji | 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. | Uwaga uwzględniona Przepis doprecyzowano. |
| 31. | Art. 5 pkt 2 | Prezes UODO | (...) 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. | Uwaga wyjaśniona Rozwiązanie, które pozwala ministrowi właściwemu do spraw informatyzacji określić zasady bezpieczeństwa systemu, jest rozwiązaniem powszechnie stosowanym, dot. np., bazy adresów elektronicznych. W celu zachowania spójności przepisów nie powinno w odniesieniu do KPP zostać uregulowane w odmienny sposób. |
| 32. | Art. 5 pkt 2 | Prezes UODO | 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 | Uwaga wyjaśniona Uwaga odnosi się do oceny skutków regulacji w zakresie danych osobowych w KPP - przedmiotowa ocena jest w trakcie przygotowania. |

| | | | | |
|-----|--------------|-------------|---|--|
| | | | informacji z systemów teleinformatycznych i rejestrów publicznych z Katalogiem Podmiotów Publicznych | |
| 33. | Art. 5 pkt 2 | Prezes UODO | 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 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. | Uwaga uwzględniona Uzasadnienie zostało uzupełnione o wskazanie niezbędności utworzenia KPP w kontekście obowiązku korzystania z doręczeń elektronicznych. |
| 34. | Art. 5 pkt 2 | Prezes UODO | 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. | Uwaga uwzględniona Przepis został przeredagowany i będzie wskazywał precyzyjnie jakich danych dotyczy. |
| 35. | Art. 5 pkt 2 | Prezes UODO | 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. Nastąpi 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. | Uwaga uwzględniona Przepis został przeredagowany w celu uwzględnienia uwagi. |

| | | | | |
|-----|--|-------------|--|--|
| 36. | Art. 5 pkt 2 | GUS | <p>Odnosnie do krajowego rejestru urzędowego podziału terytorialnego kraju (TERYT) w art. 5 pkt 2 wprowadzającym zmiany w ustawie z dnia 18 listopada 2020 r. o doręczeniach elektronicznych, w zakresie: – projektowanego art. 10a ust. 3 pkt 1 lit. r – wśród danych, których źródłem jest rejestr TERYT, oprócz identyfikatorów i nazw jednostek podziału terytorialnego oraz identyfikatorów i nazw miejscowości wskazano również w lit. r pozycję „identyfikacji adresowej ulic, nieruchomości, budynków i mieszkań”. Określenie to nie współgra z pozostałymi danymi z rejestru TERYT, które mają być ujęte w KPP, gdyż odnosi się do nazwy jednego z systemów (NOBC) wchodzącego w skład rejestru TERYT. System ten nie zawiera adresów budynków innych niż budynki z mieszkaniami (tj. nie zawiera adresów budynków będących w obszarze zainteresowania KPP). Ponadto dane z tego systemu nie są aktualnie udostępniane za pomocą usług sieciowych co uniemożliwia ich automatyczne przekazywanie do KPP, za pośrednictwem interfejsu programistycznego aplikacji systemu, zgodnie z projektowanym art. 10b pkt 2 lit. c. Tym samym przywołanie tego systemu w projekcie ustawy w kontekście wykorzystania w KPP danych zawartych w tym systemie w ocenie GUS nie jest właściwe. Do oznaczenia pełnego adresu podmiotów publicznych lub niepublicznych realizujących zadania publiczne (poza danymi wymienionymi w projektowanym art. 10a ust. 3 pkt 1) lit. p i q, powinny zostać wymienione nazwy ulic i ich identyfikatory gromadzone w Centralnym Katalogu Ulic, który również jest częścią rejestru TERYT i który, razem z systemem identyfikatorów i nazw jednostek podziału terytorialnego (TERC) oraz z systemem identyfikatorów i nazw miejscowości (SIMC), jest wykorzystywany w innych rejestrach i systemach informacyjnych administracji publicznej do kodowania adresów. Proponujemy zatem w projektowanym art. 10a ust. 3 pkt 1 w części odnoszącej się do danych pochodzących z rejestru TERYT następujące brzmienie:</p> <p>”... identyfikatory i nazwy jednostek podziału terytorialnego, identyfikatory i nazwy miejscowości, nazwy ulic i ich identyfikatory,...”.</p> | <p>Uwaga uwzględniona Przepis został przeredagowany w celu uwzględnienia uwagi</p> |
| 37. | Art. 6 pkt 1 w zakresie art. 1 pkt 5 i 6 | Prezes UODO | <p>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</p> | <p>Uwaga uwzględniona W przepisie zostanie wskazany art. 3 pkt 42 rozporządzenia eIDAS.</p> |

| | | | | |
|-----|---|-------------|--|--|
| | | | 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. | |
| 38. | Art. 6 pkt 2 w zakresie art. 14a ust. 2 | Prezes UODO | <p>W kontekście innych uregulowań projektowanej ustawy powstaje zasadnicze pytanie o adekwatność danych i celowość przetwarzania tak ukształtowanego katalogu danych.</p> <p>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 uwierzytłoni 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.</p> <p>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.”.</p> <p>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</p> | <p>Uwaga wyjaśniona</p> <p>Zgodnie z postulatem ocena skutków dla ochrony danych projektowanej ustawy została przeprowadzona.</p> <p>Nadmienić należy, że inicjatywa zastąpienia numeru PESEL innym numerem administracyjnym w identyfikacji elektronicznej w usługach online wymagałaby odrębnego projektu i odrębnej dyskusji w szczególności wymagającej kampanii wyjaśniającej ewentualne skutki rezygnacji z przetwarzania nr PESEL na rzecz innego identyfikatora lub klucza, w tym też badania opinii publicznej i nie powinna być realizowana przy okazji przepisów wdrażających rozporządzenie eIDAS. Zgodnie art. 5a ust. 5 lit. f rozporządzenia eIDAS „państwa członkowskie muszą zapewniać, aby dane identyfikujące osobę, które są dostępne w systemie identyfikacji elektronicznej, w ramach którego zapewniany jest europejski portfel tożsamości cyfrowej, niepowtarzalnie reprezentowały osobę fizyczną, osobę prawną, lub osobę fizyczną reprezentującą osobę fizyczną lub prawną, oraz były powiązane z tym europejskim portfelem tożsamości cyfrowej”. Na gruncie krajowym oparcie się na dotychczasowych zasadach wynika z tego, że europejski portfel tożsamości cyfrowej zostanie przyłączony do węzła krajowego w ramach publicznego systemu identyfikacji elektronicznej jako jeden ze środków identyfikacji elektronicznej i będzie mógł być wykorzystywany do identyfikacji elektronicznej w obecnie istniejących usługach online (te wymagają numeru PESEL, aby jednoznacznie zidentyfikować użytkownika).</p> <p>Proces identyfikacji elektronicznej jest bowiem czymś innym niż proces selektywnego przekazywania atrybutów, w którym możliwy będzie wybór danych przekazywanych stronom ufającym.</p> |

| | | | | |
|-----|---|---------------------------|---|---|
| | | | <p>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 <code>personal_administrative_number</code> 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).</p> <p>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”.</p> <p>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.</p> | |
| 39. | Art. 6 pkt 2 w zakresie art. 14a ust. 5 | Urząd Lotnictwa Cywilnego | <p>Należy jednak wskazać, że w dodawanym art. 14a ust. 5 pkt 2 do ustawy z dnia 26 maja 2023 r. o aplikacji mObywatel (art. 6 pkt 2 projektu) znajduje się odesłanie do dokumentu - Doc 9303 Machine Readable Travel</p> | <p>Uwaga wyjaśniona Specyfikacja Doc 9303 Machine Readable Travel Documents ogłoszona pod adresem https://www.icao.int/publications/doc-series/doc-9303</p> |

| | | | | |
|-----|---|--------------------------|---|---|
| | | | <p>Documents. Dokumenty Doc wydawane przez Organizację Międzynarodowego Lotnictwa Cywilnego nie są przepisami powszechnie obowiązującymi i nie obowiązują wprost, a Urząd Lotnictwa Cywilnego nie ma wiedzy na temat ewentualnego ogłoszenia przedmiotowego dokumentu w języku polskim. Jednocześnie należy zauważyć, że w projekcie nie wskazano, do której wersji tego dokumentu projektowany przepis się odwołuje. W związku z powyższym sugeruję doprecyzowanie art. 14a ust. 5 pkt 2 w tym zakresie.</p> | <p>nie ma polskiej wersji językowej, co nie znaczy że nie może być wskazana w przepisach krajowych.</p> <p>Ta właśnie specyfikacja jest wskazana w rozporządzeniu Ministra Spraw Wewnętrznych i Administracji z dnia 21 lutego 2025 r. w sprawie warstwy elektronicznej dowodu osobistego (Dz. U. poz. 267). Dokument ten jest również przywoływany w normach wskazanych w obowiązujących bezpośrednio rozporządzeniach wykonawczych wydanych przez Komisję Europejską na podstawie rozporządzenia eIDAS. Przykładowo w normie ETSI TS 119 461 V2.1.1 (2025-02) wskazanej w rozporządzeniu wykonawczym Komisji (UE) 2025/1566 z dnia 29 lipca 2025 r. ustanawiające zasady stosowania rozporządzenia Parlamentu Europejskiego i Rady (UE) nr 910/2014 w odniesieniu do norm referencyjnych dotyczących weryfikacji tożsamości i atrybutów osoby, której ma zostać wydany certyfikat kwalifikowany lub kwalifikowane elektroniczne poświadczenie atrybutów (Dz. U. UE. L. z 2025 r. poz. 1566).</p> <p>Mając na uwadze, że ostatnie wersja DOC 9303 jest to wersja ósma wydana w roku 2021. Poprzednia siódma wersja z roku 2015 była wskazana w rozporządzeniu Ministra Spraw Wewnętrznych i Administracji z dnia 26 lutego 2019 r. w sprawie warstwy elektronicznej dowodu osobistego (Dz. U. z 2022 r. poz. 1431). Zmiana rozporządzenie w tym zakresie miała miejsce dopiero w 2025 roku (Dz. U. poz. 267).</p> <p>Znaczy to, że są obiegu ważne dowody osobiste spełniające zalecenia Organizacji Międzynarodowego Lotnictwa Cywilnego w wersji siódmej i w wersji ósmej.</p> <p>Podobnie może być z dokumentami podróży nie wydawanymi w Polsce do których odnosi się przepis i których zgodność z wersją siódmą z 2015 r. lub z wersją ósmą z 2021 r. i nie ma znaczenia dla celu określonego w projektowanym art. 14a ust. 5 pkt 2</p> |
| 40. | Art. 6 pkt 2 w zakresie 14b ust. 2 | Rada do Spraw Cyfryzacji | <p>Niespójność w art. 14b ust. 2 (odwołanie 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);</p> | <p>Uwaga uwzględniona</p> <p>Poprawiono na odwołanie do ust. 1 pkt 3 lit. b.</p> |
| 41. | Art. 6 pkt 2 w zakresie art. 14b ust. 3 | Prezes UODO | <p>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</p> | <p>Uwaga wyjaśniona</p> <p>Wymogi dotyczące dodatkowej weryfikacji tożsamości będą wynikały z rozporządzenia wykonawczego komisji (UE) 2026/798 z dnia 7 kwietnia 2026 r. ustanawiające zasady stosowania rozporządzenia Parlamentu Europejskiego i Rady (UE) nr 910/2014 w odniesieniu do norm referencyjnych i specyfikacji dotyczących zdalnej rejestracji</p> |

| | | | | |
|-----|---|-------------|--|--|
| | | | <p>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).</p> | <p>użytkowników w europejskich portfelach tożsamości cyfrowej za pomocą środków identyfikacji elektronicznej zgodnych ze średnim poziomem bezpieczeństwa w połączeniu z dodatkowymi procedurami zdalnej rejestracji, jeżeli połączenie to spełnia wymogi wysokiego poziomu bezpieczeństwa wydanego na podstawie art. 5a ust. 24 rozporządzenia eIDAS.</p> <p>Została tam wskazana norma ETSI TS 119 461 V2.1.1 (2025-02) w zakresie odpowiadającym podniesieniu poziomu bezpieczeństwa weryfikacji tożsamości z określonego tej normie „Baseline Level of Identity Proofing” do „Extended Level of Identity Proofing” – z dodatkowymi niewielkimi modyfikacjami. Powyższe znaczy, że działania zgodne z tą normą są akceptowane.</p> <p>Oczywistym jest, że duża liczba punktów potwierdzających jest podyktowana chęcią zapewnienia zainteresowanym osobom uprawnionym wygodnego i powszechnego dostępu do miejsc, gdzie mogą potwierdzić swoją tożsamość do celów zarejestrowania w europejskim portfelu tożsamości cyfrowej.</p> <p>Poprawiono odesłanie.</p> |
| 42. | Art. 6 pkt 2 w zakresie art. 14c ust. 2 pkt 3 | Prezes UODO | <p>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.</p> | <p>Uwaga wyjaśniona</p> <p>Europejski portfel tożsamości cyfrowej jest środkiem identyfikacji elektronicznej, co wynika z definicji zawartej w art. 3 pkt 42 rozporządzenia eIDAS i co za tym idzie podlega w tym zakresie przepisom rozporządzenia wykonawczego Komisji (UE) 2015/1502 z dnia 8 września 2015 r. w sprawie ustanowienia minimalnych specyfikacji technicznych i procedur dotyczących poziomów zaufania w zakresie środków identyfikacji elektronicznej na podstawie art. 8 ust. 3 rozporządzenia Parlamentu Europejskiego i Rady (UE) nr 910/2014 w sprawie identyfikacji elektronicznej i usług zaufania w</p> |

| | | | | |
|-----|---|-------------|---|--|
| | | | | <p>odniesieniu do transakcji elektronicznych na rynku wewnętrznym (Dz. U. UE. L. z 2015 r. Nr 235, str. 7, z późn. zm.).</p> <p>W tym akcie prawnym w części 2.1.4 załącznika wskazuje się wymagania dotyczące powiązania między środkami identyfikacji elektronicznej osób fizycznych i prawnych, jakie powinny mieć miejsce „w stosownych przypadkach”. Takim właśnie stosownym przypadkiem będzie powiązanie, o którym mowa w projektowanych nowych przepisach art. 14 ust. 3-5 ustawy o aplikacji mObywatel. Ponadto w art. 3 ust. 7 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. U. UE. L. z 2024 r. poz. 2977) wymaga się, co następuje:</p> <p>„7 Państwa członkowskie wprowadzają do systemu użytkowników portfela zgodnie z określonymi w rozporządzeniu wykonawczym Komisji (UE) 2015/1502 wymogami dotyczącymi wprowadzania do systemu na wysokim poziomie bezpieczeństwa. Podczas wprowadzania do systemu - przed wydaniem danych identyfikujących osobę jednostce portfela odpowiedniego użytkownika portfela - dostawcy danych identyfikujących osobę przeprowadzają weryfikację tożsamości użytkownika portfela zgodnie z wymogami w zakresie sprawdzania i weryfikacji tożsamości.”</p> <p>Mając przy tym na uwadze że zgodnie art. 5a ust. 5 lit. f rozporządzenia eIDAS „muszą zapewniać, aby dane identyfikujące osobę, które są dostępne w systemie identyfikacji elektronicznej, w ramach którego zapewniany jest europejski portfel tożsamości cyfrowej, niepowtarzalnie reprezentowały osobę fizyczną, osobę prawną, lub osobę fizyczną reprezentującą osobę fizyczną lub prawną, oraz były powiązane z tym europejskim portfelem tożsamości cyfrowej” oczywiste jest, że możliwe jest przetwarzanie w jednym portfelu danych osoby fizycznej i danych osobę prawną, lub osobę fizyczną reprezentującą osobę fizyczną lub prawną - pod warunkiem, że dane te będą niepowtarzalnie reprezentowały wskazane osoby.</p> |
| 43. | Art. 6 pkt 2 w zakresie art. 14e ust. 1 | Prezes UODO | <p>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.</p> <p>Jedną z kluczowych kwestii podnoszonych w wystąpieniach organu</p> | <p>Uwaga wyjaśniona</p> <p>Ze względu na ich techniczny i doprecyzowujący względem przepisów unijnych charakter, wymagania dotyczące certyfikatów kwalifikowanego podpisu elektronicznego zostaną ustalone w wytycznych publikowanych przez ministra właściwego do spraw</p> |

| | | | | |
|--|--|--|--|--|
| | | | <p>nadzorczego do Ministra Cyfryzacji w związku z funkcjonowaniem w Polsce podpisów elektronicznych było wypracowanie rozwiązań, które zapobiegą ujawnianiu numeru PESEL jako „swoistego śladu cyfrowego” pozostawianego na podpisanych cyfrowo dokumentach.</p> <p>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 nieodpłatnego kwalifikowanego podpisu elektronicznego będzie mógł używać tego podpisu, tak aby w jego certyfikacie nie było numeru PESEL.</p> <p>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 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.”.</p> <p>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.</p> <p>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</p> | <p>informatyzacji w BIP. Niniejsze uwagi zostaną uwzględnione na etapie prac nad wytycznymi.</p> <p>Brak jest uzasadnienia, dla którego w certyfikacie nie mógłby się znaleźć numer, o którym mowa w art. 14a ust. 4 pkt 4 ustawy.</p> |
|--|--|--|--|--|

| | | | | |
|-----|---|--------------------------|---|---|
| | | | rozporządzenia 910/2014). Projektodawca powinien precyzyjnie uregulować tę 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 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. | |
| 44. | Art. 6 pkt 2 w zakresie 14f ust.1 | Rada do Spraw Cyfryzacji | 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; | Uwaga uwzględniona Poprawiono na odwołanie do art. 14e ust. 1. |
| 45. | Art. 6 pkt 2 w zakresie art. 14f ust. 2 | Prezes UODO | 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. | Uwaga wyjaśniona Sposób oznaczania podpisanego dokumentu zostanie określony w wytycznych, o których mowa w art 6 ust. 2 w zakresie art. 14e ust. 11. Ponadto w przepisach nie chodzi o to, czy przeznaczony do podpisu dokument jest wykonany w celu innym niż profesjonalny tylko czy został użyty podpis do celów innych niż profesjonalne. |
| 46. | Art. 6 pkt 2 w zakresie art. 14h | Prezes UODO | Należy rozważyć, czy materia, która miałyby 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 | Uwaga wyjaśniona Zrezygnowano z przepisu upoważniającego do wydania rozporządzenia. |

| | | | | |
|-----|---------|-----------------------------------|--|---|
| | | | <p>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.</p> | |
| 47. | Art. 11 | GUS | <p>Art. 11 (termin wejścia w życie). Sygnalizuje się konieczność przesunięcia terminu wejścia w życie przepisów dot. aktualizacji rejestru REGON w oparciu o KPP na koniec 2027 r. Wskazany termin jest związany z koniecznością dostosowania systemów rejestru REGON do proponowanych zmian - w zakresie rejestracji określonych podmiotów w oparciu o dane z KPP. Dodatkowo, w związku z koniecznymi do wdrożenia zmianami - wynikającymi ze zmian wprowadzonych ustawą z dnia 21 listopada 2025 r. o zmianie ustawy o statystyce publicznej oraz niektórych innych ustaw (Dz. U. poz. 1792) oraz rozporządzeniem Rady Ministrów z dnia 18 grudnia 2024 r. w sprawie Polskiej Klasyfikacji Działalności (PKD) (Dz. U. z 2024 r. poz. 1936) – związanymi m.in. z koniecznością dostosowania systemu REGON do możliwości przeklasyfikowania działalności podmiotów wg PKD 2025 oraz rozpoczęciem tego przeklasyfikowania od 1 stycznia 2027 r., realizacja dodatkowych zmian w rejestrze REGON mogła by kolidować ze zmianami wynikającymi z ww. przepisów.</p> | <p>Uwaga wyjaśniona Zgodnie z art. 11 ustawa wchodzi w życie z dniem 24 grudnia 2026 r., natomiast w art. 11 pkt 3 stanowi, że dodawany art. 10 g (dotyczący aktualizacji danych w REGON) wchodzi w życie po upływie 12 miesięcy od dnia ogłoszenia a więc pod koniec 2027: "3) art. 5 pkt 7 w zakresie art. 10a ust. 3 pkt 1 lit. k i l, lit. o w zakresie adresu poczty elektronicznej, lit. s, y i z oraz pkt 2 i 3, art. 10b pkt 1 lit. b w zakresie nazwy lub firmy podmiotu niepublicznego realizującego zadania publiczne pod którą ten podmiot działa oraz imienia i nazwiska, lit. g i h, lit. l w zakresie adresu poczty elektronicznej, pkt 3 lit. b oraz pkt 5, art. 10d ust. 1, 2, 3, 5, 7, 8 i 10, art. 10e, art. 10f, art. 10g i art. 10i oraz pkt 8 i pkt 33, które wchodzi w życie po upływie 12 miesięcy od dnia ogłoszenia;"</p> |
| 48. | OSR | Prezes Wyższego Urzędu Górniczego | <p>W Ocenie Skutków Regulacji przedmiotowej ustawy, w części dotyczącej podmiotów, na które oddziałuje projekt, Wyższy Urząd Górniczy został wskazany jako podmiot odpowiedzialny za „źródło autentyczne” w rozumieniu art. 3 pkt 47 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 uchylające dyrektywę 1999/93/WE (Dz. Urz. UE L 257 z 28.08.2014, str. 73, z późn. zm.), zwanego dalej „rozporządzeniem eIDAS”.</p> <p>Decyzje wydawane przez Prezesa Wyższego Urzędu Górniczego oraz dyrektorów okręgowych urzędów górniczych na podstawie przepisów art. 61 ust. 1 w zw. z art. 58 ust. 1 i 2 ustawy 9 czerwca 2011 r. – Prawo geologiczne i górnicze (Dz. U. z 2026 r. poz. 69) nie mieszczą się w minimalnym wykazie atrybutów objętych załącznikiem VI do rozporządzenia eIDAS. Tym samym, zapewnienie weryfikacji ich autentyczności drogą elektroniczną jest jedynie fakultatywne. Jednocześnie przepisy zapewniają inną formę weryfikacji – poprzez publikację wykazu osób, którym stwierdzono kwalifikacje w Biuletynie Informacji Publicznej. W tej sytuacji, przepisy ustawy nie wpływałyby</p> | <p>Uwaga wyjaśniona Zgodnie z projektowanym art. 22c ust. 1 podmioty publiczne odpowiedzialne na poziomie krajowym za źródła autentyczne (...) zapewniają kwalifikowanym dostawcom usług zaufania (...) możliwość weryfikacji tych atrybutów drogą elektroniczną, na żądanie użytkownika”, zgodnie z art. art. 45e ust. 1 eIDAS2. Oznacza to, że każdy podmiot publiczny odpowiedzialny za „źródło autentyczne” w rozumieniu art. 3 pkt 47 eIDAS (co najmniej w zakresie atrybutów wskazanych w załączniku VI do eIDAS) będzie zobowiązany do zrealizowanie obowiązku, o którym mowa a art. 45e eIDAS. W związku z tym, że Wyższy Urząd Górniczy publikuje w Biuletynie Informacji Publicznej wykaz osób, którym stwierdzono posiadanie kwalifikacji określonych w art. 50 oraz art. 58 ust. 1 i 2 ustawy z dnia 9 czerwca 2011 r. - Prawo geologiczne i górnicze (Dz. U. z 2026 r. poz. 69) oraz, którym nadano uprawnienia rzeczoznawcy do spraw ruchu zakładu górniczego, przyjęto założenie, że mieści się to w zakresie pkt 10 załącznika VI do eIDAS czyli „publicznoprawne zezwolenia i licencje”.</p> |

| | | | | |
|-----|--------------|-------------|---|---|
| | | | bezpośrednio na zadania organów nadzoru górniczego w najbliższej perspektywie czasowej. | <p>Oczywiście co do zasady podmioty publiczne odpowiedzialne za takie źródła mają najlepszą wiedzę w zakresie tego, czy mieści się ono w minimalnym wykazie atrybutów objętych załącznikiem VI do rozporządzenia eIDAS, jak również czy źródło autentyczne zarządzane przez nie spełnia wymagania definicji zawartej w art. 3 pkt 47 eIDAS: „7) „źródło autentyczne” oznacza repozytorium lub system, za prowadzenie którego odpowiedzialny jest podmiot sektora publicznego lub podmiot prywatny, które zawiera i udostępnia atrybuty dotyczące osoby fizycznej lub prawnej lub przedmiotu i które uważa się za podstawowe źródło tych informacji lub uznaje za autentyczne zgodnie z prawem Unii lub prawem krajowym, w tym z praktykami administracyjnymi;”.</p> <p>W przypadku o którym mowa wydaje się oczywiste, że mimo, że przepisy krajowe zapewniają inną formę weryfikacji – poprzez publikację wykazu osób, którym stwierdzono kwalifikacje w Biuletynie Informacji Publicznej nie wyklucza to stosowania rozporządzenia eIDAS celem umożliwienia kwalifikowanym dostawcom usług zaufania wydawania kwalifikowanych elektronicznych poświadczeń atrybutów potwierdzających uprawnienia, o których mowa w ustawie z dnia 9 czerwca 2011 r. - Prawo geologiczne i górnicze.</p> |
| 49. | Uwaga ogólna | Prezes UODO | <p>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 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</p> | <p>Uwaga wyjaśniona/częściowo uwzględniona</p> <p>Inicjatywy, aby w celu jednoznacznej identyfikacji osoby fizycznej zrezygnować z numeru PESEL jako unikatowego numeru jednoznacznie identyfikującego osobę fizyczną wpisaną do ewidencji ludności i zastąpić go innym identyfikatorem, który nie będzie zawierał daty urodzenia i oznaczenia płci albo zbiorem danych jednoznacznie identyfikujących osobę fizyczną były już przedkładane, ale nie doprowadziły do zmian w tym zakresie. Zadaniem projektodawcy celem tej ustawy nie powinna być realizacja takich postulatów. W tym kontekście warto podkreślić, że w przypadku rezygnacji z unikatowego identyfikatora osoby fizycznej i posługiwania się zamiast nim zestawem danych jednoznacznie identyfikujących osobę fizyczną nie wystarczy nawet obowiązkowy zestaw danych wskazany w tabeli 1 załącznika 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. U. UE. L. z 2024 r. poz. 2977), czyli imię + nazwisko + data urodzenia + miejsce urodzenia +</p> |

| | | | | |
|-----|--------------|--------------------------|---|--|
| | | | <p>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.</p> | <p>obywatelstwo. Taki zestaw nie daje bowiem całkowitej pewności, że nie ma więcej niż jednej osoby, którą takie dane określają. Gdyby tak było, to istotnie można byłoby zrezygnować z nadawania unikatowych identyfikatorów jednoznacznie identyfikujących osobą fizyczną na rzecz pakietów danych. Do ww. pakietu danych niezbędny jest dodatkowy atrybut. Znaczy to, że w praktyce w celu uniknięcia przetwarzania unikatowego numeru identyfikującego osobę fizyczną łącznie może być przetwarzany większy zestaw danych, który wszak i tak musi zapewnić niepowtarzalną identyfikację.</p> <p>Nie jest jednoznacznie udowodnione, że posługiwanie się szerszym zestawem danych jest lepsze dla obywateli od przetwarzania mniejszego zestawu danych, ale zawierającego niepowtarzalny identyfikator. Przykładowo zgodnie z art. 296 ust. pkt 1 ustawy dnia 12 lipca 2024 r. - Prawo komunikacji elektronicznej (Dz. U. poz. 1221, z późn. zm.). Wystarczy podanie przez abonenta dostawy usług telekomunikacyjnych imienia (imion) i nazwisko, i numeru PESEL. Nie ma potrzeby podawania większej ilości danych. Jednak w przypadku zamiast PESEL przekazywana byłaby kolekcja atrybutów jednoznacznie identyfikujących osobę fizyczną, niezawierająca numeru PESEL to zestaw danych przekazywanych dostawcy usług telekomunikacyjnych musiałby być znacząco szerszy. W efekcie niewątpliwie wpłynęłoby to na konieczność przebudowy systemów publicznych celem dostosowanie ich do innego sposobu identyfikacji użytkowników. Dlatego też tego rodzaju inicjatywa wymagałaby odrębnego projektu i odrębnej dyskusji w szczególności wymagającej kampanii wyjaśniającej ewentualne skutki rezygnacji z przetwarzania nr PESEL na rzecz innego identyfikatora lub klucza w tym też badania opinii publicznej i nie powinna być realizowana przy okazji przepisów wdrażających rozporządzenie eIDAS.</p> <p>Zgodnie z postulatem ocena skutków dla ochrony danych projektowanej ustawy została przeprowadzona.</p> |
| 50. | Uwaga ogólna | Rada do Spraw Cyfryzacji | <p>W projekcie ustawy pojawia się dużo błędów językowych:</p> <ul style="list-style-type: none"> - 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...” | <p>Uwaga wyjaśniona/częściowo uwzględniona</p> <p>Wprowadzono zmiany we wskazanych jednostkach.</p> <p>Projekt ustawy nie zawiera sformułowania „unieważnienie danych w portfelu”, natomiast rozróżnia pojęcia „unieważnienie portfela” oraz „cofnięcia powiązania danych identyfikujących osobę prawną lub osobę fizyczną prowadzącą działalność gospodarczą z europejskim portfelem tożsamości cyfrowej” (zob. projektowany art. 14c ust. 4 ustawy o aplikacji mObywatel). Wprowadzenie tych pojęć to zabieg</p> |

| | | | | |
|-----|--------------|-----------------------------|--|---|
| | | | -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 | celowy projektodawcy, który przewidział, że cofnięcie powiązania skutkować będzie unieważnieniem portfela. Pojęcia „portfel”, „instancja”, „dane” nie mogą zostać ujednolicone, ponieważ mają odrębne znaczenia przypisane im w rozporządzeniu 910/2014 i aktach wykonawczych, w szczególności rozporządzeniu wykonawczym Komisji (UE) 2024/2979 z dnia 28 listopada 2024 r. ustanawiającego zasady stosowania rozporządzenia Parlamentu Europejskiego i Rady (UE) nr 910/2014 w odniesieniu do integralności i podstawowych funkcji europejskich portfeli tożsamości cyfrowej (Dz. Urz. UE L z 2024 r. str. 2979). |
| 51. | Uwaga ogólna | Prezes UODO | 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. | Uwaga uwzględniona OSR została zmieniona w tym zakresie. |
| 52. | Uwaga ogólna | Prezes UODO | 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 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. | Uwaga wyjaśniona/uwzględniona Wszystkie europejskie portfele tożsamości cyfrowej będą w taki sam sposób technicznie zorganizowane, jeżeli chodzi o ich podstawowe funkcje, zgodnie z rozporządzeniem wykonawczym Komisji (UE) 2024/2979 z dnia 28 listopada 2024 r. ustanawiające zasady stosowania rozporządzenia Parlamentu Europejskiego i Rady (UE) nr 910/2014 w odniesieniu do integralności i podstawowych funkcji europejskich portfeli tożsamości cyfrowej (Dz. U. UE. L. z 2024 r. poz. 2979). W związku z powyższym w zgodnie z rozporządzeniem Parlamentu Europejskiego i Rady (UE) 2016/679 oraz – w stosownych przypadkach – dyrektywa 2002/58/WE Parlamentu Europejskiego i Rady mają zastosowanie do wszystkich czynności przetwarzania danych osobowych na podstawie rozporządzenia (UE) nr 910/2014. Zgodnie z postulatem ocena skutków dla ochrony danych projektowanej ustawy została przeprowadzona. |
| 53. | Uwaga ogólna | Prezes UODO | Uwaga odnosi się analogicznie do wszystkich odwołań do art. 5a ust. 2 lit. a) rozporządzenia 910/2014 w projektowanej ustawie | Uwaga wymaga doprecyzowania |
| 54. | Uwaga ogólna | Polskie Centrum Akredytacji | Obecnie proponowane zapisy ustawowe wymagają uzupełnienia o poniższe zapisy. Art. XXX. 1. Akredytacji jednostce oceniającej zgodność, o której mowa w art. 3 pkt 18 rozporządzenia 910/2014, udziela Polskie Centrum Akredytacji. | Uwaga uwzględniona |

| | | | | |
|-----|--------------|-----------------------------|--|---------------------------|
| | | | <p>2. Do akredytacji jednostki oceniającej zgodność stosuje się odpowiednio przepisy rozdziału 4 ustawy z dnia 13 kwietnia 2016 r. o systemach oceny zgodności i nadzoru rynku (Dz. U. z 2025 r. poz. 568).</p> <p>3. Polskie Centrum Akredytacji uzgadnia z ministrem właściwym do spraw informatyzacji program akredytacji określający zasady i procesy akredytacji jednostek oceniających zgodność.</p> <p>4. Minister właściwy do spraw informatyzacji i Polskie Centrum Akredytacji mogą zawrzeć porozumienie o współpracy w zakresie monitorowania działalności jednostek oceniających zgodność i wzajemnym przekazywaniu informacji dotyczących tych jednostek.</p> | |
| 55. | Uwaga ogólna | Polskie Centrum Akredytacji | W OSR w tabeli na początku części 6 proponujemy dodanie pozycji 0,3 mln zł dla 2026 r. (rok zerowy) a następnie w kolejnych latach zwiększanie jej o 0,01 mln zł. | Uwaga uwzględniona |
| 56. | Uwaga ogólna | Polskie Centrum Akredytacji | <p>W uzasadnieniu proponujemy następujące zapisy:</p> <p>Wejście w życie projektowanej ustawy związane jest z rozszerzeniem działalności akredytacyjnej Polskiego Centrum Akredytacji (PCA) co powoduje konieczność zwiększenia zatrudnienia w wymiarze jednego etatu oraz przydzielenia dodatkowych zadań już zatrudnionym osobom. Projekt ustawy o zmianie ustawy o usługach zaufania oraz identyfikacji elektronicznej oraz niektórych innych ustaw zakłada, że Polskie Centrum Akredytacji jest zobowiązane do akredytacji jednostek oceniających zgodność na potrzeby ustawy oraz 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 (...).</p> <p>Przyjęte dyspozycje zobowiązują zatem PCA do opracowania i utrzymywania dedykowanego przedmiotowym przepisom prawa programu akredytacji, uruchomienie akredytacji wg opracowanego programu, w tym przeprowadzanie procesów akredytacji oraz nadzoru nad udzielonymi akredytacjami zgodnie z przepisami rozporządzenia 765/2008 oraz przepisami o systemach oceny zgodności i nadzoru rynku. Zastosowanie mają w tym przypadku wszystkie horyzontalne dokumenty PCA (np. DA-01 „Opis systemu akredytacji”, DA-08 „Prawa i obowiązki akredytowanego podmiotu”, DA-09 Zakres działalności akredytacyjnej PCA, DA-10 „Akredytacja w zakresach elastycznych” itp.) oraz dokumenty odnoszące się do danego typu jednostek oceniających zgodność, związane z rozszerzeniem działalności akredytacyjnej PCA o nowy obszar oceny zgodności przewidziany w przedmiotowym przepisie prawa.</p> | Uwaga uwzględniona |

| | | | | |
|--|--|--|---|--|
| | | | <p>W przypadku ustawy o zmianie ustawy o usługach zaufania oraz identyfikacji elektronicznej oraz niektórych innych ustaw UC122, przyjęte rozwiązanie zakłada również notyfikację akredytowanej jednostki oceniającej zgodność przez ministra właściwego do spraw gospodarki. W konsekwencji w procesie akredytacji i w procesach nadzoru nad udzieloną akredytacją zastosowanie mają zasady określone w dokumencie DA-11 „Akredytacja jednostek oceniających zgodność do celów notyfikacji”, co dodatkowo rozszerza zakres realizowanych przez PCA ocen i skomplikowanie nadzoru nad udzielonymi akredytacjami. Ponadto akredytacja do celów notyfikacji zobowiązuje PCA do udziału w pracach właściwych grup dla „notifying authorities” łącznie z reprezentantami organów notyfikujących i zainteresowanych stron.</p> <p>W konsekwencji powyższego, dla realizacji zadań określonych w przedmiotowym przepisie prawa PCA musi dysponować odpowiednimi - poszerzonymi kompetencjami (obszar ten dotychczas nie był objęty akredytacją) i poszerzonymi zasobami personelu. Kompetencje te będą obejmować znajomość wymagań i warunków akredytacji, znajomość i rozumienie zagadnień związanych z certyfikacją w specyficznym obszarze regulowanym przepisami oraz wiedzę z zakresu projektowanej regulacji prawnej. Kompetencje te muszą być pozyskane przez PCA w ramach poszerzenia zasobów osobowych do realizacji procesów akredytacji i nadzoru o ekspertów z wysokim poziomem kompetencji, z unikalnego obszaru technicznego o dużym znaczeniu gospodarczym, a tym samym wymagającego znacznych inwestycji finansowych dla pozyskania ekspertów.</p> <p>Powierzenie nowych obowiązków obecnym pracownikom PCA nie jest możliwe z punktu widzenia merytorycznego i ograniczonych możliwości posiadanych zasobów. Aktualnie PCA nie zatrudnia ekspertów z zakresu portfeli tożsamości cyfrowej, do której odnoszą się wdrażane przepisy i nie dysponuje wystarczającą wiedzą w tym zakresie. Ponadto, aktualny stan zatrudnienia PCA uniemożliwia nałożenie na obecnych pracowników wszystkich dodatkowych zadań wynikających z rozszerzenia działalności akredytacyjnej PCA w zakresie obszaru oceny zgodności określonej w projektowanym zakresie.</p> <p>Osoby te muszą dysponować wiedzą zarówno w odniesieniu do przepisów dotyczących portfeli tożsamości cyfrowej jak i w odniesieniu do rozwiązań odnoszących się do akredytacji i realizować nowe zadania w poniższych głównych kierunkach wymagających rozdzielenia stanowiskowej:</p> <p>a) w zakresie programu akredytacji będą zobowiązane do opracowania treści postanowień programu w korelacji z międzynarodowymi normami</p> | |
|--|--|--|---|--|

| | | | | |
|--|--|--|---|--|
| | | | <p>zharmonizowanymi i procedurami operacyjnymi PCA, uzgodnienia treści programu z regulatorem i zainteresowanymi stronami i przeprowadzenia procedury zatwierdzenia programu do stosowania, wdrożenie programu do działalności PCA (operacyjnie i merytorycznie) w celu rozszerzenia działalności akredytacyjnej. Po rozszerzeniu działalności akredytacyjnej, będą zobowiązane monitorować aktualność programu i zapewnić (w trybie jak powyżej) ciągłą przydatność programu do zamierzonego zastosowania;</p> <p>b) w zakresie procesu akredytacji będą zobowiązane do weryfikacji wniosku o akredytację, wstępnego przygotowania oceny akredytacyjnej, uzgodnienie zakresu oceny, komunikacji z jednostką oceniającą zgodność oraz zespołem oceniającym, podjęciem odpowiednich działań w systemie e-Akredytacja, brania udziału w ocenie jako audytorzy wiodący i bezpośrednio nadzorować ocenę (tu dodatkowo wymagana jest znajomość norm akredytacyjnych np. PN/ EN ISO 17065), po ocenie biorą udział w przygotowywaniu i zatwierdzaniu raportu oraz w działaniach związanych z obsługą kart niezgodności, przygotowują dokumenty w procesie decyzyjnym oraz biorą udział w procesie decyzyjnym. Jednocześnie wszystkie te czynności wykonywane są zgodnie z przepisami rozporządzenia nr 765/2008, ustawy o systemach oceny zgodności i nadzoru rynku oraz normy ISO/IEC 17011 co prowadzi np. do konieczności rozdzielenia osobowego w procesie realizacji oceny od podejmowania decyzji na bazie wyników tej oceny.</p> <p>c) w zakresie procesu nadzoru nad udzieloną akredytacją będą zobowiązane do opracowania programu nadzoru a następnie organizacji ocen w nadzorze oraz obserwacji działania jednostek oceniających zgodność w rzeczywistości. Proces organizacji ocen w nadzorze jest analogiczny do ocen akredytacyjnych.</p> <p>Reasumując, wejście w życie przepisów projektu ustawy będzie rodziło skutek w postaci zobligowania PCA do realizacji zadań związanych z akredytacją w nowym obszarze oceny zgodności, o których mowa w rozporządzeniu 910/2014. Przyjęcie przez PCA powyższych zadań związane jest z rozszerzeniem działalności akredytacyjnej o obszar wskazany w ustawie, a tym samym z koniecznością realizacji nowych zadań:</p> <ul style="list-style-type: none"> – opracowania i uzgodnienia z zainteresowanymi stronami programu akredytacji związanego z rozszerzeniem działalności akredytacyjnej, co wymaga zarówno bardzo dobrej znajomości rozwiązań dotyczących portfeli tożsamości cyfrowej jak i rozwiązań dotyczących systemu akredytacji | |
|--|--|--|---|--|

| | | | |
|--|--|---|--|
| | | <ul style="list-style-type: none"> – szkolenia audytorów PCA oraz spotkań informacyjnych z jednostkami oceniającymi zgodność, kandydującymi w przedmiocie akredytacji do celów projektowanego przepisu, – komunikacji z regulatorem i zainteresowanymi stronami w temacie przedmiotowego programu akredytacji, – organizacji procesów akredytacji jednostek ubiegających się o akredytację do celów uprawnienia do certyfikacji portfeli tożsamości cyfrowej, – monitorowanie i doskonalenie działalności akredytacyjnej w przedmiotowym obszarze <p>Oprócz konieczność zwiększenia zatrudnienia w PCA w wymiarze jednego etatu dla dwóch już zatrudnionych osób w obszarze procesów akredytacji zostaną przydzielone dodatkowe zadania związane z pełnieniem funkcji audytorów wiodących i weryfikacji merytorycznej wyników ocen w procesach akredytacji i nadzoru jednostek notyfikowanych. Nie przewiduje się wydatków majątkowych PCA w przedmiotowym obszarze. Zatrudnienie dodatkowej osoby w PCA wymagało będzie uwzględnienia w planie finansowym i zwiększenia wydatków w funduszu osobowym o 0,3 mln. zł. rocznie, po wejściu w życie projektowanego przepisu – począwszy od 2026 roku. (w 2026 kwota do aktualizacji w zależności od terminu wejścia w życie) Od 2026 r. zabezpieczone środki powinny wynieść 0,3 mln zł. Na kwotę tę składa się kwota na wynagrodzenie osoby zatrudnionej na etat oraz dodatki dla osób wykonujących zadania związane z wejściem w życie projektowanej ustawy.</p> | |
|--|--|---|--|