Tabela uwag
zgłoszonych w ramach uzgodnień
do projektu ustawy o zmianie ustawy o usługach zaufania oraz identyfikacji elektronicznej oraz niektórych innych ustaw (UD122)

Lp.	Jednostka redakcyjna, do której wnoszone są uwagi	Podmiot wnoszący uwagi	Zgłoszone uwagi	Stanowisko
1.	Art. 1 pkt 2 i pkt 3 – dot. art. 8 ust. 1 i 3a oraz ust. 4 ustawy	MFiG (MRiT)	Relacja pomiędzy zmienianym art. 8 ust. 1 i 3a oraz ust. 4 art. 8 ustawy. Zgodnie z proponowanym brzmieniem art. 8 ust. 1 minister właściwy do spraw informatyzacji wykreśla kwalifikowanego dostawcę usług zaufania, świadczoną przez niego kwalifikowaną usługę lub świadczoną przez niego usługę wydawania certyfikatów dostępu strony ufającej portfelowi i certyfikatów rejestracji strony ufającej portfelowi z rejestru w drodze decyzji. Zgodnie z ust. 3a decyzja o wykreśleniu z rejestru usługi wydawania certyfikatów dostępu strony ufającej portfela i certyfikatów rejestracji oznacza odebranie kwalifikowanemu dostawcy usług zaufania uprawnienia do wydawania takich certyfikatów. Art. 8 ust. 4 ustawy wskazuje przypadki, po wystąpieniu których minister ds. informatyzacji wydaje decyzję o wykreśleniu z rejestru. Ust. 4 odnosi się wyłącznie do kwalifikowanego dostawcy usług zaufania lub świadczonej przez niego kwalifikowanej usługi zaufania. Brak jest odniesienia do usługi wydawania certyfikatów dostępu strony ufającej portfelowi i certyfikatów rejestracji strony ufającej portfelów.	**Uwaga uwzględniona** W związku z uwzględnieniem licznych uwag różnych podmiotów dotyczących niekwalifikowanych usług zaufania wprowadzono zmiany w całym rozdziale 2 ustawy.
2.	Art. 1 pkt 3 - dot. art. 8	RCL	Mając na uwadze zakres zmian wprowadzonych do art. 8 ust. 1 dotyczących usługi wydawania certyfikatów dostępu strony ufającej portfelowi i certyfikatów rejestracji strony ufającej, wyjaśnienia (bądź ewentualnego uzupełnienia) wymaga pominięcie w przedmiotowym projekcie nowelizacji art. 7 pkt 2 (w zakresie konieczności informowania przez dostawcę usługi zaufania o zamiarze zaprzestania świadczenia także usług wydawania certyfikatów dostępu strony ufającej portfela oraz certyfikatów rejestracji strony ufającej portfela), a także pominięcie nowelizacji art. 8 ust. 4 – dotyczącego decyzji o wykreśleniu z rejestru, oraz art. 9 ustawy o usługach zaufania.	**Uwaga uwzględniona** W związku z uwzględnieniem licznych uwag różnych podmiotów dotyczących niekwalifikowanych usług zaufania wprowadzono zmiany w całym rozdziale 2 ustawy.
3.	Art. 1 pkt 3 – dot. art. 8 ust. 1 i 3a oraz ust. 5	MFiG (MRiT)	Relacja pomiędzy zmienianym art. 8 ust. 1 i 3a oraz ust. 5 art. 8 ustawy. Art. 8 ust. 5 wskazuje, że 5. Decyzja o wykreśleniu, o której mowa w ust. 1, jest podstawą wykreślenia dostawcy usług zaufania z zaufanej listy oraz może być podstawą do unieważnienia certyfikatów, o których mowa w art. 10 ust. 1 pkt 1. Z ustępu tego nie wynika, czy decyzja o wykreśleniu może być podstawą do unieważnienia certyfikatów dostępu	**Uwaga uwzględniona** W związku z uwzględnieniem licznych uwag różnych podmiotów dotyczących niekwalifikowanych usług zaufania wprowadzono zmiany w całym rozdziale 2 ustawy.

			strony ufającej portfelowi i certyfikatów rejestracji strony ufającej portfelowi. W ust. 3a wskazano jedynie, że decyzja o wykreśleniu z rejestru usługi wydawania certyfikatów (…) oznacza odebranie kwalifikowanemu dostawcy usług zaufania uprawnienia do wydawania takich certyfikatów, a czy jednocześnie będzie stanowić podstawę do unieważnienia tych certyfikatów?	
4.	Art. 1 pkt 3 – dot. art. 8 ust. 1 i 3a oraz art. 9	MFiG (MRiT)	Relacja pomiędzy zmienianym art. 8 ust. 1 i 3a oraz art. 9 ustawy. Na mocy art. 9 decyzja o wykreśleniu kwalifikowanego dostawcy usług zaufania z rejestru oraz decyzja o wykreśleniu wpisu kwalifikowanej usługi zaufania z rejestru podlega natychmiastowemu wykonaniu. Przepisów prawo o postępowaniu przed sądami administracyjnymi nie stosuje się. W nowelizacji nie wyjaśniono czy rygor natychmiastowej wykonalności będzie miał także zastosowanie do decyzji, o której mowa w art. 3a projektu.	**Uwaga uwzględniona** Wprowadzono zmiany w art. 9 ust. 1.
5.	Art. 1 pkt 3 lit. b - dot. dodawanego ust. 3a w art. 8	MFiG (MRiT)	Proponuję zastosować prawidłowa formę odmiany w kontekście technicznym i prawnym (eIDAS) - powinno być: „strony ufającej portfelowi” a nie: portfela, dodatkowo wyrażenie: certyfikatów rejestracji powinno być dookreślone poprzez dodanie: strony ufającej portfelowi. W treści innych jednostek redakcyjnych występuje poprawna forma, toteż zasadne jest, aby dokonać korekty w tej jednostce redakcyjnej. Proponowana treść: „3a. Decyzja o wykreśleniu z rejestru usługi wydawania certyfikatów dostępu strony ufającej portfelowi i certyfikatów rejestracji strony ufającej portfelowi oznacza odebranie kwalifikowanemu dostawcy usług zaufania uprawnienia do wydawania takich certyfikatów.	**Uwaga uwzględniona** W oficjalnym tłumaczeniu rozporządzenia wykonawczego Komisji (UE) 2025/848 z dnia 6 maja 2025 r. ustanawiającego 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) zarówno w tytule tego aktu prawnego jak w treści używany jest zwrot „strona ufająca portfela”. Z uwagi na prawidłową odmianę w języku polskim, przyjęto, że będzie stosowany zwrot „strona ufająca portfelowi”.
6.	Art. 1 pkt 5 - dot. art. 21a ust. 1 pkt 2 lit. c	RCL	Proponuje się wyjaśnienie i ewentualne doprecyzowanie określenia „systemu scentralizowanego”, którego funkcjonowanie będzie zapewniać minister właściwy do spraw informatyzacji, o którym mowa w rozporządzeniu 2025/846 i w którym przetwarza się dane osobowe określone w art. 22a ust. 3 zmienianej ustawy – z przepisów nie wynika bowiem, czy ten system jest systemem teleinformatycznym w rozumieniu ustawy z dnia 17 lutego 2005 r. o informatyzacji działalności podmiotów realizujących zadania publiczne (Dz. U. z 2025 r. poz. 1703).	**Uwaga wyjaśniona** Z przepisów rozporządzenia 2025/846 wynika, że system scentralizowany będzie systemem teleinformatycznym z uwagi na to, że będzie zapewniał zgodnie z art. 2 ust 2 tego rozporządzenia "otrzymywanie i walidację autentyczności informacji wymienionych w ust. 3 lub 4, stosownie do przypadku". Znaczy to, że będzie zapewniał możliwość wysyłania i odbierania danych ze środków identyfikacji elektronicznej, o których mowa w ust 3 i 4.
7.	Art. 1 pkt 5 - dot. art. 21a ust. 6a	RCL	Zauważenia wymaga, że wskazany przepis określa, przez odpowiednie odesłania, zakres przetwarzanych przez ministra właściwego do spraw informatyzacji danych osobowych osób, którym wydano środki identyfikacji elektronicznej (w celu uwierzytelnienia z wykorzystaniem węzła krajowego). Mając na uwadze wskazane w ust. 6a odesłania, wymaga podkreślenia, że zarówno przepisy rozporządzenia 2015/1501, jak i rozporządzenia 2024/2977, do których odsyła nowododawany przepis art. 21a ust. 6a	**Uwaga wyjaśniona** Przepis odnosi się do danych osobowych, a zatem do danych, które oznaczają wszelkie informacje o zidentyfikowanej lub możliwej do zidentyfikowania osobie fizycznej, a nie prawnej (zob. art. 4 pkt 1 RODO). Rodzaje danych będą wynikały z zakresów określonych we wskazanych aktach wykonawczych. Celowo nie przepisano ich do

			ustawy, wskazują: – w załączniku do rozporządzenia 2015/1501 – minimalny zestaw danych dotyczących osoby fizycznej oraz minimalny zestaw danych dotyczących osoby prawnej, przy czym każdy z tych zestawów może zawierać co najmniej jeden ze wskazanych w załączniku elementów dodatkowych, – w załączniku do rozporządzenia 2024/2977 – obowiązkowe dane identyfikujące osobę w przypadku osoby fizycznej oraz obowiązkowe dane identyfikujące osobę w przypadku osoby prawnej (przy czym załącznik określa także, dla każdej z tych osób – opcjonalne dane identyfikujące osobę). Wobec powyższego wyjaśnienia i ewentualnego doprecyzowania wymaga, dane której osoby (fizycznej czy prawnej) i jakiego rodzaju będzie przetwarzać minister właściwy do spraw informatyzacji na podstawie projektowanego przepisu ust. 6a. Wyjaśnienia wymaga także, na jakiej podstawie wskazany minister będzie przetwarzał dane, takie jak: imiona rodziców oraz numer dokumentu potwierdzającego tożsamość osób, o których mowa w ust. 6a pkt 3 – która nie została wyraźnie określona.	ustawy z dwóch powodów. Po pierwsze zostały one jasno opisane we wskazanych przepisach, co znaczy, że ich zakres jest znany i można to łatwo sprawdzić, a po drugie wskazane rozporządzenia mogą być nowelizowane w zakresie danych, które następnie będą mogły być przekazane w ramach uwierzytelniania transgranicznego - co ma obecnie miejsce w przypadku rozporządzenia 2024/2977. Imiona rodziców oraz seria nr dokumentu tożsamości będą przetwarzane w celu umożliwienia jednoznacznego dopasowania tożsamości, o którym mowa w art. 11a rozporządzenia eIDAS oraz w art. 22a projektu ustawy.
8.	Art. 1 pkt 5 lit. c – dot. art. 21a ust. 6a pkt 3 oraz art. 22a ust. 3 pkt 3	MFiG (MRiT)	W art. 21a ustawy z dnia 5 września 2016 r. o usługach zaufania oraz identyfikacji elektronicznej dodaje się ust. 6a - zgodnie z pkt 3 tego artykułu minister właściwy do spraw informatyzacji przetwarza dane osobowe osób, którym wydano środki identyfikacji elektronicznej obejmujące imiona rodziców osób oraz numer ważnego dokumentu potwierdzającego tożsamość osób (...). Wydaje się, że występuje niezgodność zakresu danych osobowych przetwarzanych w systemie scentralizowanym prowadzonym przez ministra właściwego ds. informatyzacji określonych w ww. art. 6a pkt 3 oraz dodawanym do ustawy o usługach zaufania (…) art. 22a ust. 3 pkt 3 - w tym drugim przypadku wskazane jest dodatkowo przetwarzanie numeru PESEL osób fizycznych, o czym nie ma mowy w art. 6a pkt 3 wskazującym zakres przetwarzanych danych osobowych w systemie scentralizowanym. Przepisy należy uspójnić.	**Uwaga wyjaśniona** W ust. 6a pkt 3 wskazuje się, że przetwarza się dane osobowe, o których mowa w rozporządzeniach wykonawczych 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.) oraz 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), a w ramach tych zakresów danych może znaleźć się numer PESEL.
9.	Art. 1 pkt 5 lit. c – dot. art. 21a ust. 6a pkt 3	MSWiA	Art. 1 pkt 5 lit. c – dot. art. 21a ust. 6a pkt 3 zmienianej ustawy o usługach zaufania oraz identyfikacji elektronicznej. Zgodnie z projektowanym przepisem minister właściwy do spraw informatyzacji przetwarza dane osobowe osób, którym wydano środki identyfikacji elektronicznej, obejmujące imiona rodziców osób oraz numer dokumentu potwierdzającego tożsamość osób, o których mowa w pkt 1 i 2.	**Uwaga uwzględniona** Wprowadzono zmiany w art. 21a ust. 6a pkt 3 i art. 22a ust. 3 pkt 3.

			Rozważenia wymaga doprecyzowanie danych dotyczących dokumentu potwierdzającego tożsamość przez wskazanie rodzaju, serii i numeru tego dokumentu. Analogiczną uwagę należy odnieść do art. 22a ust. 3 pkt 3 ustawy o usługach zaufania oraz identyfikacji elektronicznej.	
10.	Art. 1 pkt 5 lit. c – dot. art. 21a ust. 6a pkt 3	MI	Art. 1 pkt 5 lit. c ustawy zmieniającej w odniesieniu do art. 21a ust. 6a pkt 3 ustawy o usługach zaufania oraz identyfikacji elektronicznej (ustawa zmieniana). Proponowany art. 21a ust. 6a pkt 3 przewiduje przetwarzanie danych obejmujących imiona rodziców oraz numer dokumentu tożsamości osób, o których mowa w pkt. 1 i 2. Zakres ten wykracza poza ramy określone w przywołanych przepisach europejskich i prowadzi do nieuzasadnionego rozszerzenia katalogu danych podlegających przetwarzaniu. Budzi to również zastrzeżenia w świetle zasady minimalizacji danych wynikającej z art. 5 ust. 1 RODO.	**Uwaga wyjaśniona** Zakresy danych określone w projekcie ustawy wskazują na dane identyfikujące osobę jakie zostały wskazane w art. 2 ust. 3 i 4 rozporządzenia wykonawczego 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). 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 wykonawczego (UE) 2015/1501, w tym, w stosownych przypadkach, dodatkowymi informacjami lub procedurami uzupełniającymi. Mając na uwadze, że zestawy danych identyfikujących osobę o których mowa ww. rozporządzeniach: 2024/2977 oraz 2015/1501 nie są wystarczające do dopasowania tożsamości do rejestru PESEL, ponieważ nawet w przypadku zgodności imienia, nazwiska daty urodzenia i miejsca urodzenia nie można mieć pewności, że zestaw danych dotyczy tej samej osoby, przetwarzanie dodatkowych danych jest zatem niezbędne. Przewiduje się przetwarzanie dodatkowych danych obejmujących imiona rodziców oraz numer dokumentu tożsamości osób z uwagi na to, że takie dane znajdują się w rejestrze PESEL, do którego w pierwszej kolejności będzie realizowane dopasowanie.
11.	Art. 1 pkt 6 - dot. art. 21aa ust. 4	RCL	Wyjaśnienia wymaga skąd użytkownik może pobrać określony w tym przepisie dokument elektroniczny – nie jest bowiem jasne czy taka możliwość ma być zapewniania w ramach usługi, o której mowa w ust. 1 tego przepisu.	**Uwaga uwzględniona** Wprowadzono zmiany w art. 21aa ust. 4.
12.	Art. 1 pkt 9 – dot. art.	MSWiA	Art. 1 pkt 9 – dot. art. 22a ust. 2 pkt 1 projektowanej zmiany ustawy o usługach zaufania oraz identyfikacji elektronicznej.	**Uwaga wyjaśniona**

	22a ust. 2 pkt 1		Pod rozwagę poddaję przeredagowanie projektowanego pkt 1, aby określenie „która polega na identyfikacji elektronicznej, europejskim portfelu tożsamości cyfrowej lub innym środku identyfikacji elektronicznej" odnosiło się do usługi online, a nie do osoby fizycznej lub prawnej. Z tego względu proponuję następujące brzmienie przepisu: „1) dopasowywanie tożsamości do danych gromadzonych w rejestrze PESEL, gdy osoba fizyczna po raz pierwszy wystąpi z wnioskiem o udzielenie dostępu do świadczonej przez stronę ufającą, będącą osobą fizyczną lub prawną, zwaną dalej „stroną ufającą", usługi online, która polega na identyfikacji elektronicznej, europejskim portfelu tożsamości cyfrowej lub innym środku identyfikacji elektronicznej, lub na usłudze zaufania, a ta strona ufająca wymaga podania numeru PESEL w celu ustalenia, czy osoba fizyczna posiada już nadany numer PESEL;".	W ocenie projektodawcy przepis w obecnym brzmieniu odnosi się do usługi online świadczonej przez stronę ufającą, będącą osobą fizyczną lub prawną, a nie do tej osoby fizycznej lub prawnej.
13.	Art. 1 pkt 9	MFiG (MRiT)	W projekcie ustawy pojawia się koncepcja *scentralizowanego systemu dopasowywania tożsamości*. Wnoszę o doprecyzowanie, w jaki sposób system ten ma rozwiązać jeden z najczęściej występujących problemów praktycznych - brak numeru PESEL u użytkowników transgranicznych, który obecnie uniemożliwia lub znacząco utrudnia korzystanie z wielu usług publicznych w Polsce. • Jakie konkretne mechanizmy dopasowywania tożsamości będą wykorzystywane w przypadku osób nieposiadających numeru PESEL? Czy planowane jest stosowanie przypisywanych identyfikatorów zastępczych dla użytkowników transgranicznych?	**Uwaga wyjaśniona** Nie jest planowane przypisywanie identyfikatorów zastępczych na poziomie ogólnokrajowym. System scentralizowany ma co do zasady zweryfikować, czy transgraniczny użytkownik krajowej usługi online ma nadany już numer PESEL, ale jego celem nie jest nadanie takiego numeru, jeżeli użytkownik go nie ma. Z uwagi na to, że przepisy wymagające wzajemnego transgranicznego uznawania notyfikowanych środków identyfikacji elektronicznej obowiązują już od 29 września 2018 r., rozwiązania sektorowe odpowiednie dla różnych systemów powinny już funkcjonować. Z praktyki jednak wynikało, że w całej UE był problem z transgranicznym uznawaniem środków identyfikacji elektronicznej mimo, że za ich ważność ręczyły państwa członkowskie notyfikujące systemy identyfikacji, w ramach których są one wydawane. Znowelizowane rozporządzenie eIDAS podniosło ten problem do rangi odpowiedzialności państw członkowskich i umożliwiło (akt wykonawczy) poleganie na systemach scentralizowanych. Z uwagi na specyfikę różnych usług online nie można było jednak zaproponować nic poza centralną weryfikacją nr PESEL oraz (w przypadku niepowodzenia w tym zakresie) umożliwieniem przekazania za pośrednictwem systemu scentralizowanego do dostawcy usługi końcowej serii i numeru dokumentu tożsamości. Zaproponowano takie rozwiązanie, gdyż w przepisach krajowych, w których wskazuje się zakresy danych osobowych przetwarzanych w ramach różnych usług wymaga się podania

				numeru PESEL, a w przypadku gdy nie nadano numeru PESEL – najczęściej numeru i serii dokumentu potwierdzającego tożsamość. Oznacza to że jeżeli podmioty świadczące usługi online przetwarzają już takie dane, to mogą podjąć próbę ich dopasowania do danych, jakie zostaną przekazane z systemu scentralizowanego. Celem dopasowania tożsamości nie jest bowiem nadanie numeru PESEL i traktowanie takiego użytkownika jak użytkownika nowego, tylko dopasowanie tożsamości do istniejących danych, w których nie ma nr PESEL.
14.	Art. 1 pkt 9 – dot. art. 22a ust. 2 pkt 1	MI	Art. 1 pkt 9 ustawy zmieniającej w odniesieniu do art. 22a ust. 2 pkt 1 ustawy o usługach zaufania oraz identyfikacji elektronicznej (ustawa zmieniana). Użyte sformułowanie *„dopasowanie tożsamości do danych gromadzonych w rejestrze”* budzi wątpliwości co do jego precyzji, zwłaszcza w kontekście przetwarzania tak szerokiego zakresu informacji. Trudno ocenić, czy wynika to z niedostatecznego doprecyzowania projektowanych rozwiązań, czy z przyjęcia podejścia, które może prowadzić do niezamierzonych błędów identyfikacyjnych.	**Uwaga wyjaśniona** Przepis art. 3 pkt 55 eIDAS wskazuje, że dopasowanie tożsamości oznacza proces, w którym dane identyfikujące osobę lub środki identyfikacji elektronicznej są dopasowywane lub przyporządkowywane do istniejącego konta należącego do tej samej osoby. Ponadto w motywie 1 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) znajdujemy następujące wyjaśnienie: „(…) W takich przypadkach transgranicznego uwierzytelniania rejestry zawierające informacje dotyczące użytkownika portfela lub użytkownika notyfikowanych środków identyfikacji elektronicznej są czasami już dostępne dla strony ufającej za pośrednictwem rejestru strony ufającej lub rejestru zewnętrznego, a często w formie konta użytkownika. W takich przypadkach niektóre informacje dotyczące użytkownika uzyskane z portfeli lub notyfikowanych środków identyfikacji elektronicznej mogą być dopasowane przez tę stronę ufającą lub w jej imieniu. Można to osiągnąć na przykład przez zastosowanie scentralizowanego rozwiązania obsługiwanego przez podmiot sektora publicznego w zestawieniu z informacjami już posiadanymi przez tę stronę ufającą lub będącymi w rejestrze, z którego korzysta strona ufająca, orientacyjnie w rejestrze ludności lub bazie danych zawierającej informacje o koncie użytkownika”. Podsumowując, sformułowanie „dopasowywanie tożsamości do danych gromadzonych w rejestrze PESEL” jest uzasadnione i

				precyzyjne. Chodzi w nim o zweryfikowanie, czy dane identyfikujące osobę, w szczególności środek identyfikacji elektronicznej, można dopasować do określonego wpisu w ewidencji ludności.
15.	Art. 1 pkt 9 - dot. art. 22a ust. 2 pkt 2	RCL	Wyjaśnienia wymaga, w jakim trybie strona ufająca będzie żądała od osoby fizycznej podania dodatkowych danych w przypadku, gdy dopasowanie tożsamości będzie niejednoznaczne.	**Uwaga wyjaśniona** Będzie to usługa w systemie scentralizowanym.
16.	Art. 1 pkt 9 - dot. 22a ust. 3	RCL	Nie jest jasne, czy wymieniony przepis należy odnosić jedynie danych obligatoryjnych, czy także danych dodatkowych – spośród zamieszczonych w załączniku do rozporządzenia 2015/1501, a także do danych obowiązkowych i opcjonalnych – spośród zamieszczonych w załączniku do rozporządzenia 2024/2977 (przywołanych w uwadze 2.1. pkt 2 lit. b), co wymaga wyjaśnienia i ewentualnie doprecyzowania.	**Uwaga wyjaśniona** Przepis odnosi się do wszelkich danych spośród zamieszczonych w załączniku do rozporządzenia 2015/1501, a także do danych obowiązkowych i opcjonalnych – spośród zamieszczonych w załączniku do rozporządzenia 2024/2977 (w tym również metadanych). Z uwagi na to, że nie jest wiadome, jakie zakresy danych będą przesyłane przez użytkowników, nie można doprecyzować przepisów w tym zakresie.
17.	Art. 1 pkt 9 – dot. art. 22b ust. 1	MI	Art. 1 pkt 9 ustawy zmieniającej w odniesieniu do art. 22b ust. 1 ustawy o usługach zaufania oraz identyfikacji elektronicznej (ustawa zmieniana). Zasadne jest ustalenie, czy właściwe ministerstwo przeprowadziło ocenę skutków dla ochrony danych w odniesieniu do narzędzi informatycznych wykorzystywanych w procesach przewidzianych ustawą. Jeżeli taka ocena nie została wykonana, warto rozważyć jej przeprowadzenie, zwłaszcza w świetle obowiązków wynikających z art. 22b ust. 1 ww. ustawy zmienianej.	**Uwaga wyjaśniona** Ocena skutków dla ochrony danych osobowych zostanie przygotowana Należy nadmienić, że obowiązki wynikające z przywołanego w uwadze art. 22b ust. 1 ustawy, czyli prowadzenie rejestru stron ufających europejskiemu portfelowi tożsamości cyfrowej, o którym mowa w art. 3 ust. 1 rozporządzenia 2025/848, są efektem wymogów wskazanych właśnie w tym rozporządzeniu. Zgodnie z art. 3 ust. 4 tego rozporządzenia państwa członkowskie udostępniają publicznie w Internecie informacje określone w załączniku I dotyczące zarejestrowanych stron ufających portfela zarówno w formie nadającej się do odczytu przez człowieka, jak i w formie przeznaczonej do automatycznego przetwarzania.
18.	Art. 1 pkt 9 – dot. art. 22b ust. 1 pkt 5	MI	Art. 1 pkt 9 ustawy zmieniającej w odniesieniu do art. 22b ust. 1 pkt 5 ustawy o usługach zaufania oraz identyfikacji elektronicznej (ustawa zmieniana). Warto doprecyzować, w jakiej formie mają zostać określone wskazane zasady - czy będzie to instrukcja wewnętrzna, akt wykonawczy w postaci rozporządzenia, czy inny rodzaj regulacji.	**Uwaga wyjaśniona** Zakłada się, że będzie to instrukcja wewnętrzna. Przyjęto, że nie ma potrzeby wskazywania tego w ustawie, gdyż brak sformułowania w ustawie przepisu kompetencyjnego, który zobowiązywałby ministra do wydania rozporządzenia, wyklucza taką formą regulacji. Podobne rozwiązania zostały przyjęte w szeregu ustaw, np. w art. 78 ust. 2 ustawy o dokumentach paszportowych, art. 5 ust. 2 ustawy -Prawo o aktach stanu cywilnego, art. 10 ust. 9 ustawy o systemie powiadamiania ratunkowego, art. 14ha ust. 3 ustawy o

				ochronie przeciwpożarowej, art. 18 § 4 pkt 5 ustawy - Kodeks wyborczy.
19.	Art. 1 pkt 9 – dot. art. 22b ust. 1 pkt 6	MI	Art. 1 pkt 9 ustawy zmieniającej w odniesieniu do art. 22b ust. 1 pkt 6 ustawy o usługach zaufania oraz identyfikacji elektronicznej (ustawa zmieniana). Zasady zgłaszania naruszeń zostały już kompleksowo uregulowane w RODO. Warto więc rozważyć, czy wprowadzanie odrębnych, alternatywnych procedur jest uzasadnione, czy też może prowadzić do rozbieżności w stosowaniu obowiązujących przepisów.	**Uwaga wyjaśniona** Podobne rozwiązania zostały przyjęte w szeregu ustaw, np. w art. 78 ust. 2 ustawy o dokumentach paszportowych, art. 5 ust. 2 ustawy -Prawo o aktach stanu cywilnego, art. 10 ust. 9 ustawy o systemie powiadamiania ratunkowego, art. 14ha ust. 3 ustawy o ochronie przeciwpożarowej, art. 18 § 4 pkt 5 ustawy - Kodeks wyborczy.
20.	Art. 1 pkt 9 - dot. art. 22b ust. 5	RCL	W zakresie danych, które powinny być zawarte we wniosku o wpis do rejestru stron ufających europejskiego portfela tożsamości cyfrowej, określonych w załączniku I rozporządzenia 2025/848, proponuje się rozszerzenie przepisu i dodanie obok „danych” – także „informacji” zawartych w załączniku I do ww. rozporządzenia (taką „informacją” dotyczącą stron ufających portfela jest np. opis rodzaju usług, które świadczy strona ufająca portfela).	**Uwaga uwzględniona** Wprowadzono zmiany w art. 22b ust. 5.
21.	Art. 1 pkt 9 - dot. art. 22b ust. 6 i 7	RCL	Wyjaśnienia wymaga jaki jest cel weryfikacji przez ministra zgodności danych zawartych we wniosku z danymi wpisanymi do rejestrów wskazanych w pkt 1–5, w sytuacji, gdy strona ufająca pobiera dane do wniosku automatycznie bezpośrednio ze wskazanych rejestrów.	**Uwaga wyjaśniona** Formularz elektroniczny, o którym mowa w ust. 3 pkt 1, umożliwia po uwierzytelnieniu strony ufającej europejskiemu portfelowi tożsamości cyfrowej, pobranie danych z rejestrów, o których mowa w ust. 7, w celu wstępnego automatycznego uzupełnienia wniosku. Wniosek jednak może być składany również za pośrednictwem kwalifikowanego dostawcy usług zaufania świadczącego usługę wydawania certyfikatów dostępu strony ufającej portfelowi lub certyfikatów rejestracji strony ufającej portfelowi.
22.	Art. 1 pkt 9 - dot. art. 22b ust. 9	RCL	Przepis wymaga doprecyzowania przedmiot umowy, której elektroniczne poświadczenie zgodności odpisu z umową okazaną załącza się do wniosku (jakiej umowy ten przepis dotyczy).	**Uwaga uwzględniona** Wprowadzono zmiany we wprowadzeniu do wyliczenia w art. 22b ust. 9.
23.	Art. 1 pkt 9 - dot. art. 22b ust. 10	RCL	Wskazania wymaga, że zgodnie z art. 6 ust. 2 rozporządzenia 2025/848 podmioty rejestrujące bez zbędnej zwłoki rozpatrują wnioski o rejestrację i udzielają wnioskodawcy odpowiedzi na wniosek o rejestrację w terminie określonym w mającej zastosowanie polityce rejestracji, z wykorzystaniem odpowiednich środków oraz zgodnie z przepisami i procedurami państwa członkowskiego, w którym ustanowiono rejestr krajowy; kwestia ta wydaje się pominięta w projekcie, mając na uwadze, że zgodnie z projektowanym art. 22b ust. 10 wpis do rejestru następuje po zweryfikowaniu kompletności danych zawartych we wniosku, zgodnie z ust. 7–9 tego artykułu, i stanowi czynność materialnotechniczną, co wymaga wyjaśnienia.	**Uwaga uwzględniona** Wprowadzono zmiany w art. 22b ust. 10.

24.	Art. 1 pkt 9 - dot. art. 22b ust. 13	RCL	Wyjaśnienia wymaga jak należy rozumieć pojęcie „podmiotu publicznego”, o którym mowa w ust. 13 – gdyż nie zostało ono zdefiniowane w przepisach ustawy o usługach zaufania.	**Uwaga uwzględniona** Wprowadzono zmiany w art. 22b ust. 13.
25.	Art. 1 pkt 9 - dot. art. 22b ust. 17	RCL	Proponuje się ponowne przeanalizowanie i korektę wytycznych do wydania rozporządzenia wskazywanych w upoważnieniu zawartym we wskazanym przepisie, które w swojej treści odnoszą się nie do opracowania wzoru wniosku o wpis do rejestru ufających europejskiemu portfelowi tożsamości cyfrowej, a do kwestii związanych z procedurą składaniem wniosków.	**Uwaga uwzględniona** Wprowadzono zmiany w art. 22b ust. 17.
26.	Art. 1 pkt 9 - dot. art. 22d ust. 1	RCL	Przepis – w zakresie wniosku o zgłoszenie przez ministra atrybutów do katalogu atrybutów prowadzonego przez Komisję Europejską – wymaga doprecyzowania o wskazanie podmiotu, do którego składa się ten wniosek.	**Uwaga uwzględniona** Wprowadzono zmiany w art. 22d ust. 1.
27.	Art. 1 pkt 9 – dot. art. 22f	MSWiA	Art. 1 pkt 9 – dot. art. 22f ustawy o usługach zaufania oraz identyfikacji elektronicznej Wątpliwości budzi rozwiązanie zaproponowane w projektowanym brzmieniu dodawanego do ustawy o usługach zaufania oraz identyfikacji elektronicznej art. 22f, zgodnie z którym wyłącznie minister właściwy do spraw informatyzacji będzie mógł wydawać, w imieniu podmiotów odpowiedzialnych za źródła autentyczne, elektroniczne poświadczenia atrybutów, o których mowa w art. 45f rozporządzenia Parlamentu Europejskiego i Rady (UE) nr 910/2014 z dnia 23 lipca 2014 r. w sprawie identyfikacji elektronicznej i usług zaufania w odniesieniu do transakcji elektronicznych na rynku wewnętrznym oraz uchylającego dyrektywę 1999/93/WE (zwanego dalej „rozporządzeniem 910/2024”). Wydaje się, że podmiot publiczny będący emitentem dokumentów publicznych w rozumieniu art. 2 ust. 1 pkt 3 ustawy z dnia 22 listopada 2018 r. o dokumentach publicznych (Dz. U. z 2024 r. poz. 1669 i 1863 oraz z 2025 r. poz. 1881) powinien mieć możliwość, w porozumieniu z ministrem właściwym do spraw wewnętrznych (z wyłączeniem sytuacji, w której emitentem dokumentu publicznego jest minister właściwy do spraw wewnętrznych), wydawania elektronicznych poświadczeń atrybutów, o których mowa w art. 45f rozporządzenia 910/2014, w oparciu o dane zawarte w dokumencie publicznym lub powierzania wydawania tych poświadczeń innym podmiotom zapewniającym systemy teleinformatyczne niezbędne w procesie wytwarzania dokumentów publicznych lub dokonywania personalizacji blankietów dokumentów publicznych. Odpowiedniego dostosowania wymagałyby, w przypadku wprowadzenia zmian we wskazanym kierunku w projekcie ustawy, uzasadnienie oraz ocena skutków regulacji, w której należy uwzględnić koszty dotyczące wykonywania przez Centrum Personalizacji Dokumentów poświadczania	**Uwaga wyjaśniona** Istotą przepisów rozporządzenia eIDAS jest w tym przypadku nie to, kto wydaje odpowiednio zabezpieczone dokumenty publiczne, tylko kto jest odpowiedzialny za źródło autentyczne, w którym można potwierdzić drogą elektroniczną określone atrybuty. Wydawanie elektronicznych poświadczeń atrybutów co do zasady jest możliwe przez: - kwalifikowanych dostawców usług zaufania, - podmioty publiczne odpowiedzialne za źródła autentyczne, - podmioty publiczne wskazane przez państwa członkowskie do wydawania elektronicznych poświadczeń atrybutów w imieniu podmiotów publicznych odpowiedzialnych za źródła autentyczne. Ponadto z definicji źródła autentycznego zawartej w art. 3 pkt 47 rozporządzenia eIDAS wynika: „47) "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;” Łącznie oznacza to, że jeżeli emitent dokumentów publicznych w rozumieniu art. 2 ust. 1 pkt 3 ustawy o dokumentach publicznych jest jednocześnie podmiotem odpowiedzialnym za źródło autentyczne, czyli repozytorium lub system, w którym można zweryfikować ważność określonego atrybutu, jaki znajduje się w emitowanych przez ten podmiot dokumentach publicznych, to

			atrybutów przy personalizacji dokumentów na potrzeby dokumentów cyfrowych w wysokości 15 mln + 200 tys. miesięcznie.	znaczy, że może on również wprost na podstawie przepisów rozporządzenia eIDAS wydawać elektroniczne poświadczenia atrybutów w oparciu o źródło, którym zarządza. Oczywiście po warunkiem, że spełnia wymagania, jakie stawia się dostawcom usług zaufania wydającym takie poświadczenia. W celu wyeliminowania wątpliwości w tym zakresie zostały wprowadzone zmiany w art. 4 i art. 8 oraz dodawanym art. 22f ustawy o usługach zaufania oraz identyfikacji elektronicznej. Z uwagi na to, że podmiotem odpowiedzialnym za źródła autentyczne, o których mowa w załączniku VI pkt 1-6 oraz pkt 10, w części dotyczącej ewidencji kierowców jest minister właściwy do spraw informatyzacji, zasadne wydaje się, że ten właśnie organ powinien wydawać elektroniczne poświadczenie atrybutów jako podmiot publiczny odpowiedzialny za stosowne źródła autentyczne.
28.	Art. 1 pkt 9 - dot. art. 22f i 22g ust. 1	RCL	W których przyznaje się ministrowi właściwemu do spraw informatyzacji fakultatywność przy wydawaniu elektronicznych poświadczeń atrybutów, o których mowa w art. 45f rozporządzenia 910/2014, oraz elektronicznych poświadczeń atrybutów w rozumieniu art. 3 pkt 44 rozporządzenia 910/2014 – bez określenia żadnych przesłanek lub kryteriów wskazujących jakie okoliczności czy warunki będą brane pod uwagę przy skorzystaniu przez organ z tego uprawnienia; proponowany w wymienionych przepisach zakres swobodnego uznania wymaga wyjaśnienia i rozważenia jego dookreślenia z uwzględnieniem zapewnienia pewności co do prawa jego adresatom.	**Uwaga uwzględniona** Wprowadzono zmiany w art. 22f. Zakres uznaniowości ministra ograniczy się do kwestii określonych przepisami. Jest to powtórzenie na poziomie krajowym przepisów art. 8 ust. 2 rozporządzenia 2025/1569, w którym wskazuje się, że wnioski o włączenie schematów elektronicznych poświadczeń atrybutów podlegają ocenie Komisji pod względem stworzenia wspólnej bezpiecznej i niezagrażającej prywatności interakcji elektronicznej między obywatelami, przedsiębiorstwami i organami publicznymi, a także do wspierania interoperacyjności. Nie powinno się bowiem dopuścić do sytuacji, w której będzie ze środków publicznych realizowane wydawanie elektronicznych poświadczeń atrybutów, które nie będą spełniały takich warunków. Ponadto, zostało wprowadzone zmiany, powodujące, że wnioski do ministra właściwego do spraw informatyzacji o wydawanie elektronicznych poświadczeń atrybutów będą mogły składać wyłącznie podmioty odpowiedzialne za źródła autentyczne, a zatem te podmioty które i tak mają do tego prawo po spełnieniu wymagań, o których mowa w art. 45f ust. 2 eIDAS oraz wymogów krajowych dotyczących uzyskania wpisu do rejestru stron ufających i na zaufaną listę. Ponadto przepis z art. 3 pkt 46 rozporządzenia eIDAS: "46) elektroniczne poświadczenie atrybutów wydane przez podmiot sektora publicznego odpowiedzialny za źródło

				autentyczne lub w jego imieniu" oznacza elektroniczne poświadczenie atrybutu wydane przez podmiot sektora publicznego, który jest odpowiedzialny za źródło autentyczne, lub przez podmiot sektora publicznego, który jest wyznaczony przez państwo członkowskie do wydawania takich poświadczeń atrybutów w imieniu podmiotów sektora publicznego odpowiedzialnych za źródła autentyczne zgodnie z art. 45f oraz z załącznikiem VII;" Oznacza to, że rozporządzenie eIDAS przewiduje sytuację, w której państwo członkowskie wyznaczy podmiot sektora publicznego, upoważniony do wydawania takich poświadczeń atrybutów w imieniu podmiotów sektora publicznego odpowiedzialnych za źródła autentyczne. Przepis ustawy konsumuje tę możliwość.
29.	Art. 1 pkt 9 - dot. art. 22g ust. 3	MSWiA	Art. 1 pkt 9 - dot. art. 22g ust. 3 ustawy o usługach zaufania oraz identyfikacji elektronicznej. Projektowany przepis stanowi, że elektroniczne poświadczenie atrybutów, o którym mowa w ust. 1, wywołuje taki sam skutek prawny jak dokument wydany na podstawie przepisów prawa powszechnie obowiązującego potwierdzający dany stan prawny lub uprawnienia osób posługujących się nim, w tym dokument publiczny w rozumieniu ustawy z dnia 22 listopada 2018 r. o dokumentach publicznych (Dz. U. z 2024 r. poz. 1669 i 1863 oraz z 2025 r. poz. 1881), zaświadczenie w rozumieniu ustawy z dnia 14 czerwca 1960 r. - Kodeks postępowania administracyjnego lub dokument mobilny w rozumieniu ustawy dnia 26 maja 2023 r. o aplikacji mObywatel. Należy wskazać, że art. 45b ust. 1 rozporządzenia Parlamentu Europejskiego i Rady (UE) nr 910/2014 stanowi, że elektronicznemu poświadczeniu atrybutów nie można odmówić skutku prawnego ani dopuszczalności jako dowodu w postępowaniu sądowym wyłącznie z tego powodu, że ma postać elektroniczną lub że nie spełnia wymogów dotyczących kwalifikowanych elektronicznych poświadczeń atrybutów. W pierwszej kolejności wskazać należy, że nie jest jasne, dlaczego projektodawca odnosi się do dokumentu wydanego na podstawie przepisów prawa powszechnie obowiązującego potwierdzającego dany stan prawny lub uprawnienia osób posługujących się nim, w tym dokumentu publicznego w rozumieniu ustawy z dnia 22 listopada 2018 r. o dokumentach publicznych (Dz. U. z 2024 r. poz. 1669 i 1863 oraz z 2025 r. poz. 1881), zaświadczenia w rozumieniu ustawy z dnia 14 czerwca 1960 r. - Kodeks postępowania administracyjnego lub	**Uwaga wyjaśniona** Na wstępie należy zaznaczyć, że obowiązek polegania na europejskich portfelach tożsamości cyfrowej (w tym na danych identyfikujących osobę) wynika wprost z art. 5f ust. 1 i 2 rozporządzenia eIDAS. Z uwagi na to, że przepisy art. 5a ust. 4 rozporządzenia eIDAS jednoznacznie wskazują, że portfele takie zapewniają uwierzytelnianie wobec stron ufających w trybie online oraz, w stosownych przypadkach, w trybie offline, w celu uzyskania dostępu do usług publicznych i prywatnych. W nowym art. 14d ust. 1 ustawy o aplikacji mObywatel wskazano taki stosowny przypadek – adekwatnie do tego jaki ma już miejsce przypadku dokumentu mObywatel. Mając na uwadze, że europejskie portfele tożsamości cyfrowej z założenia spełniają wymagania dla wysokiego poziomu bezpieczeństwa i wymagają certyfikacji w tym zakresie, za oczywiste należało przyjąć, że to narzędzie powinno równie skutecznie potwierdzać tożsamość jak dokument mObywatel. Celem przepisu art. 22g ust. 3 ustawy o usługach zaufania oraz identyfikacji elektronicznej ustanawiającego skutki prawne elektronicznych poświadczeń atrybutów jest wyjście naprzeciw założeniom europejskich ram tożsamości cyfrowej określonych rozporządzeniem Parlamentu Europejskiego i Rady (UE) 2024/1183 z dnia 11 kwietnia 2024 r. w sprawie zmiany rozporządzenia (UE) nr 910/2014 w odniesieniu do ustanowienia europejskich ram tożsamości cyfrowej (Dz. U. UE. L. z 2024 r. poz. 1183 z późn. zm.).

			dokumentu mobilnego w rozumieniu ustawy dnia 26 maja 2023 r. o aplikacji mObywatel. Powyższa regulacja rodzi wątpliwości w kontekście posługiwania się elektronicznym poświadczeniem atrybutów. Powyższy projektowany przepis może być rozumiany w taki sposób, że elektroniczne poświadczenie atrybutów jest cyfrowym odpowiednikiem dokumentu publicznego, o ile jest to dokument potwierdzający stan prawny lub uprawnienia osób posługujących się nim. W związku z tym w pierwszej kolejności nie jest jasnym, czy zestaw atrybutów, które będą poświadczane w celu stwierdzenia tożsamości lub obywatelstwa również wywoła taki skutek jak wyżej opisany, uwzględniając, że ustawa o dokumentach publicznych odnosi się również do dowodu osobistego. Biorąc pod uwagę powyższe oraz mając na uwadze szerokie spektrum dokumentów regulowanych przez ustawę o dokumentach publicznych, wskazane odesłanie wymaga ponownej analizy.	Tamże w motywie 7 preambuły wyjaśniono między innymi że „Każdy powinien mieć możliwość bezpiecznego dostępu do usług publicznych i prywatnych, za pomocą ulepszonego systemu usług zaufania i zweryfikowanych dowodów potwierdzających tożsamość oraz elektronicznych poświadczeń atrybutów, takich jak kwalifikacje akademickie, w tym dyplomy ukończenia studiów wyższych, lub inne uprawnienia edukacyjne lub zawodowe. Europejskie ramy tożsamości cyfrowej mają na celu przejście od polegania wyłącznie na krajowych rozwiązaniach w zakresie tożsamości cyfrowej do zapewnienia elektronicznych poświadczeń atrybutów, które są ważne i prawnie uznawane w całej Unii. Dostawcy elektronicznych poświadczeń atrybutów powinni skorzystać na jasnym i jednolitym zestawie przepisów, natomiast administracje publiczne powinny mieć możliwość polegania na dokumentach elektronicznych w określonym formacie” W motywie 10 napisano między innymi: „Zarówno użytkownicy, jak i dostawcy usług powinni mieć możliwość korzystania z przyznania elektronicznym poświadczeniom atrybutów takiej samej wartości prawnej w całej Unii”. Warto jednocześnie podkreślić wyjątkowe cechy elektronicznego poświadczenia atrybutów oraz danych identyfikujących osobę, jakie europejskie portfele tożsamości cyfrowej zapewnią użytkownikom, a mianowicie możliwość selektywnego ujawniania danych – w szczególności potwierdzenia wyłącznie wieku, wykształcenia, określonych uprawnień publicznoprawnych itd. bez ujawniania przy tym jakichkolwiek danych, na których opiera się to stwierdzenie (motyw 14 rozporządzenia 2024/1183). Łącznie znaczy to, że należy zapewnić, aby co najmniej kwalifikowane elektroniczne poświadczenia atrybutów oraz elektroniczne poświadczenie atrybutów wydane przez podmiot sektora publicznego odpowiedzialny za źródło autentyczne lub w jego imieniu służyły celom, dla których zostały umocowane. Takie umocowanie dla kwalifikowanych elektronicznych poświadczeń atrybutów oraz elektronicznych poświadczeń atrybutów wydanych przez podmiot sektora publicznego zostało już ustanowione w art. 45b ust. 2 rozporządzenia eIDAS.

				Z uwagi na to, że skutek ten odnosi się do skutku prawnego „poświadczenia wydanego zgodnie z prawem w postaci papierowej" (ang. „legal effect as lawfully issued attestations in paper form"), celowo, w związku z tym, że na gruncie prawa krajowego takie sformułowania nie występują odwołano się między innymi do dokumentów publicznych w rozumieniu ustawy z dnia 22 listopada 2018 r. o dokumentach publicznych. W art. 22g ust. 3 ustawy o usługach zaufania oraz identyfikacji elektronicznej nie chodzi o to, że elektroniczne poświadczenia atrybutów będą jakkolwiek w pełni zastępowały dokumenty publiczne w rozumieniu art. 2 ust. 1 pkt 2 ustawy o dokumentach publicznych, tylko o to, że będą miały taki sam skutek prawny – czyli (jak określono w tym przepisie) mogły skutecznie „potwierdzać identyfikację osób, rzeczy lub potwierdzać stan prawny lub prawa osób posługujących się nimi". Taki jest właśnie cel europejskich portfeli tożsamości cyfrowej i elektronicznych poświadczeń atrybutów. W żadnej mierze przepis ten nie ma na celu wyeliminowania dokumentów publicznych w rozumieniu art. 2 ust. 1 pkt 2 ustawy o dokumentach publicznych. Należy dodać, że oczywistym oczekiwaniem użytkowników europejskiego portfela tożsamości cyfrowej jest możliwość skutecznego wykorzystywania go w usługach online i w stosownych przypadkach offline (podczas obecności fizycznej). Gdyby dane identyfikujące osobę lub elektroniczne poświadczenia atrybutów nie mogły skutecznie potwierdzać identyfikacji osób, rzeczy lub potwierdzać stanu prawnego lub prawa osób posługujących się nimi, to nie byłoby zasadne ich wydawanie i co za tym idzie również nie byłoby zasadne wprowadzanie europejskich ram tożsamości cyfrowej.
30.	Art.1 pkt 9 - dot. art. 22h ust. 3-5	RCL	W odniesieniu do przewidywanego trybu rozpatrywania wniosków o wydanie przez ministra właściwego do spraw informatyzacji europejskiego portfela tożsamości cyfrowej potwierdzenia wymaga, czy w zakresie nieuregulowanym w projekcie znajdą zastosowanie przepisy kodeksu postępowania administracyjnego (np. terminy, regulacje dotyczących uzupełnienia wniosku).	**Uwaga wyjaśniona** Nie przewiduje się wskazania, że w zakresie nieuregulowanym w projekcie znajdą zastosowanie przepisy Kodeksu postępowania administracyjnego.
31.	Art. 1 pkt 9 - dot. art. 22i pkt 3	RCL	Wyznacza się ministra właściwego do spraw informatyzacji do pełnienia roli organu nadzoru, o którym mowa w art. 46a rozporządzenia 910/2014 oraz do przekazywania odpowiednich informacji do Komisji	**Uwaga wyjaśniona** Zadania organu nadzoru zostały wskazane wprost w rozporządzeniu eIDAS w art. 46a.

			Europejskiej w tym zakresie – niejasny pozostaje zakres zastosowania tego przepisu, co wymaga doprecyzowania.	
32.	Art. 1 pkt 11 – dot. art. 23 pkt 2	Koordynator Służb Specjalnych	Zgodnie z projektowanym przepisem art. 23 pkt 2 ustawy z dnia 5 września 2016 r. *o usługach zaufania oraz identyfikacji elektronicznej,* minister właściwy do spraw informatyzacji *„po uzyskaniu opinii CSIRT GOV, CSIRT MON i CSIRT NASK, o których mowa w art. 2 pkt 1-3ustawy z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa (Dz. U. z 2024 r. poz. 1077), udostępnia kod źródłowy poszczególnych komponentów oprogramowania europejskiego portfela tożsamości, o którym mowa w ustawie z dnia 26 maja 2023 r. o aplikacji mObywatel”.* Wskazać należy, że obowiązek udostępnienia kodu źródłowego niesie za sobą szereg zagrożeń dla funkcjonowania europejskiego portfela tożsamości cyfrowej, w szczególności związanych z nieuprawnionym wykorzystaniem tego kodu. Dodatkowo udostępnienie kodu źródłowego może stanowić zagrożenie dla poufności i integralności danych, które zostaną powiązane z ww. portfelem. Podkreślić należy, że w rozporządzeniu elDAS 2.0. odniesiono się do upublicznienia przez państwo członkowskie kodu źródłowego komponentów oprogramowania użytkownika europejskiego portfela tożsamości. W motywie 33 ww. rozporządzenia zawarto uzasadnienie dla wprowadzenia obowiązku upublicznienia ww. kodu źródłowego, co znalazło odzwierciedlenie w art. 5a ust. 3 zdaniu pierwszym rozporządzenia elDAS, zgodnie z którym *„kod źródłowy komponentów oprogramowania użytkowego europejskich portfeli tożsamości cyfrowej musi być objęty licencją otwartego oprogramowania”.* Jednocześnie jednak dodano, że „w *niektórych przypadkach ujawnienie kodu źródłowego wykorzystywanych bibliotek programistycznych, kanału komunikacji lub innych elementów, które nie są przechowywane na urządzeniu użytkownika, mogłoby zostać ograniczone przez państwa członkowskie z należycie uzasadnionych powodów, zwłaszcza ze względu na bezpieczeństwo publiczne.”* Tym samym, art. 5a ust. 3 zdanie drugie rozporządzenia elDAS stanowi, że *„państwa członkowskie mogą postanowić, że z należycie uzasadnionych powodów nie ujawnia się kodu źródłowego poszczególnych komponentów innych niż zainstalowane na urządzeniach użytkownika.”* Wobec powyższego proponuję usunięcie z projektowanej ustawy obowiązku nałożonego na ministra właściwego do spraw informatyzacji	**Uwaga uwzględniona/wyjaśniona** Wprowadzono zmiany w art. 23 pkt 2 ustawy o usługach zaufania oraz identyfikacji elektronicznej. W odniesieniu do sugestii ponownego wykorzystania już posiadanych produktów cyfrowych, co powinno się przełożyć na optymalizację prowadzonych prac pod względem czasowym oraz ekonomicznym, m.in. wykorzystania dotychczas wykorzystywanych komponentów lub mikrousług, to tak właśnie się dzieje i już od pewnego czasu przygotowywane są rozwiązania, w możliwym zakresie, w taki sposób, aby mogły być one wykorzystane w europejskim portfelu tożsamości cyfrowej.

			do udostępniania kodu źródłowego poszczególnych komponentów oprogramowania europejskiego portfela tożsamości. Alternatywnie, jeżeli za konieczne zostanie uznane wprowadzenie ww. przepisu, niezbędne będzie doprecyzowanie brzmienia projektowanego art. 23 pkt 2 ustawy z dnia 5 września 2016 r. o usługach zaufania oraz identyfikacji elektronicznej na wzór art. 81a ustawy z dnia 26 maja 2023 r. o aplikacji mObywatel (Dz. U. z 2024 r. poz. 1275 z późn. zm.), zgodnie z którym „minister właściwy do spraw informatyzacji, po uzyskaniu opinii CSIRT GOT, CSIRT MON i CSIRT NASK, o których mowa w art. 2 pkt 1- 3 ustawy z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa (Dz. U. z 2024 r. poz. 1077), udostępni w Biuletynie Informacji Publicznej na swojej stronie podmiotowej kod źródłowy aplikacji mObywatel w zakresie niezagrażającym bezpieczeństwu tej aplikacji oraz jej użytkowników lub systemu mObywatel.” Tym samym projektowany art. 23 pkt 2 ustawy z dnia 5 września 2016 r. o usługach zaufania oraz identyfikacji elektronicznej otrzymałby następujące brzmienie: ,,2) po uzyskaniu opinii CSIRT GOT, CSIRT MON i CSIRT NASK, o których mowa w art. 2 pkt 1-3 ustawy z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa (Dz. U. z 2026 r. poz. 20 i 252), udostępnia kod źródłowy poszczególnych komponentów oprogramowania europejskiego portfela tożsamości, o którym mowa w ustawie z dnia 26 maja 2023 r. o aplikacji mObywatel, w zakresie niezagrażającym bezpieczeństwu tego portfela oraz jego użytkowników lub systemu zapewniającego funkcjonalności niezbędne do Jego działania;”. Niezależnie od powyższego, odnosząc się do zakładanej koncepcji, zgodnie z którą aplikacja mObywatel oraz europejski portfel tożsamości cyfrowej będą funkcjonowały rozdzielnie oraz niezależnie od siebie, należy rozważyć ponowne wykorzystanie już posiadanych produktów cyfrowych, co powinno się przełożyć na optymalizację prowadzonych prac pod względem czasowym oraz ekonomicznym. W tym aspekcie zasadnym podejściem byłoby m.in. posłużenie się dotychczas opracowanymi oraz wykorzystywanymi rozwiązaniami stworzonymi m.in. przez Centralny Ośrodek Informatyki, takimi jak np. komponenty interfejsu, moduły logiczne lub mikrousługi.	
33.	Art. 1 pkt 11 – dot.	MFiG (MF)	Należy zaktualizować publikator ustawy o ksc, w związku z publikacją tekstu jednolitego: (Dz. U. z 2026 r. poz.20) oraz mając na uwadze zmiany wprowadzone Ustawą z dnia 23 stycznia 2026 r. o zmianie	**Uwaga uwzględniona** Wprowadzono odpowiednie zmiany.

	art. 23 pkt 2		ustawy o krajowym systemie cyberbezpieczeństwa oraz niektórych innych ustaw (Dz. U. z 2026 r. poz. 252).	
34.	Art. 1 pkt 11 – dot. art. 23 pkt 6	MFiG (MRiT)	Należy uzupełnić nazwę rozporządzenia, do którego jest odwołanie art. 5b ust. 2 powinno być: 6) udostępnia publicznie informacje, o których mowa w art. 5b ust. 2 rozporządzenia 910/2014 (...)	**Uwaga uwzględniona** Wprowadzono odpowiednie zmiany.
35.	Art. 1 pkt 11	MSZ	W art. 5a ust. 9 rozporządzenia 910/2014 został nałożony obowiązek zapewnienia by europejski portfel tożsamości cyfrowej mógł zostać unieważniony w następujących przypadkach: a) na wyraźne żądanie użytkownika; b) w przypadku bezpieczeństwo europejskiego portfela tożsamości cyfrowej zostało skompromitowane; c) po śmierci użytkownika lub zaprzestaniu działalności przez osobę prawną. W projektowanej ustawie nie przewidziano przepisów regulujących mechanizm zawieszenia lub unieważnienia portfela tożsamości cyfrowej, w szczególności projekt nie określa podmiotów uprawnionych do podjęcia decyzji, trybu dokonania unieważnienia, relacji pomiędzy unieważnieniem portfela a unieważnieniem jego komponentów (np. certyfikatów). Analogiczna uwaga dotyczy braku ustanowienia procedury zawieszenia europejskiego portfela tożsamości cyfrowej, przewidzianego w art. 5a ust. 6 rozporządzenia 910/2014.	**Uwaga uwzględniona** Wprowadzono zmiany w art. 23 (dodano nowe punkty dot. kwestii poruszonych w uwadze).
36.	Art. 1 pkt 11	MSZ	W art. 46c rozporządzenia 910/2014 został nałożony obowiązek wyznaczenia pojedynczego punktu kontaktowego ds. usług zaufania, europejskich portfeli tożsamości cyfrowej i notyfikowanych systemów identyfikacji elektronicznej. Z przedłożonego do uzgodnień projektu ustawy nie wynika by ten obowiązek został spełniony. W tym względzie projektowana ustawa wymaga uzupełnienia.	**Uwaga uwzględniona** Wprowadzono zmiany w art. 23 (dodano nowy punkt dot. kwestii poruszonych w uwadze).
37.	Art. 1 pkt 14 - dot. art. 24a ust. 1 i 4	RCL	a) wyjaśnienia i doprecyzowania wymagają zastosowane w przepisie niejasne na gruncie projektowanych przepisów pojęcia „rozwiązania” i „dostawcy rozwiązania”, do których należy odnosić wniosek o uznanie jako europejskiego portfela tożsamości cyfrowej wydawanego niezależnie od jednego z państw członkowskich Unii Europejskiej (ust. 1) oraz jego uznania po pozytywnym rozpatrzeniu wniosku (ust. 4), b) doprecyzowania wymaga forma w jakiej zgodnie z zamiarem projektodawcy ma następować „uznanie” europejskiego portfela	**Uwaga uwzględniona** Wprowadzono zmiany w art. 24a ust. 1 i art. 24a ust. 4.

			tożsamości cyfrowej wydawany niezależnie od jednego z państw członkowskich Unii Europejskiej.	
38.	Art. 1 pkt 14 – dot. art. 24a ust. 4	MFiG (MRiT)	Po wyrażeniu: „i informuje Komisję Europejską i Grupę Współpracy o ... oraz" - brakuje części zdania o przedmiocie informacji przekazywanym KE i Grupie Współpracy	**Uwaga uwzględniona** Wprowadzono zmiany w art. 24a ust. 4.
39.	Art. 1 pkt 16-19	MSZ	Zgodnie z art. 16 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, w brzmieniu nadanym przez rozporządzenie Parlamentu Europejskiego i Rady (UE) 2024/1183 z dnia 11 kwietnia 2024 r. w sprawie zmiany rozporządzenia (UE) nr 910/2014 w odniesieniu do ustanowienia europejskich ram tożsamości cyfrowej, państwa członkowskie zapewniają, aby naruszenia rozporządzenia przez kwalifikowanych i niekwalifikowanych dostawców usług zaufania podlegały administracyjnej karze pieniężnej w maksymalnej wysokości co najmniej: a) 5 000 000 EUR – w przypadku gdy dostawca usług zaufania jest osobą fizyczną; lub b) w przypadku gdy dostawca usług zaufania jest osobą prawną – 5 000 000 EUR lub 1 % całkowitego rocznego światowego obrotu przedsiębiorstwa, do którego należał dostawca usług zaufania, w roku obrotowym poprzedzającym rok, w którym miało miejsce naruszenie, w zależności od tego, która z tych wartości jest wyższa. W projektowanej ustawie nie został określony wymiar kary dla ww. podmiotów, nie przewiduje go również ustawa o usługach zaufania oraz identyfikacji elektronicznej nie spełnia tych wymogów. W związku z tym projekt powinien zostać uzupełniony.	**Uwaga uwzględniona** Wprowadzono zmiany w rozdziale 7.
40.	Art. 1	RCL	Z uwagi na częste posługiwanie się w zmienianych przepisach pojęciem „strony ufającej" oraz „atrybutu" proponuje się ich zdefiniowanie przez odpowiednie odesłanie do określeń wprowadzonych przepisami rozporządzenia 910/2014.	**Uwaga wyjaśniona** Ustawa o usługach zaufania oraz identyfikacji elektronicznej nie zawiera słownika przenoszącego definicje znajdujące się w art. 3 rozporządzenia eIDAS. Było to rozwiązanie przyjęte przy pierwszej wersji tej ustawy zakładające, że nie ma potrzeby ponownego definiowania pojęć, które znajdują się w już przepisach eIDAS obowiązujących bezpośrednio. Podczas stosowania przepisów ustawy mimo braku takich przepisów wiadomo było co to jest kwalifikowany podpis elektroniczny, środek identyfikacji elektronicznej czy też strona ufająca, mimo

				że pojęcia były zdefiniowane tylko w eIDAS. W ocenie projektodawcy zasadne jest niezmienianie tej praktyki.
41.	Art. 4 pkt 3 lit. b – dot. art. 20ac ust. 2 pkt 1b	MI	Art. 4 pkt 3 lit. b ustawy zmieniającej w odniesieniu do art. 20ac ust. 2 pkt 1b ustawy o informatyzacji działalności podmiotów realizujących zadania publiczne (ustawa zmieniana). Pojawiają się wątpliwości, czy przewidziano skuteczne mechanizmy weryfikacji, że osoby fizyczne posiadające profil zaufany do reprezentowania podmiotów publicznych nadal są do tego uprawnione. Dotyczy to również procedur związanych z niezwłocznym odbieraniem uprawnień. Przykładowo: w przypadku rozwiązania stosunku pracy, jak długo były pracownik może jeszcze wykonywać czynności w imieniu podmiotu publicznego, skoro nadal dysponuje własnymi danymi identyfikacyjnymi? Doprecyzowanie tych kwestii wydaje się kluczowe dla zapewnienia bezpieczeństwa i integralności procesu.	**Uwaga wyjaśniona** Takie mechanizmy zostały określone w art. 20cd ust. 3 pkt 1 ustawy o informatyzacji działalności podmiotów realizujących zadania publiczne. Podmiot publiczny, który nadał uprawnienie do posługiwania się profilem zaufanym osoby fizycznej reprezentującej podmiot publiczny może unieważnić ten profil za pomocą swojego profilu zaufanego podmiotu publicznego. Istotą tej czynności jest to, że zostanie w ten sposób odebrana możliwość reprezentowania podmiotu publicznego, ale osoba fizyczna nadal będzie dysponowała swoim profilem zaufanym. Należy nadmienić, że zgodnie z projektowanym przepisem art. 20cd ust. 3 pkt 2 ustawy o informatyzacji działalności podmiotów realizujących zadania publiczne prawo do unieważnienia profilu zaufanego osoby fizycznej reprezentującej podmiot publiczny będzie miała również osoba dysponująca tym profilem.
42.	Art. 4 pkt 3 lit. b i pkt 4 lit. b	RCL	Wątpliwości budzi zakres projektowanej regulacji odnoszący się do pojęcia „podmiotu publicznego”, którym posługują się zarówno przepisy ustawy o informatyzacji (art. 2 ust. 1), jak i przepisy ustawy z dnia 18 listopada 2020 r. o doręczeniach elektronicznych (art. 2 pkt 6), zmienianej w art. 5 projektu. Należy podkreślić, że w obu przypadkach zakres pojęcia podmiotu publicznego określany jest nieco odmiennie. Mając na względzie przewidywane projektem wprowadzenie do ustawy o informatyzacji przepisów zawierających odesłania do instytucji prawnych wprowadzanych projektem do ustawy o doręczeniach elektronicznych rozważenia wymaga następujące zagadnienie. Na gruncie nowelizacji ustawy o doręczeniach elektronicznych (art. 5 projektu) wprowadza się do systemu prawa instytucję KPP (Katalogu Podmiotów Publicznych), do której odsyła się w dodawanym do ustawy o informatyzacji art. 20ac ust. 2 pkt 1a (w art. 4 pkt 3 lit. b projektu). Zgodnie z treścią tego odesłania w systemie, o którym mowa w art. 20aa ust. 1 ustawy 6 o informatyzacji, przetwarza się dane podmiotu publicznego (tu: w rozumieniu art. 2 ust. 1 tej ustawy), któremu wydano profil zaufany, obejmujące: nazwę zgodną z KPP i numer KPP – które z kolei należy odnosić do pojęcia podmiotu publicznego w rozumieniu ustawy o doręczeniach elektronicznych (kwestia ta pojawia się także w projektowanych art. 20ac ust. 2 pkt 1b, 1c, art. 20ad ust. 1a i 1b oraz art. 20cc ustawy o informatyzacji). Mając na uwadze powyższe, należy wskazać, że nazwy zgodnej z KPP i numeru KPP nie będą miały podmioty publiczne w rozumieniu ustawy o informatyzacji, takie jak instytuty badawcze, Centrum	**Uwaga uwzględniona** Proponowane przepisy art. 3 pkt 14 lit. b i c ustawy o informatyzacji działalności podmiotów realizujących zadania publiczne będą wskazywały na dane identyfikujące i opisujące podmiot publiczny wpisany do Katalogu Podmiotów Publicznych, o którym mowa w art. 10a ust. 3 ustawy o doręczeniach elektronicznych, który został wydany w sposób, o którym mowa w art. 20cc ustawy o informatyzacji działalności podmiotów realizujących zadania publiczne, oraz na dane identyfikujące i opisujących osobę fizyczną reprezentującą podmiot publiczny wpisany do KPP, który został wydany w sposób, o którym mowa w art. 20cd ustawy o informatyzacji działalności podmiotów realizujących zadania publiczne.

			Łukasiewicz oraz instytuty działające w ramach Sieci Badawczej Łukasiewicz – gdyż nie są one podmiotami publicznymi w rozumieniu art. 2 pkt 6 ustawy o doręczeniach elektronicznych. Powyższy problem wymaga ponownej analizy zakresów ww. pojęcia podmiotu publicznego i eliminacji niespójności z przedmiotowego projektu.	
43.	Art. 4 pkt 3 lit. b - dot. w art. 20ac ust. 2 pkt 1d	RCL	Proponuje się doprecyzowanie odesłania zawartego w tym przepisie, z uwagi na powielenie w nim danych, które są przetwarzane w systemie, o którym mowa w art. 20aa ust. 1 ustawy o informatyzacji. Dodawany projektem również w art. 20ac ust. 2 przepis pkt 1a wskazuje, że w przypadku podmiotu publicznego, któremu wydano profil zaufany w systemie, o którym mowa w art. 20aa ust. 1, przetwarza się dane, takie jak nazwa zgodna z KPP oraz numer KPP. Natomiast w dodawanym w art. 20ac ust. 2 przepisie pkt 1d wskazuje się, że w ww. systemie przetwarza się dane, o których mowa w art. 14a ust. 3 ustawy o aplikacji mObywatel (zmienianej w art. 6 projektu), tj. dane identyfikujące osobę prawną lub osobę fizyczną prowadzącą działalność gospodarczą obejmujące: nazwę – firmę – zgodną z wpisem do CEIDG, KRS, KPP, numer NIP, numer KRS oraz numer KPP. W obecnie proponowanym kształcie relacja ww. pkt 1a i 1d pozostaje nie w pełni zrozumiała.	**Uwaga wyjaśniona** Przepisy art. 20ac ust. 2 ustawy o informatyzacji działalności podmiotów realizujących zadania publiczne odnoszą się do zakresu danych przetwarzanych w systemie teleinformatycznym zapewniającym obsługę publicznego systemu identyfikacji elektronicznej. Punkty 1a-1c dodawane do tego przepisu dotyczą danych przetwarzanych w związku ze zmianami w profilu zaufanym. Pkt 1a odnosi się do danych jakie mogą być przetwarzane w tym systemie w związku z istnieniem profilu zaufanego podmiotu publicznego, któremu wydano profil zaufany, pkt 1b - do danych osoby fizycznej, której wydano profil zaufany osoby reprezentującej podmiot publiczny, a pkt 1c - do danych administratora profilu zaufanego wydanego podmiotowi publicznemu. Pkt 1d został dodany w związku z obsługą w publicznym systemie identyfikacji elektronicznej środka identyfikacji elektronicznej, jakim będzie europejski portfel tożsamości cyfrowej osoby prawnej. Będzie to środek identyfikacji elektronicznej dowolnej osoby prawnej w rozumieniu motywu 68 rozporządzenia eIDAS. Znaczy to, że zakres podmiotów, jakim można wydać dane identyfikujące osobę prawną posiadającą europejski portfel tożsamości cyfrowej jest znacząco większy niż w przypadku podmiotów, jakim można wydać dane identyfikujące osobę prawną posiadającą profil zaufany. Pkt 1a i 1d dotyczą danych przetwarzanych w środkach identyfikacji elektronicznej osób prawnych, ale przeznaczonych dla podmiotów należących do różnych zbiorów.
44.	Art. 5	MFiG (MF)	W art. 5 projektu zawarta jest zmiana do ustawy o doręczeniach elektronicznych która w tożsamej treści znajduje się w procedowanym projekcie ustawy z 19 lutego br. o zmianie ustawy o doręczeniach elektronicznych oraz niektórych innych ustaw (UD236) – do wyjaśnienia.	**Uwaga wyjaśniona** Jak wskazano w cz. VI uzasadnienia: „Przedmiotowe zmiany spowodowane są koniecznością wejścia w życie, najpóźniej wraz z przepisami dostosowującymi do europejskich ram tożsamości cyfrowej, przepisów umocowujących powstanie Katalogu Podmiotów Publicznych, który 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). W zakresie tych zmian, do projektu ustawy włączono przepisy procedowane w ramach projektu ustawy o zmianie ustawy o doręczeniach elektronicznych oraz niektórych innych ustaw (UD236). Odpowiednio, w zależności od postępu prac nad projektem UD236, niezbędne będzie bieżące uwzględnianie tych prac.”.
45.	Art. 5	MSWiA	W związku z równoczesnym przesłaniem do konsultacji dwóch projektów ustaw zmieniających ustawę o doręczeniach elektronicznych, tj. projektu ustawy o zmianie ustawy o doręczeniach elektronicznych oraz niektórych innych ustaw (UD236) – w wersji skierowanej do ponownych uzgodnień oraz projektu ustawy o zmianie ustawy o usługach zaufania oraz identyfikacji elektronicznej oraz niektórych innych ustaw, w których zakres zmian jest zbieżny tylko w części, wyjaśnienia wymaga, w którym projekcie i w jakim zakresie znajdą się ostatecznie zmiany przepisów ustawy o doręczeniach elektronicznych.	**Uwaga wyjaśniona** Jak wskazano w cz. VI uzasadnienia: „Przedmiotowe zmiany spowodowane są koniecznością wejścia w życie, najpóźniej wraz z przepisami dostosowującymi do europejskich ram tożsamości cyfrowej, przepisów umocowujących powstanie Katalogu Podmiotów Publicznych, który 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). W zakresie tych zmian, do projektu ustawy włączono przepisy procedowane w ramach projektu ustawy o zmianie ustawy o doręczeniach elektronicznych oraz niektórych innych ustaw (UD236). Odpowiednio, w zależności od postępu prac nad projektem UD236, niezbędne będzie bieżące uwzględnianie tych prac.”.
46.	Art. 5	RCL	Przedmiotowy projekt, w art. 5, nowelizuje ustawę z dnia 18 listopada 2020 r. o doręczeniach elektronicznych (Dz. U. z 2026 r. poz. 3) w zakresie dotyczącym wprowadzenia Katalogu Podmiotów Publicznych (KPP) – zauważyć należy, że tożsama zmiana jest wprowadzana projektem ustawy o zmianie ustawy o doręczeniach elektronicznych oraz niektórych innych ustaw (UD236) obecnie znajdującym się na etapie uzgodnień. Projektodawca wyjaśnia tę „dwutorową” nowelizację w uzasadnieniu projektu, wskazując na konieczność umocowania w przedmiotowym projekcie regulacji związanych z KPP, „który 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	**Uwaga wyjaśniona** Jak wskazano w cz. VI uzasadnienia: „Przedmiotowe zmiany spowodowane są koniecznością wejścia w życie, najpóźniej wraz z przepisami dostosowującymi do europejskich ram tożsamości cyfrowej, przepisów umocowujących powstanie Katalogu Podmiotów Publicznych, który 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

			profilu zaufanego podmiotu publicznego oraz wydawanie europejskiego portfela tożsamości cyfrowej osoby prawnej)", deklarując jednocześnie, w zależności od postępu prac nad projektem UD236, wzięcie pod uwagę tych prac. W tym kontekście, mając na uwadze inne przyczyny stanowiące o ratio legis obu projektów, a także możliwość zgłaszania odmiennych stanowisk i podjęcia odmiennych rozstrzygnięć w zakresie każdego z nich, zauważa się, że nie jest właściwe z legislacyjnego i proceduralnego punktu widzenia przeprowadzanie inicjatywy podwójnej nowelizacji ww. ustawy. W związku z powyższym proponuje się dalsze kontynuowanie prac nad wprowadzeniem zmian dotyczących KPP tylko w jednym z dwóch przygotowywanych w tym zakresie projektów nowelizacji i zrezygnowanie z tych prac w zakresie drugiego z projektów. Powyższy postulat dotyczy także proponowanych nowelizacji ustaw: ustawy z dnia 29 czerwca 1995 r. o statystyce publicznej (Dz. U. z 2024 r. poz. 1799 oraz z 2025 r. poz. 1792) – art. 2 projektu, oraz ustawy z dnia 20 sierpnia 1997 r. o Krajowym Rejestrze Sądowym (Dz. U. z 2025 r. poz. 869, 1556 i 1792) – art. 3 projektu. Również te zmiany są powielane w projekcie UD236. Jednocześnie Rządowe Centrum Legislacji uprzejmie informuje, że uwagi zgłoszone do projektów nowelizacji ww. ustaw w przypadku projektu ustawy UD236 (przy piśmie z dnia 18 marca 2026 r., znak RCL.DISIP.550.4.2025), pozostają aktualne.	podmiotu publicznego oraz wydawanie europejskiego portfela tożsamości cyfrowej osoby prawnej). W zakresie tych zmian, do projektu ustawy włączono przepisy procedowane w ramach projektu ustawy o zmianie ustawy o doręczeniach elektronicznych oraz niektórych innych ustaw (UD236). Odpowiednio, w zależności od postępu prac nad projektem UD236, niezbędne będzie bieżące uwzględnianie tych prac.".
47.	Art. 5	RCL	Jednocześnie Rządowe Centrum Legislacji uprzejmie informuje, że uwagi zgłoszone do projektów nowelizacji ww. ustaw w przypadku projektu ustawy UD236 (przy piśmie z dnia 18 marca 2026 r., znak RCL.DISIP.550.4.2025), pozostają aktualne (uwagi zgłoszone do ustawy UD236 zostały wymieniono w lp. 47 -53). <u>Podtrzymania wymagają uwagi zgłoszone przy piśmie z dnia 15 września 2025 r. dotyczące:</u> 1) art. 1 pkt 7 projektu w zakresie: a) art. 10a ust. 3 pkt 1 lit. s oraz pkt 2 lit. b ustawy z dnia 18 listopada 2020 r. o doręczeniach elektronicznych (Dz. U. z 2026 r. poz. 3), zwanej dalej „zmienianą ustawą", (uwaga nr 4 pkt 3 pisma, lp. 41 tabeli uwag) – dotycząca powielenia zakresu przetwarzanych w Katalogu Podmiotów Publicznych „danych o reprezentantach podmiotu" (pkt 1 lit. s) i danych „osób fizycznych, które są uprawnione do reprezentacji" (pkt 2 lit. b); inaczej niż wynika z przedstawionych przez Wnioskodawcę wyjaśnień, z projektowanych przepisów nie wynika zróżnicowanie wymaganych danych, w tym ze względu na ich źródło; mając na uwadze konieczność precyzyjnego i jednoznacznego sformułowania podstawy i zakresu przetwarzanych w Katalogu Podmiotów Publicznych Danych proponuje	**Uwaga uwzględniona** W zakresie uwagi z lit. a uwaga uwzględniona i przepis będzie wskazywał na dane o reprezentantach podmiotu i sposobie reprezentacji – są to dane z KRS. Projektowane przepisy będą wskazywały, że w KPP gromadzi się dane osób fizycznych (imię, nazwisko, numer PESEL oraz wykorzystywane do realizacji obowiązków służbowych numer telefonu, adres poczty elektronicznej lub adres do doręczeń elektronicznych), które są uprawnione do zarządzania podmiotem, o którym mowa w pkt 1. Odniesiono się zatem do określenia "osób uprawnionych do zarządzania", które zostało użyte w dodawanych art. 20cc do ustawy o informatyzacji. W zakresie uwagi z lit. b uwaga uwzględniona i minister właściwy do spraw informatyzacji będzie mógł wprowadzać, wycofywać lub aktualizować niektóre dane, o których mowa w art. 10a ust. 3 pkt 1, o podmiotach publicznych oraz o podmiotach niepublicznych realizujących zadania publiczne na podstawie danych udostępnionych w Biuletynie Informacji Publicznej

			się albo wyraźnie odróżnienie ww. danych, albo skreślenie z projektowanego art. 10a ust. 3 pkt 1 lit. s ogólnego wskazania dotyczącego danych o reprezentantach, b) art. 10c zmienianej ustawy (uwaga nr 4 pkt 8 lit. b pisma, lp. 49 tabeli uwag) – w zakresie konieczności wskazania rejestrów, z jakich mają pochodzić wprowadzane, cofane i aktualizowane dane (niektóre spośród określanych w projektowanym art. 10a ust. 3 pkt 1 zmienianej ustawy); zaproponowana ogólna kompetencja ministra właściwego do spraw informatyzacji do przetwarzania danych pochodzących z nieokreślonego katalogu rejestrów publicznych lub danych posiadanych przez tego ministra (a zwłaszcza, jak wyjaśnia Projektodawca, rejestrów, które w przyszłości mogą dopiero zostać utworzone) nie będzie stanowić wystarczającej podstawy prawnej jego działania; zakres i cele przetwarzania danych w rejestrze oparty jest bowiem o stosowną regulację ustawową wyznaczającą jednocześnie granice działania organu; zatem modyfikacja zakresu i celu przetwarzania danych w rejestrze prowadzonym na podstawie odrębnych przepisów ustawowych wymaga odpowiedniego i precyzyjnego dookreślenia również w przepisach rangi ustawowej (tym bardziej, że zakres odesłania proponowanego w art. 10c nie wyklucza przetwarzania również danych osobowych – np. imienia i nazwiska komornika sądowego, o których mowa w projektowanym art. 10a ust. 3 pkt 1 lit. a); Rządowe Centrum Legislacji mając na uwadze powyższe, proponuje rozważenie rezygnacji z obecnego brzmienia art. 10c i sformułowanie go na wzór projektowanego art. 10b (bądź rozbudowanie art. 10b) – wskazującego poszczególne rejestry lub systemy, z których minister będzie mógł pobierać dane, wraz ze wskazaniem danych pobieranych z tych rejestrów lub systemów, c) art. 10d ust. 2 zmienianej ustawy (uwaga nr 4 pkt 9 lit. a pisma, lp. 50 tabeli uwag) – dotycząca konieczności doprecyzowania przesłanek utworzenia konta dla podmiotu publicznego z urzędu przez ministra – w zaproponowanych przepisach minister może bowiem założyć konto podmiotowi publicznemu „jeżeli podmiot publiczny nie złoży wniosku, o którym mowa w ust. 1” – przy czym projekt nie określa np. terminów, w jakich podmiot ma obowiązek złożyć taki wniosek; z obecnej wersji projektu wynika, że konto z urzędu może być utworzone w każdych okolicznościach, co może budzić wątpliwości co do celowości składania w tej sprawie wniosku; we wskazanym zakresie proponuje się uzupełnienie projektowanej regulacji,	podmiotu publicznego lub w portalu danych, lub w innym systemie teleinformatycznym podmiotu publicznego albo podmiotu niepublicznego realizującego zadania publicznego, w trybie ustawy o otwartych danych i ponownym wykorzystywaniu informacji sektora publicznego, a także prostować oczywiste błędy i omyłki pisarskie. W zakresie lit. c doprecyzowano przepis i art. 10d ust. 1 i 3 będzie podstawą do tego, aby minister właściwy do spraw informatyzacji na wniosek podmiotu publicznego złożony w systemie teleinformatycznym w terminie 30 dni od dnia utworzenia tego podmiotu, przy użyciu którego prowadzony jest Katalog Podmiotów Publicznych z wykorzystaniem usługi online udostępnionej przez ministra właściwego do spraw informatyzacji, tworzył konto podmiotu w Katalogu Podmiotów Publicznych, które zawiera dane opisujące ten podmiot, o których mowa w art. 10a ust. 3, w zakresie w jakim dotyczą tego podmiotu. Natomiast jeżeli podmiot publiczny nie złoży w terminie wniosku minister właściwy do spraw informatyzacji tworzy, na podstawie danych powszechnie dostępnych, a więc z rejestrów i systemów, o których mowa w art. 10b i art. 10c, albo innych danych i informacji udostępnianych przez podmiot publiczny na swojej stronie podmiotowej w Biuletynie Informacji Publicznej, a jeżeli nie prowadzi strony podmiotowej w Biuletynie Informacji Publicznej – na swojej stronie internetowej, z urzędu temu podmiotowi konto podmiotu w Katalogu Podmiotów Publicznych. Minister właściwy do spraw informatyzacji powiadamia niezwłocznie podmiot publiczny o utworzeniu temu podmiotowi konta w Katalogu Podmiotów Publicznych. W zakresie uwagi z lit. d doprecyzowano czym jest konto podmiotu i konto administratora podmiotu: a) konto podmiotu w Katalogu Podmiotów Publicznych, to konto, które zawiera dane opisujące ten podmiot, o których mowa w art. 10a ust. 3, w zakresie w jakim dotyczą tego podmiotu, b) konto administratora podmiotu to konto służące do zarządzania danymi opisującymi ten podmiot, o których mowa w art. 10a ust. 3, w zakresie w jakim dotyczą tego podmiotu, na kontem koncie podmiotu w Katalogu Podmiotów Publicznych oraz do nadawania uprawnień.

			d) art. 10i zmienianej ustawy (uwaga 4 pkt 14, lp. 55 tabeli uwag) – dotycząca konieczności: – dookreślenia (art. 10i pkt 1) jakie dane spośród zawartych w art. 10a ust. 3 zmienianej ustawy, będą wymagały następnie uszczegółowienia planowanym w akcie wykonawczym (zgodnie z deklaracją Wnioskodawcy wyrażoną w wyjaśnieniach w tabeli uwag), – uzupełnienia materii ustawowej o ogólne warunki i sposób administrowania kontem podmiotu i kontem administratora podmiotu w Katalogu Podmiotów Publicznych, które w przepisach wykonawczych (art. 10i pkt 2) mają zostać uszczegółowione, – doszczegółowienia wytycznych do upoważnienia – w celu uniknięcia zarzutu ich pozorności;	W zakresie uwag do art. 10i przepis został doprecyzowany i uzupełniono materię ustawową o ogólne warunki i sposób administrowania kontem.
48.	Art. 5	RCL	Należy wskazać na konieczność uspójnienia przepisów dotyczących zakresu przetwarzania danych określanego w art. 10a ust. 1–3 i 6 zmienianej ustawy oraz w art. 20 ust. 1c pkt 3 lit. b ustawy z dnia 20 sierpnia 1997 r. o Krajowym Rejestrze Sądowym (Dz. U. z 2025 r. poz. 869, z późn. zm.) – zmienianej w art. 7 projektu; w niektórych przypadkach stanowi się bowiem wyłącznie o gromadzeniu danych w Katalogu Podmiotów Publicznych (w art. 10a ust. 1 we wprowadzeniu do wyliczenia i w ust. 2 zmienianej ustawy oraz w art. 7 projektu), w innych zaś stanowi się o przetwarzaniu danych (w art. 10a ust. 1 pkt 2, 5, 8 oraz w ust. 6 zmienianej ustawy), które jest pojęciem szerszym – art. 4 pkt 2 RODO;	**Uwaga uwzględniona** Uspójniono przepisy wskazując na „przetwarzanie” danych, w ramach którego mieści się również ich „gromadzenie”.
49.	Art. 5	RCL	w przypadku projektowanego art. 10d zmienianej ustawy: a) ust. 1 – należy uzupełnić regulację o niezbędne elementy wniosku o założenie konta w Katalogu (analogiczną uwagę należy odnieść do projektowanego art. 10d ust. 3 zmienianej ustawy, w zakresie wniosku o założenie konta w Katalogu dla podmiotu niepublicznego realizującego zadanie publiczne); wskazanie katalogu danych zawieranych we wniosku jest niezbędne – zgodnie bowiem z art. 10d ust. 5 projektu brak danych lub nieprawidłowe dane podane we wniosku powodują jego zwrot przez ministra, b) ust. 2 – wskazany przepis wymaga uzupełnienia o wskazanie sposobu powiadamiania podmiotu publicznego o założeniu konta tego podmiotu w Katalogu z urzędu (kwestia ta nie została określona);	**Uwaga uwzględniona/wyjaśniona** W zakresie lit. a – uwaga uwzględniona i przepis został doprecyzowany o minimalny zakres danych wniosku. Ponadto w związku ze zgłoszoną uwagą doprecyzowano, że wniosek składa się z wykorzystaniem usługi online udostępnionej przez ministra właściwego do spraw informatyzacji w systemie teleinformatycznym przy użyciu którego prowadzony jest Katalog Podmiotów Publicznych, w terminie 30 dni od dnia rozpoczęcia realizacji lub wsparcia świadczenia zadań publicznych na podstawie odrębnych przepisów albo powierzenia lub zlecenia realizacji tych zadań. Doprecyzowano także przepis o dane, jakie powinien zawierać wniosek oraz informacje o podstawie prawnej i terminie, jeżeli został określony, realizacji lub wsparcia świadczenia zadania publicznego albo powierzenia lub zlecenia tego zadania.

				W zakresie uwagi z lit. b – należy zauważyć, że sposób powiadamiania wynika już z ustawy o doręczeniach elektronicznych – art. 4 i art. 5 tej ustawy, które to przepisy również w przypadku ww. wniosków znajdą zastosowanie. MC posiada ADE i powiadomienie wymaga potwierdzenia nadania tym samym MC przekaże powiadomienie na ADE podmiotu publicznego albo niepublicznego realizującego zadania publiczne. Natomiast gdyby ten podmiot nie posiadał ADE powiadomienie zostanie przesłane PUH – uzasadnienie w tym zakresie zostanie uzupełnione.
50.	Art. 5	RCL	art. 10e zmienianej ustawy wymaga uzupełnienia o: a) niezbędne elementy wniosku o utworzenie konta administratora – nie będzie bowiem możliwe „odpowiednie" zastosowanie przepisu art. 10d ust. 1, ze względu na inny przedmiot wniosku, b) elementy procedury mającej zastosowanie w przypadku niezłożenia przez podmiot wniosku o utworzenie ww. konta;	**Uwaga uwzględniona/wyjaśniona** W zakresie lit. a doprecyzowano przepis przez wskazanie niezbędnych elementów wniosku o utworzenie konta administratora. W zakresie uwagi z lit. b – doprecyzowano procedurę postępowania, tworzenia konta podmiotu. Natomiast nie ma konieczności doprecyzowania procedury w przypadku nieutworzenia konta administratora podmiotu, bowiem istotne jest utworzenie konta podmiotu i konto podmiotu będzie zawierało dane z innych rejestrów.
51.	Art. 5	RCL	Zgodnie z projektowanym art. 10f zmienianej ustawy 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, wprowadzają do Katalogu Podmiotów Publicznych podmioty publiczne oraz podmioty niepubliczne realizujące zadania publiczne; we wskazanym wyżej katalogu znajdują się dane takie jak: nazwa lub firma, pod którą podmiot działa, adres siedziby, forma własności, wykonywana działalność (w tym rodzaj wykonywanej działalności), akt prawny będący podstawą działalności, dane o reprezentantach podmiotu, dane administratora skrzynki doręczeń (imię i nazwisko, numer PESEL, adres poczty elektronicznej) i informacje o jednostkach lokalnych, które, zgodnie z projektowanym art. 10b pkt 1, 3 i 5, są przekazywane do ww. Katalogu automatycznie za pośrednictwem interfejsu programistycznego aplikacji danego systemu, po utworzeniu konta podmiotu – z krajowego rejestru urzędowego podmiotów gospodarki narodowej, bazy adresów elektronicznych oraz Krajowego Rejestru Sądowego; powyższa niespójność wymaga więc weryfikacji i stosownej korekty zakresu danych, które samodzielnie wprowadzać będą podmioty, oraz danych przekazywanych z systemu automatycznie; Ponadto należy wskazać, że zgodne z art. 10c, część z tych danych może także wprowadzać do Katalogu minister właściwy do spraw	**Uwaga uwzględniona** Wprowadzono zmiany w art. 10f.

			informatyzacji – na podstawie danych z rejestrów publicznych lub na podstawie danych do których ma dostęp ze względu na prowadzenie przez niego systemów teleinformatycznych, w których są przetwarzane te dane – co także wymaga doprecyzowania sytuacji, w których minister uzupełnia te dane samodzielnie;	
52.	Art. 5	RCL	W przypadku projektowanego art. 10h zmienianej ustawy: a) ust. 1 – proponuje się doprecyzowanie zawartego w nim odesłania przez wymienienie konkretnych jednostek redakcyjnych, spośród zawartych w wyliczeniu w art. 10a ust. 3 pkt 1, które odnoszą się do danych osobowych wyłączonych z obowiązku udostępniania podmiotom publicznym i niepublicznym realizującym zadania publiczne, b) ust. 2 – wątpliwości budzi ogólne sformułowanie przesłanki cofnięcia z urzędu dostępu do danych polegającej na wystąpieniu „ryzyka naruszenia bezpieczeństwa", które proponuje się doprecyzować – nie wiadomo np. o jakim rodzaju bezpieczeństwa, które może być naruszone, jest w tym przepisie mowa, a co za tym idzie nie jest jasne czy zakres zastosowania przepisu będzie adekwatny do jego *ratio legis*;	**Uwaga uwzględniona** Wprowadzono zmiany w art. 10h.
53.	Art. 5	RCL	Odnośnie do art. 1 pkt 8 projektu w zakresie projektowanego art. 11 pkt 3 zmienianej ustawy wyjaśnienia także wymaga jaki tryb postępowania przewiduje Projektodawca w sytuacji, w której podmiot niepubliczny wpisywany do Katalogu Podmiotów Publicznych, będzie już wcześniej posiadał skrzynkę doręczeń i wskazanego administratora tej skrzynki.	**Uwaga wyjaśniona** Z uwagi na to, że podmiot niepubliczny realizujący zadania publiczne w związku z realizacją tych zadań będzie obowiązany do posiadania ADE (albo odrębnego ADE gdyby już na innej podstawie posiadał ADE), to znajdą zastosowanie ogólne zasady wpisywania i wykreślania tego ADE, odpowiednio zmienione w związku z dodaniem tej nowej kategorii podmiotów obowiązanych do posiadania ADE.
54.	Art. 5	MFiG (MF)	W kwestii utworzenia Katalogu Podmiotów Publicznych (rozdział 1a) wątpliwości budzą wzajemne relacje między tym katalogiem a istniejącym obecnie katalogiem adresów ADE. W przypadku utworzenia KPP i utrzymania istnienia obecnych funkcjonalności może dojść do niespójności tych dwóch źródeł - podmiot publiczny może mieć w tych dwóch rejestrach inne ADE. Dlatego proponujemy rozważenie, aby zamiast tworzyć nowy rejestr (KPP) rozszerzyć obecne funkcjonalności o znacznik podmiot publiczny i udostępnić dane z niego na zasadach opisanych jako planowane dla KPP. Pozwoli to utrzymać istniejące funkcjonalności (z drobnymi rozszerzeniami). W przypadku utworzenia nowego rejestru (KPP) koszty mogą być wyższe, ponieważ może się okazać konieczna integracja z obydwoma rozwiązaniami. Wydaje się to nieekonomiczne i nieracjonalne. Dlatego proponujemy usunięcie zapisów o KPP, a zamiast tego rozszerzenie zakresu danych w aktualnym rejestrze ADE.	**Uwaga wyjaśniona** Celem Katalogu Podmiotów Publicznych jest stworzenie rejestru podmiotów publicznych, który będzie referencyjny (będzie stanowić autentyczne źródło danych) dla wszelkich potrzeb związanych z ustaleniem danych podmiotu publicznego. Podobnie jak ma to miejsce w zakresie spółek wpisanych do Krajowego Rejestru Sądowego czy osób fizycznych prowadzających jednoosobową działalność gospodarcza, wpisaną do Centralnej Ewidencji i Informacji o Działalności Gospodarczej. Przedmiotowy rejestr będzie niezbędny w celu zasilania referencyjnymi danymi: Bazy Adresów Elektronicznych (w rozumieniu art. 25 ustawy z dnia 18 listopada 2020 r. o doręczeniach elektronicznych), ale również rejestru stron ufających (o którym mowa w art. 3 ust. 1 rozporządzenia wykonawczego Komisji (UE) 2025/848 z dnia 6 maja 2025 r.

				ustanawiającego zasady stosowania rozporządzenia Parlamentu Europejskiego i Rady (UE) nr 910/2014 w odniesieniu do rejestracji stron ufających portfela), a nadto niezbędnymi do funkcjonowania w przyszłości europejskiego portfela biznesowego.
55.	Art. 5 pkt 2	MI	Art. 5 pkt 2 ustawy zmieniającej w odniesieniu do dodanego nowego Rozdziału 1a ustawy o doręczeniach elektronicznych (ustawa zmieniana). Postuluję wyłączenie z Katalogu Podmiotów Publicznych informacji, które są objęte tajemnicą przedsiębiorstwa lub chronione na podstawie ustawy z dnia 5 sierpnia 2010 r. o ochronie informacji niejawnych (Dz. U. z 2025 r. poz. 1209) oraz opracowanie procedury dotyczącej weryfikacji ww. okoliczności (ewentualnie dookreślić to w rozporządzeniu, o którym mowa w dodawanym art. 10i ww. ustawy zmienianej).	**Uwaga wyjaśniona** W KPP gromadzone są przede wszystkim dane gromadzone w innych rejestrach (REGON, KRS, BAE).KPP nie zawiera danych, które są objęte tajemnicą przedsiębiorstwa lub chronione na podstawie ustawy z dnia 5 sierpnia 2010 r. o ochronie informacji niejawnych. Należy również zauważyć, że już obecnie większość tych danych (oprócz danych osobowych), jest również dostępna na portalu otwarte dane.
56.	Art. 5 pkt 2	MI	Art. 5 pkt 2 ustawy zmieniającej w odniesieniu do art. 10a ust. 3 pkt 1 ustawy o doręczeniach elektronicznych (ustawa zmieniana). Zasadne jest wyłączenie z Katalogu Podmiotów Publicznych informacji o jednostkach lokalnych oraz siedzibach podmiotów publicznych posiadających obiekty, o których mowa w rozporządzeniu Rady Ministrów z dnia 21 kwietnia 2022 r. w sprawie obiektów szczególnie ważnych dla bezpieczeństwa lub obronności państwa oraz ich szczególnej ochrony (Dz. U. poz. 880) - jednym z rodzajów obiektów uznanych za szczególnie ważne dla bezpieczeństwa lub obronności państwa.	**Uwaga wyjaśniona** W KPP nie są gromadzone takie dane, bowiem w KPP są dostępne dane już ujawnione w innych rejestrach (REGON, KRS). Ponadto w przypadku danych niepobieranych z innych rejestrów, a podawanych przez podmiot, nie zostaną ujawnione w KPP, jeżeli są na mocy odrębnych przepisów objęte wyłączeniem (w tym objęte tajemnicą).
57.	Art. 5 pkt 2	MFiG (MRiT)	W uzasadnieniu do projektu wskazano, że w zakresie tych zmian, do projektu ustawy włączono przepisy procedowane w ramach projektu ustawy o zmianie ustawy o doręczeniach elektronicznych oraz niektórych innych ustaw (UD236). Odpowiednio, w zależności od postępu prac nad projektem UD236, niezbędne będzie bieżące uwzględnianie tych prac. Zwracam uwagę na zgłaszane uwagi w odniesieniu do prac UD236. MRIT zgłaszał uwagi m.in. do art: Art. 10a ust. 3 pkt 1 lit. g – propozycja dodania: „adres siedziby, o ile posiada”. W przypadku podmiotów niepublicznych realizujących zadania publiczne wpisanych w CEIDG nie każdy z tych podmiotów posiada adres siedziby. Z art. 10b wynika, że adres siedziby jest przekazywany automatycznie z rejestru REGON do Katalogu Podmiotów Publicznych, po utworzeniu konta podmiotu. Z kolei GUS pozyskuje dane na temat osób fizycznych prowadzących działalność gospodarczą z CEIDG. W rejestrze CEIDG oraz w rejestrze REGON znajdują się podmioty niepubliczne realizujący zadania publiczne bez wskazania adresu siedziby/adresu stałego miejsca wykonywania działalności gospodarczej.	**Uwaga uwzględniona/wyjaśniona** 1. W zakresie art. 10a ust. 3 pkt 1 lit. g - uwaga uwzględniona. 2. W zakresie art. 10a ust. 3 pkt 1 lit. h - zgodnie z art. 10f dane wskazane w tym przepisie, 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. Przepis ten dotyczy również adresu do korespondencji (lit. h). 3. W zakresie art. 10a ust. 3 pkt 1 lit. j - uwaga uwzględniona poprzez zmianę wyrazów „data powstania podmiotu" na "data rozpoczęcia działalności". Data rozpoczęcia działalności wypełnia ogólne założenia projektowe jednocześnie zgodnie ze

			Art. 10a ust. 3 pkt 1 lit h) adres do korespondencji. Z projektu nie wynika skąd będzie pobierana informacja dotycząca adresu do korespondencji. Rejestr REGON nie gromadzi informacji na temat adresu do korespondencji. Art. 10a ust. 3 pkt 1 lit j) data powstania podmiotu". Propozycja dodania w kolejnej literze „data rozpoczęcia działalności". Rejestr REGON rozróżnia datę powstania podmiotu oraz datę rozpoczęcia działalności. Złożenie wniosku o wpis do CEIDG nie jest jednoznaczne z datą rozpoczęcia działalności (wpis ma charakter deklaratoryjny a zatem we wniosku można wpisać datę rozpoczęcia działalności gospodarczej wcześniejszą niż data złożenia wniosku). Przedsiębiorca w CEIDG ma obowiązek podać datę rozpoczęcia działalności zgodnie ze stanem faktycznym. Może wpisać datę wsteczną, bieżącą lub datę przyszłą	wskazaniami zgłaszającego obejmuje swym "zakresem" podmioty w CEIDG.
58.	Art. 5 pkt 2 – dot. art. 10a ust. 3 pkt 2 lit. a	MI	Art. 5 pkt 2 ustawy zmieniającej w odniesieniu do art. 10a ust. 3 pkt 2 lit. a ustawy o doręczeniach elektronicznych (ustawa zmieniana). Zasadne jest doprecyzowanie, co jest rozumiane przez osoby, które *„kierują"* podmiotami, w szczególności, że odrębnie w lit. b jest mowa osobach reprezentujących, więc bezsprzecznie katalog osób *„kierujących"* jest szerszy niż tylko członkowie zarządów czy prezesi państwowych osób prawnych, co może budzić wątpliwość kto jest *„osobą kierującą"*.	**Uwaga uwzględniona** Zmieniono pkt 2, który będzie dotyczył danych osób fizycznych (imię, nazwisko, numer PESEL oraz wykorzystywane do realizacji obowiązków służbowych numer telefonu, adres poczty elektronicznej lub adres do doręczeń elektronicznych), które: a) są uprawnione do zarządzania podmiotem, o którym mowa w pkt 1, oraz b) administrują kontem podmiotu w Katalogu Podmiotów Publicznych. Zaproponowano zatem odniesienie się do określenia "osób uprawnionych do zarządzania", które zostało użyte w art. 20cc ustawy o informatyzacji działalności podmiotów realizujących zadania publiczne – w celu zachowania spójności przepisów.
59.	Art. 5 pkt 2	MFiG (MRiT)	Dotyczy niepowtarzalnego identyfikatora nadanego przez jedno z państw członkowskich UE. Art. 10a ust. 3 pkt 3 W Katalogu Podmiotów Publicznych gromadzi się i przetwarza następujące dane: imię i nazwisko administratora skrzynki doręczeń podmiotu, o którym mowa w pkt 1, jego adres poczty elektronicznej oraz numer PESEL, a jeżeli nie został nadany – niepowtarzalny identyfikator nadany przez jedno z państw członkowskich Unii Europejskiej dla celów transgranicznej identyfikacji, o którym mowa w rozporządzeniu wykonawczym Komisji 2015/1501. W art. 10b pkt 3 lit b) - imię i nazwisko administratora skrzynki doręczeń podmiotu, o którym mowa w art. 10a ust. 3 pkt 1, jego adres poczty elektronicznej oraz numer PESEL, a jeżeli nie został nadany – niepowtarzalny identyfikator nadany przez jedno z państw członkowskich Unii Europejskiej dla celów transgranicznej identyfikacji, o którym mowa w rozporządzeniu wykonawczym Komisji 2015/1501; Rozporządzenie wykonawcze Komisji 2015/1501 stanowi, że niepowtarzalny	**Uwaga wyjaśniona /uwzględniona** Nie ma potrzeby weryfikacji niepowtarzalnego identyfikatora nadanego przez jedno z państw członkowskich UE ani żadnych innych danych identyfikujących osobę znajdujących się w środkach identyfikacji elektronicznej pod kątem ich autentyczności, gdyż obowiązek polegania na tych danych i co za tym idzie uznawania ich za autentyczne wynika wprost z art. 6 rozporządzenia eIDAS. Możliwość weryfikacji zapewniają notyfikujące państwa członkowskie UE zgodnie art. 7 lit. f rozporządzenia eIDAS. Ponadto w związku ze zgłoszoną uwagą dokonano odpowiednich zmian w art. 10a ust. 3 pkt 3.

			identyfikator jest zbudowany przez wysyłające państwo członkowskie zgodnie ze specyfikacjami technicznymi do celów transgranicznej identyfikacji, który jest możliwie jak najtrwalszy. Z projektu nowelizacji nie wynika w jaki sposób będzie następowała weryfikacja niepowtarzalnego identyfikatora nadanego przez jedno z państw członkowskich UE pod kątem jego autentyczności? Kto będzie dokonywał tej weryfikacji? I czy będzie tworzony rejestr umożliwiający weryfikację poprawności ww. identyfikatorów.	
60.	Art. 6	MFiG (MRiT)	Zgodnie z projektem, użytkownikiem europejskiego portfela tożsamości cyfrowej może zostać osoba uwierzytelniona przy użyciu Profilu Zaufanego, pod warunkiem przeprowadzenia dodatkowej weryfikacji tożsamości. Jakie dokładnie formy dodatkowej weryfikacji tożsamości będą wymagane od osoby korzystającej z Profilu Zaufanego? Projekt przewiduje, że minister właściwy do spraw informatyzacji zapewni usługę weryfikacji określonych danych. Wnoszę o doprecyzowanie założeń i parametrów technicznych tego rozwiązania.	**Uwaga wyjaśniona** 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 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 ma podstawie art. 5a ust. 24 rozporządzenia eIDAS. 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.
61.	Art. 6 pkt 1	RCL	a) w zakresie dodawanych w art. 1 przepisów pkt 6 i 7 ustawy o aplikacji mObywatel – ponownej analizy i potwierdzenia poprawności wymaga odesłanie w przepisie zakresowym do art. 5a ust. 2 lit. a rozporządzenia 910/2014, w którym wyznacza się państwom członkowskim możliwość bezpośredniego zapewnienia europejskiego portfela tożsamości cyfrowej (jako co najmniej jednego ze wskazanych w tym rozporządzeniu sposobów zapewnienia tej instytucji) – w miejsce odesłania do definicji europejskiego portfela tożsamości cyfrowej zawartego w art. 3 pkt 42 ww. rozporządzenia (przy czym definicję taką proponuje się zamieścić w słowniczku zwartym art. 2 ustawy o aplikacji mObywatel); b) proponuje się weryfikację i wyjaśnienie czy proponowane w projekcie brzmienie przepisu zakresowego w pełni odzwierciedla zakres regulacji wprowadzanych do zmienianej ustawy o aplikacji mObywatel dotyczących europejskiego portfela tożsamości	**Uwaga uwzględniona** Zmodyfikowano odesłania znajdujące się w pkt 6 i 7. W celu pełnego odzwierciedlenia w art. 1 zakresu regulacji wprowadzanych do zmienianej ustawy o aplikacji mObywatel wprowadzono nowy pkt. Pozostały zakres w pełni mieści się już w dodawanych punktach, z uwagi na to, że wymagania funkcjonalne dla europejskich portfeli tożsamości cyfrowej zostały określone w art. 5a rozporządzenia eIDAS i przepisach wykonawczych wydanych na podstawie tego artykułu. Dodano do słowniczka w art. 2 nowy punkt zawierający definicję europejskiego portfela tożsamości cyfrowej . W związku z tym zmieniono brzmienie wprowadzenie do wyliczenia w art. 14a ust. 1.

			cyfrowej – np. w odniesieniu do zapewnienia nowych usług, których mowa np. w art. 14e zmienianej ustawy (składanie kwalifikowanych podpisów elektronicznych), w art. 14g zmienianej ustawy (udostępnienie usług aplikacji mObywatel w europejskim portfelu tożsamości cyfrowej) czy art. 16 zmienianej ustawy (udostępnienia nowych usług zarówno w aplikacji mObywatel, jak i w europejskim portfelu tożsamości cyfrowej). Proponowane w obecnym brzmieniu projektu przepisy art. 1 pkt 6 i 7 ustawy o aplikacji mObywatel wyraźnie wskazują jedynie na sposób zapewnienia i funkcjonowania europejskiego portfela tożsamości cyfrowej oraz warunki i sposób jego pobierania przez użytkownika. Odnoszące się do usług zapewnianych w aplikacji mObywatel i zadań ministra właściwego do spraw informatyzacji przepisy art. 1 pkt 4 i 5 ustawy o aplikacji mObywatel nie są w powyższym kontekście zmieniane.	
62.	Art. 6 pkt 2 - dot. art. 14a	RCL	Mając na uwadze definicję europejskiego portfela tożsamości cyfrowej zawartą w rozporządzeniu 910/2014, wątpliwości budzi konstrukcja przepisu ust. 1 wskazująca, że na europejski portfel tożsamości cyfrowej składają się elementy wymienione w art. 14a ust. 1 (tj. oprogramowanie przeznaczone dla urządzeń mobilnych albo dane identyfikujących osobę, o których mowa w art. 14a ust. 2). Zgodnie z definicją europejski portfel tożsamości cyfrowej, jest środkiem identyfikacji elektronicznej, który umożliwia użytkownikowi bezpieczne przechowywanie i walidację danych identyfikujących osobę i elektronicznych poświadczeń atrybutów oraz bezpieczne zarządzanie tymi danymi i poświadczeniami na potrzeby udostępniania ich stronom ufającym oraz innym użytkownikom europejskich portfeli tożsamości cyfrowej, i który umożliwia składanie kwalifikowanych podpisów elektronicznych lub kwalifikowanych pieczęci elektronicznych (art. 3 pkt 42 rozporządzenia 910/2014). Kwestia zgodności projektowanego przepisu a ww. rozporządzeniem wymaga w tym zakresie wyjaśnienia i ewentualnego przeredagowania projektowanego art. 14a ust. 1.	**Uwaga wyjaśniona** Zapewniając europejski portfel tożsamości cyfrowej minister zapewni środek identyfikacji elektronicznej, który dodatkowo umożliwi użytkownikowi bezpieczne przechowywanie i walidację danych identyfikujących osobę i elektronicznych poświadczeń atrybutów oraz bezpieczne zarządzanie tymi danymi i poświadczeniami na potrzeby udostępniania ich stronom ufającym oraz innym użytkownikom europejskich portfeli tożsamości cyfrowej, i który umożliwia składanie kwalifikowanych podpisów elektronicznych lub kwalifikowanych pieczęci elektronicznych. Aby to zrobić minister będzie musiał zapewnić również wskazane w ustawie elementy, co wynika z: - rozporządzenia eIDAS (art. 5a ust. 18 lit b i c sugeruje, że podmiot odpowiedzialny za dostarczenie europejskiego portfela tożsamości cyfrowej i podmiot odpowiedzialny za zapewnienie powiązania danych identyfikujących osobę z europejskim portfelem tożsamości cyfrowej to mogą być podmioty różne) - rozporządzenia 2024/2979, które narzuca określoną konstrukcję portfela. Przepis art. 14a ust. 1 ma rozwiać wątpliwości w zakresie tego, kto zapewnia wskazane w tym przepisie elementy.
63.	Art. 6 pkt 2 - dot. art. 14a	RCL	Doprecyzowania wymaga pojęcie „użytkownika” wskazane w ust. 1 pkt 1 – ustawa o aplikacji mObywatel posługuje się bowiem pojęciem użytkownika jedynie w kontekście użytkownika aplikacji mObywatel, zdefiniowanego w art. 2 pkt 16 ustawy o aplikacji mObywatel,	**Uwaga wyjaśniona** W przypadku użytkownika europejskiego portfela tożsamości cyfrowej nie chodzi o użytkownika aplikacji mObywatel w rozumieniu w art. 2 pkt 16 ustawy o aplikacji mObywatel tylko o

			natomiast przepisy europejskie, jako użytkownika, w kontekście przepisów o europejskim portfelu tożsamości cyfrowej, nakazują definiować osobę fizyczną, prawną lub osobę fizyczną reprezentującą inną osobę fizyczną lub osobę prawną, korzystającą z usług zaufania lub środków identyfikacji elektronicznej świadczonych lub zapewnianych zgodnie z rozporządzeniem 910/2014 (art. 3 pkt 5a tego rozporządzenia).	użytkownika tego portfela (mimo, że może to być ta sama osoba fizyczna).
64.	Art. 6 pkt 2 - dot. art. 14a ust. 1 pkt 4	RCL	Wątpliwości budzi stwierdzenie, zgodnie z którym wśród elementów europejskiego portfela tożsamości cyfrowej, które ma zapewniać minister właściwy do spraw informatyzacji, wymieniono „dane identyfikujące osobę, o których mowa w ust. 2" zmienianego art. 14a. Należy bowiem zauważyć, że zgodnie z projektowanym art. 14a ust. 5 zmienianej ustawy dane, o których mowa w ust. 2 tego artykułu mają być pobierane w sposób automatyczny. Powyższe stwierdzenie wymaga w tym kontekście potwierdzenia co do jego poprawności i zgodności z intencją projektodawcy.	**Uwaga wyjaśniona** Rozporządzenie eIDAS w art. 5a ust. 18 lit b i c sugeruje, że podmiot odpowiedzialny za dostarczenie europejskiego portfela tożsamości cyfrowej i podmiot odpowiedzialny za zapewnienie powiązania danych identyfikujących osobę z europejskim portfelem tożsamości cyfrowej to mogą być podmioty różne, ale z pewnością należy przekazać Komisji informacje w tej sprawie, co znaczy, że należy również wyznaczyć taki podmiot. To, że dane identyfikujące osobę będą pobierane automatycznie, wcale nie przekreśla tego, że będą one zapewniane przez ministra. Ktoś bowiem musi zapewnić możliwość pobrania tych danych a następnie wydania ich w formacie przewidzianym w rozporządzeniu 2024/2977 w: 1) formacie określonym w normie ISO/IEC 18013-5:2021; 2) formacie "Verifiable Credentials Data Model 1.1." (model weryfikowalnych danych uwierzytelniających 1.1.), zalecenie W3C, 3 marca 2022 r.
65.	Art. 6 pkt 2 – dot. art. 14a ust. 2 pkt 4 i 8	MSWiA	Art. 6 pkt 2 dot. art. 14a ust. 2 pkt 8 ustawy o aplikacji mObywatel. Zgodnie z art. 14a ust. 2 pkt 8 europejski portfel tożsamości cyfrowej, o którym mowa w art. 5a ust. 2 lit. a rozporządzenia 910/2014, zawiera zestaw danych identyfikujących osobę fizyczną, obejmujący między innymi nazwisko rodowe, jeżeli występuje w rejestrze PESEL. Mając na uwadze, że w ust. 5 wskazano, że dane zawarte w europejskim portfelu tożsamości cyfrowej, o których mowa w ust. 2 pkt 1-8 pochodzą z rejestru PESEL, nadmiarowe wydaje się sformułowanie w części „jeżeli występuje w rejestrze PESEL". Oczywistym bowiem jest, że w przypadku braku takich danych, nie zostaną one zamieszczone w europejskim portfelu tożsamości cyfrowej. Podobna sytuacja może wystąpić w przypadku danych dot. miejsca urodzenia.	**Uwaga wyjaśniona** Uwarunkowanie „jeżeli występuje w rejestrze PESEL" wpisano z ostrożności z uwagi na potrzebę rozwiania ewentualnych wątpliwości i sporów w zakresie: - czy można / należy wpisywać do danych identyfikujących osobą określone informacje, gdy taka informacja nie znajduje się w rejestrze PESEL, ale jest znana danej osobie i może zostać potwierdzona na podstawie aktualnego dokumentu potwierdzającego tożsamość, - czy w ogóle można wydać zestaw danych identyfikujących osobę, skoro przepis wymaga określonych danych a nie ma ich w rejestrze PESEL.
66.	Art. 6 pkt 2 - dot. art. 14a ust. 2 pkt 9 w	MSWIA	Art. 6 pkt 2 dot. art. 14a ust. 2 pkt 9 w związku z ust. 5 pkt 2 ustawy o aplikacji mObywatel. Zgodnie z projektowanym przepisem zamieszczane w europejskim portfelu tożsamości dane dotyczące wizerunku twarzy użytkownika	**Uwaga uwzględniona** Wprowadzono zmianę w art. 14a ust. 2 pkt 9.

	związku z ust. 5 pkt 2		portfela pobierane są automatycznie z Rejestru Dowodów Osobistych lub jeżeli nie jest to możliwe z dokumentu potwierdzającego tożsamość spełniającego zalecenia Organizacji Międzynarodowego Lotnictwa Cywilnego, zwanej dalej „ICAO", określone w dokumencie - Doc 9303 Machine Readable Travel Documents część 10, 11 i 12. Zgodnie z art. 56 ust. 1 pkt 2 ustawy o dowodach osobistych w Rejestrze Dowodów Osobistych gromadzi się fotografię, o której mowa w art. 29. W związku z powyższym zasadne jest doprecyzowanie projektowanego przepisu i określenie, że europejski portfel tożsamości cyfrowej zawiera fotografię użytkownika portfela. Należy przy tym zauważyć, że podobne sformułowanie występuje na gruncie ustawy o aplikacji mObywatel w art. 7 ust. 1 pkt 2, zgodnie z którym dokument mObywatel zawiera fotografię użytkownika aplikacji mObywatel pobraną z Rejestru Dowodów Osobistych. Jednocześnie powyżej zaproponowaną korektę należy rozszerzyć na inne projektowane przepisy	
67.	Art. 6 pkt 2 - dot. art. 14a ust. 3	RCL	Mając na uwadze, że zarówno definicja europejskiego portfela tożsamości cyfrowej jak i rozporządzenie 2024/2977 posługują się wyłącznie pojęciem „osoby fizycznej" oraz „osoby prawnej" – wyjaśnienia w uzasadnieniu wymaga wyróżnienie w przedmiotowym projekcie również danych osoby fizycznej prowadzącej działalność gospodarczą – w zakresie danych dotyczących osoby prawnej.	**Uwaga wyjaśniona** Zgodnie z projektowanym art. 14a ust. 3 europejski portfel tożsamości cyfrowej zawiera zestaw danych identyfikujących osobę prawną lub osobę fizyczną prowadzącą działalność gospodarczą, obejmujący między innymi "1) nazwę (firmę) zgodną z odpowiednim wpisem do: a) Centralnej Ewidencji i Informacji o Działalności Gospodarczej" oraz (...) "2) numer identyfikacji podatkowej (NIP);" Przepis ten jest zgodny z obowiązkowym zakresem danych wskazanym w tabeli 2 rozporządzenia 2024/2977 gdzie wymaga się tylko dwóch elementów - nazwy oraz identyfikatora.
68.	Art. 6 pkt 2 - dot. art. 14a ust. 3 pkt 1	RCL	Zauważenia wymaga, że wskazany przepis dotyczy zestawu danych w europejskim portfelu tożsamości cyfrowej identyfikujących osobę prawną lub osobę fizyczną prowadzącą działalność gospodarczą obejmujący, w pkt 1, dane – „nazwa (firma) zgodna z odpowiednim wpisem do:". Tymczasem zgodnie z art. 5 ust. 1 pkt 1 i 2 ustawy z dnia 6 marca 2018 r. o Centralnej Ewidencji i Informacji o Działalności Gospodarczej i Punkcie Informacji dla Przedsiębiorcy (Dz. U. z 2026 r. poz. 30), wpisowi do CEIDG podlegają m.in. dane ewidencyjne: imię i nazwisko przedsiębiorcy, numer PESEL, o ile taki posiada, oraz data urodzenia, o ile nie posiada numeru PESEL oraz dodatkowe określenia, które przedsiębiorca włącza do firmy, o ile przedsiębiorca takich używa – co powinno zostać uwzględnione w projektowanej regulacji.	**Uwaga wyjaśniona** W obowiązkowym zakresie danych wskazanym w tabeli 2 rozporządzenia 2024/2977 wymaga się tylko dwóch elementów - nazwy oraz niepowtarzalnego identyfikatora.

69.	Art. 6 pkt 2 – dot. art. 14a ust. 4 pkt. 1	MI	Art. 6 pkt 2 ustawy zmieniającej w odniesieniu do art. 14a ust. 4 pkt. 1 ustawy o aplikacji mObywatel (ustawa zmieniana). Pojawia się pytanie, czy zastrzeżenie numeru PESEL lub dokumentu tożsamości - przewidziane w odrębnych przepisach - będzie równoznaczne z wygaśnięciem danych identyfikujących daną osobę w rozumieniu art. 14a ust. 4 pkt. 1. Doprecyzowanie relacji między tymi mechanizmami wydaje się istotne dla jednoznacznego stosowania przepisów.	**Uwaga wyjaśniona** Zastrzeżenie numeru PESEL lub dokumentu tożsamości - przewidziane w odrębnych przepisach nie będzie równoznaczne z wygaśnięciem danych identyfikujących daną osobę w rozumieniu art. 14a ust. 4 pkt. 1. Takie zastrzeganie nie będzie miało wpływu i nie powinno mieć na ważność europejskiego portfela tożsamości cyfrowej. Przepisy są jednoznaczne w tym zakresie i nie ma potrzeby takiego doprecyzowania.
70.	Art. 6 pkt 2 - dot. art. 14a ust. 5 pkt 2	RCL	Wyjaśnienia wymaga, z którego systemu czy rejestru będą pobierane automatycznie dane z dokumentu potwierdzającego tożsamość spełniającego zalecenia Organizacji Międzynarodowego Lotnictwa Cywilnego, zwanej dalej „ICAO", określone w dokumencie - Doc 9303 Machine Readable Travel Documents część 10, 11 i 12.	**Uwaga wyjaśniona** Dane będą pobierane wprost z dokumentu potwierdzającego tożsamość. Dokumenty spełniające zalecenia Organizacji Międzynarodowego Lotnictwa Cywilnego, zwanej dalej „ICAO", określone w dokumencie - Doc 9303 Machine Readable Travel Documents część 10, 11 i 12 zawierają fotografię w postaci elektronicznej, która może być pobrana.
71.	Art. 6 pkt 2 Art. 14a ust. 5 pkt 2	MI	Poza powyższym zauważenia wymaga, że w dodawanym art. 14a ust. 5 pkt 2 projektu znajduje się odesłanie do dokumentu - Doc 9303 Machine Readable Travel Documents. Dokumenty Doc wydawane przez Organizację Międzynarodowego Lotnictwa Cywilnego nie są przepisami powszechnie obowiązującymi i nie obowiązują wprost, a brakuje informacji 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 proponuję doprecyzowanie art. 14a ust. 5 pkt 2 w tym zakresie.	**Uwaga wyjaśniona** Specyfikacja Doc 9303 Machine Readable Travel Documents ogłoszona pod adresem https://www.icao.int/publications/doc-series/doc-9303 nie ma polskiej wersji językowej, co nie znaczy że nie może być wskazana w przepisach krajowych. 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). Ostatnia wersja DOC 9303 jest wersją ósmą wydaną 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). Oznacza to, że są w obiegu ważne dowody osobiste spełniające zalecenia Organizacji Międzynarodowego Lotnictwa Cywilnego w wersji siódmej i w wersji ósmej. Podobnie może być z dokumentami podróży niewydawanymi w Polsce do których odnosi się przepis i których zgodność z wersją siódmą z 2015 r. lub z wersją ósmą z 2021 r. nie ma znaczenia dla celu określonego w projektowanym art. 14a ust. 5 pkt 2.
72.	Art. 6 pkt 2 - dot. art. 14a ust. 6 pkt 1	RCL	Proponuje się doprecyzowanie przepisu w ten sposób, aby wskazywał (przez odesłanie do odpowiedniej regulacji) jakie dane osobowe użytkowników europejskiego portfela tożsamości cyfrowej będą przetwarzane przez ministra właściwego do spraw informatyzacji w zakresie, o którym mowa w tym przepisie.	**Uwaga wyjaśniona** Wydaje się, że nie ma takiej potrzeby. Nie stosuje się takiej praktyki w przypadku przechowywania jakiejkolwiek dokumentacji w tym np. w przypadku przechowywania dokumentacji związanej z dowodami osobistymi czy też profilu zaufanego.
73.	Art. 6 pkt 2 - dot. art. 14a ust. 6 pkt 2 i ust. 7	RCL	Wyjaśnienia wymaga czy jest możliwe doprecyzowanie w większym stopniu katalogu danych niezbędnych do świadczenia usługi europejskiego portfela tożsamości cyfrowej (przez wskazanie bądź odesłanie do konkretnych danych, ich 9 rodzajów lub choćby ich charakteru), gdyż w proponowanym brzmieniu ust. 7 zostały one określone jedynie przez ich funkcję (umożliwienia użytkownikom odtworzenia europejskiego portfela tożsamości cyfrowej oraz jego konfiguracji) – przez co katalog ten jest w istocie nieokreślony.	**Uwaga wyjaśniona** Nie jest możliwe odesłanie do konkretnych danych ponad wskazanie, że chodzi o dane umożliwiające odtworzenie rejestru transakcji (czyli zgodnie ze wskazanym przepisem art. 5a ust. 4 lit. d przeglądanie aktualnej listy stron ufających, z którymi użytkownik ustanowił połączenie, oraz, w stosownych przypadkach, wszystkich udostępnionych danych), ponieważ nie wiadomo, jakie dane (rodzaje nie wartości) i komu użytkownicy udostępnią. Nie można również dookreślić elementów konfiguracji portfela użytkownika, gdyż to również wyłącznie od tego użytkownika zależy, jakie elektroniczne poświadczenia atrybutów będzie miał i z jakich usług będzie korzystał. Ponadto specyficzna architektura rozwiązania w zakresie portfela oraz systemu identyfikacji elektronicznej, w ramach którego będzie zapewniany) będzie wynikała z krajowego programu certyfikacji, o którym mowa w art. 3 rozporządzenia wykonawczego Komisji (UE) 2024/2981 z dnia 28 listopada 2024 r. ustanawiające zasady stosowania rozporządzenia Parlamentu Europejskiego i Rady (UE) nr 910/2014 w odniesieniu do certyfikacji europejskich portfeli tożsamości cyfrowej (Dz. U. UE. L. z 2024 r. poz. 2981).

				Należy zwrócić uwagę na art. 21 ww. rozporządzenia, w którym wskazuje się konieczność przejścia na europejski program certyfikacji cyberbezpieczeństwa w momencie, w którym zostanie on wydany.
74.	Art. 6 pkt 2	MSWiA	Art. 6 pkt 2 dot. art. 14b ust. 1 pkt 2 w związku z ust. 3 ustawy o aplikacji mObywatel. Zgodnie z propozycją użytkownikiem europejskiego portfela tożsamości cyfrowej, o którym mowa w art. 5a ust. 2 lit. a rozporządzenia 910/2014, może zostać osoba fizyczna, która została uwierzytelniona za pomocą profilu zaufanego, z dodatkową weryfikacją tożsamości spełniającą wymagania określone w przepisach wykonawczych wydanych na podstawie art. 5a ust. 24 rozporządzenia 910/2014. Powyższa regulacja umożliwia uwierzytelnienie za pomocą środka identyfikacji elektronicznej, na średnim poziomie bezpieczeństwa, przewidując jednocześnie, że będzie to połączone z dodatkową weryfikacją tożsamości. Skuteczność tego rozwiązania zależy od jakości przyszłych przepisów wykonawczych. Kluczowe jest, aby dodatkowa weryfikacja tożsamości realnie mitygowała ryzyka wynikające ze specyfiki środka o średnim poziomie bezpieczeństwa. Wskazane jest, aby katalog metod dodatkowej weryfikacji uwzględniał najnowsze standardy techniczne, zapewniając spójność metadanych identyfikujących osobę.	**Uwaga wyjaśniona** Rozporządzenie wykonawcze 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 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, wydane na podstawie art. 5a ust. 24 będą zapewnia właściwe rozwiązania i uwzględnia najnowsze standardy techniczne.
75.	Art. 6 pkt 2 – dot. art. 14b ust. 2 i ust. 3	MFiG (MRiT)	W zakresie dodawanego art. 14 b ust. 2 i ust. 3 - jest niewłaściwe odwołanie do ust. 1 pkt 2 lit. b, o punkcie potwierdzającym tożsamość mowa jest w ust. 1 pkt 3. Dodatkowo zasadnym jest uzupełnienie informacji, czy w procesie potwierdzania tożsamości przez wojewodę (ust. 2 pkt 1) ma znaczenie właściwość miejscowa, czy też w każdym przypadku wojewoda będzie mógł pełnić funkcję tego punktu.	**Uwaga uwzględniona/ wyjaśniona** Wprowadzono zmianę w zakresie odwołania. Zakłada się, że właściwość miejscowa wojewody nie powinna mieć znaczenia podobnie jak nie ma w przypadku potwierdzania profilu zaufanego.
76.	Art. 6 pkt 2 - dot. art. 14c ust. 2 pkt 2	MSWiA	Art. 6 pkt 2 dot. art. 14c ust. 2 pkt 2 ustawy o aplikacji mObywatel. Projektowany przepis wymaga poprawienia pod względem redakcyjnym. Zgodnie z aktualnym brzmieniem wniosek zawiera: imię (imiona), nazwisko i numer PESEL osoby fizycznej uprawnionej do zostania użytkownikiem europejskiego portfela tożsamości cyfrowej.	**Uwaga uwzględniona** Przepis został zmieniony.
77.	Art. 6 pkt 2 - dot. art. 14b ust. 2 pkt 2 lit. b	RCL	Mając na uwadze, że przepis wskazuje, jako podmiot pełniący funkcję punktu potwierdzającego tożsamość, „organy gminy będącej siedzibą władz powiatu lub organ miasta na prawach powiatu" – wyjaśnienia wymaga, czy w przypadku gminy będącej siedzibą władz powiatu właściwymi organami będą zarówno organ stanowiący, jak i organ wykonawczy (a jeżeli jeden z nich – należy tę kwestię doprecyzować), zaś w przypadku „organu miasta na prawach powiatu" – należy	**Uwaga wyjaśniona** Zgodnie z proponowanymi przepisami, funkcję punktów potwierdzających tożsamość wskazane organy będą mogły pełnić za zgodą ministra, co powoduje że: - nie ma znaczenia, który z organów wskazanej jednostki samorządu terytorialnego będzie wnioskował do ministra i następnie pełnił funkcję punktu potwierdzającego,

			doprecyzować, który z organów wskazanej jednostki samorządu terytorialnego będzie pełnił funkcję punktu potwierdzającego. Dodatkowo, mając na uwadze ww. nowe zadanie nałożone na jednostki samorządu terytorialnego, ponownej analizy i potwierdzenia wymaga informacja zawarta w pkt 6 OSR – zgodnie z którą projektowana regulacja nie będzie mieć wpływu na budżety jednostek samorządu terytorialnego.	- regulacja nie nakłada nowego zadania na jednostki samorządu terytorialnego tylko umożliwia jego realizację.
78.	Art. 6 pkt 2 - dot. art. 14b ust. 3	RCL	Zawierającego upoważnienie ministra właściwego do spraw informatyzacji do określenia w drodze rozporządzenia wymagań dotyczących weryfikacji tożsamości przez fakultatywne (za zgodą tego ministra) punkty potwierdzające tożsamość oraz warunki, jakie te punkty muszą spełniać należy zauważyć, że: – – wyjaśnienia wymaga wpływ na zakres przedmiotowy projektowanego rozporządzenia przepisów wykonawczych wydanych na podstawie art. 5a ust. 24 rozporządzenia 910/2014 (jeżeli zostaną wydane na podstawie tego fakultatywnego upoważnienia), – – projekt należy uzupełnić o choćby podstawowe regulacje dotyczące warunków organizacyjno-technicznych, jakie musi spełniać punkt potwierdzający tożsamość, o którym mowa w dodawanym art. 14b ust. 1 pkt 2 lit. b zmienianej ustawy, z uwagi na ryzyko uznania przedmiotowego upoważnienia za blankietowe, – – wyjaśnienia wymaga, czy określone w tym przepisie wytyczne do wydania rozporządzenia nie powinny zostać doprecyzowane w zakresie konieczności uwzględnienia wymogów dotyczących wysokiego poziomu bezpieczeństwa – spośród wymogów określonych w rozporządzeniu wykonawczym 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 10 zaufania w odniesieniu do transakcji elektronicznych na rynku wewnętrznym (Dz. Urz. UE L 235 z 09.09.2015, str. 7, z późn. zm.)	**Uwaga wyjaśniona** Rozporządzenie na podstawie art. 5a ust. 24 rozporządzenia 910/2014 właśnie zostało wydane. Jest to rozporządzenie wykonawcze 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 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. Jeżeli chodzi o zamieszczanie w ustawie podstawowych regulacji dotyczących warunków organizacyjno-technicznych, jakie musi spełniać punkt potwierdzający tożsamość, to nie jest to niezbędne. Przykładowo nie wskazano takich warunków w art. 20d pkt 1 lit. g ustawy o informatyzacji działalności podmiotów realizujących zadania publiczne. To oczywiste, że muszą być spełnione warunki dla wysokiego poziomu bezpieczeństwa wskazane w rozporządzeniu wykonawczym Komisji (UE) 2015/1502, skoro europejski portfel tożsamości cyfrowej ma spełniać te wymagania, co wynika z kolei w przepisu art. 5a ust. 5 lit. d rozporządzenia eIDAS. W związku z tym nie ma potrzeby doprecyzowania wytycznych w trym zakresie.
79.	Art. 6 pkt 2 - dot. art. 14c ust. 1	RCL	Mając na uwadze, że w projektowanych przepisach art. 14a ust. 3, 4 i 6 ustawy Projektodawca odrębnie uregulował kwestie dotyczące osoby prawnej i pojęcie osoby fizycznej prowadzącej działalność gospodarczą – proponuje się konsekwentne utrzymanie tego wyodrębnienia w projektowanym przepisie art. 14c ust. 1 we wprowadzeniu do wyliczenia.	**Uwaga wyjaśniona** W art. 14c ust. 1 chodzi o osoby fizyczne, które mogą zostać użytkownikami europejskiego portfela tożsamości cyfrowej, o którym mowa w art. 14a ust. 1 5a ust. 2 lit. a rozporządzenia 910/2014, osoby prawnej. W szczególności może być nim osoba fizyczna prowadząca działalność gospodarczą. Z tego względu nie wydaje się zasadne dokonanie zmian.

80.	Art. 6 pkt 2 - dot. art. 14c ust. 5	RCL	Mając na uwadze zakres materii przekazywanej do uregulowania w akcie wykonawczym (określenie sposobu powiązania i sposobu cofnięcia tego powiązania), należy wskazać na konieczność uzupełnienia materii ustawowej w tym zakresie tak, aby wprowadzić podstawę do jej uszczegóławiania w akcie wykonawczym.	**Uwaga uwzględniona** Wprowadzono zmiany w art. 14c.
81.	Art. 6 pkt 2 - dot. 14d	RCL	Wyjaśnienia wymaga, czy „pełny" zestaw danych identyfikujących osobę fizyczną, jaki zawiera europejski portfel tożsamości cyfrowej, oznacza zestaw danych określonych w projektowanym art. 14a ust. 2 ustawy o aplikacji mObywatel – jeżeli tak – proponuje się odpowiednie doprecyzowanie regulacji.	**Uwaga uwzględniona** Wprowadzono zmiany w art. 14d.
82.	Art. 6 pkt 2 - dot. 14e ust. 2	RCL	Mając na uwadze fakultatywność wyrażenia zgody przez ministra właściwego do spraw informatyzacji na świadczenie usługi (dotyczącego udostępniania przy użyciu europejskiego portfela tożsamości cyfrowej usługi umożliwiającej użytkownikom tego portfela składanie kwalifikowanych podpisów elektronicznych w celach innych niż profesjonalne) , przepis wymaga uzupełnienia o wskazanie przesłanek, którymi będzie się kierował minister, podejmując decyzję o wyrażeniu zgody na świadczenie tej usługi. Jednocześnie, mając na uwadze, że minister wydaje zgodę w drodze decyzji – wyjaśnienia wymaga procedura i forma rozstrzygnięcia w przypadku braku zgody ministra albo w przypadku, gdy testy, o których mowa w ust. 4, nie zakończyły się pozytywnie.	**Uwaga wyjaśniona** Decyzja zostanie wydana po spełnieniu wszystkich przesłanek wskazanych w ustawie (czyli musi to być kwalifikowany dostawca usług podpisu składanego za pomocą urządzeń składania podpisu na odległość, rozwiązanie musi przejść testy i musi być uwzględnione w polityce świadczenia usług zaufania).
83.	Art. 6 pkt 2 - dot. 14e ust. 11-13	RCL	Wyjaśnienia wymaga ratio legis wprowadzenia wytycznych ministra właściwego do spraw informatyzacji do świadczenia usługi umożliwiającej użytkownikom europejskiego portfela tożsamości cyfrowej nieodpłatne składanie kwalifikowanych podpisów elektronicznych w celach innych niż profesjonalne – w drodze ich udostępnienia w BIP. Zasadnym wydaje się ich wprowadzenie w drodze aktu powszechnie obowiązującego – pewne wątpliwości może bowiem budzić charakter materii wytycznych obejmującej np. sposób weryfikacji tożsamości albo sposób oznaczania podpisanych dokumentów. Jednocześnie wyjaśnienia wymaga wzajemna relacja ww. wytycznych i przepisu ust. 13 zawierającego upoważnienie do wydania rozporządzenia określającego sposób świadczenia usługi umożliwiającej użytkownikom europejskiego portfela tożsamości cyfrowej nieodpłatne składanie kwalifikowanych podpisów elektronicznych w celach innych niż profesjonalne. W tym zakresie wątpliwości budzi, czy ww. sposób świadczenia usługi nie obejmuje także kwestii przekazanych do określenia w ww. wytycznych ministra – co wymaga ponownej analizy zakresów obu przepisów i wyjaśnienia. Niezależnie od powyższego,	**Uwaga wyjaśniona** Wytyczne dotyczące świadczenia usługi umożliwiającej użytkownikom europejskiego portfela tożsamości cyfrowej nieodpłatne składanie kwalifikowanych podpisów elektronicznych w celach innych niż profesjonalne powinny znaleźć się BIP, ponieważ będą to wymaganie techniczne, które nie będą zawierały regulacji mających wpływ na obywateli. Regulacje ogólne odpowiadające zakresowi określonemu w art. 14e ust. 13 pkt 1 znajdują się w art. 14e ust. 1.

			mając na uwadze przepis ust. 13 – projektowane przepisy ustawy należy uzupełnić o regulacje ogólne odpowiadające zakresowi określonemu pkt 1 tego ustępu (sposób świadczenie usługi) tak, aby uniknąć zarzutu uzupełniania ustawy aktem wykonawczym.	
84.	Art. 6 pkt 2 - dot. art. 14g ust. 1 pkt 1 i ust. 2 oraz art. 14h	RCL	Zauważenia wymaga, że brak wskazania w tej regulacji (bądź w ustawach szczególnych) konkretnej podstawy prawnej do pobierania i przekazywania danych rejestrów publicznych, rejestrów niepublicznych lub systemów teleinformatycznych, w celu świadczenia usług za pomocą europejskiego portfela tożsamości cyfrowej, może budzić wątpliwości co do należytej podstawy przetwarzania danych w tych rejestrach. Powyższe będzie miało też wpływ na ocenę przewidywanego rozporządzenia Rady Ministrów, które zostanie wydane na podstawie przepisu art. 14h, zgodnie z którym Rada Ministrów określi zakres danych i wykaz rejestrów publicznych oraz systemów teleinformatycznych, z których użytkownik europejskiego portfela tożsamości cyfrowej może pobrać dane, oraz (wykaz) podmiotów publicznych prowadzących te rejestry publiczne i systemy teleinformatyczne – w zakresie odpowiedniego umocowania wskazanych w tym akcie danych zawartych w rejestrach i systemach.	**Uwaga wyjaśniona** Co do zasady europejskie portfele tożsamości cyfrowej to narzędzia, które mają pozwolić ich użytkownikom na pobranie dowolnych danych ich dotyczących na podstawie wspólnych zharmonizowanych przepisów europejskich. W motywie 7 preambuły Rozporządzenia Parlamentu Europejskiego i Rady (UE) 2024/1183 z dnia 11 kwietnia 2024 r. w sprawie zmiany rozporządzenia (UE) nr 910/2014 w odniesieniu do ustanowienia europejskich ram tożsamości cyfrowej (Dz. U. UE. L. z 2024 r. poz. 1183, z późn. zm.). wskazano m.in. że: "Każdy powinien mieć możliwość bezpiecznego dostępu do usług publicznych i prywatnych, za pomocą ulepszonego systemu usług zaufania i zweryfikowanych dowodów potwierdzających tożsamość oraz elektronicznych poświadczeń atrybutów, takich jak kwalifikacje akademickie, w tym dyplomy ukończenia studiów wyższych, lub inne uprawnienia edukacyjne lub zawodowe. Europejskie ramy tożsamości cyfrowej mają na celu przejście od polegania wyłącznie na krajowych rozwiązaniach w zakresie tożsamości cyfrowej do zapewnienia elektronicznych poświadczeń atrybutów, które są ważne i prawnie uznawane w całej Unii. Dostawcy elektronicznych poświadczeń atrybutów powinni skorzystać na jasnym i jednolitym zestawie przepisów, natomiast administracje publiczne powinny mieć możliwość polegania na dokumentach elektronicznych w określonym formacie." Taki jasny i jednolity zestaw przepisów został wskazany w rozporządzeniu eIDAS. W szczególności wymaga się od wszystkich państw członkowskich, aby: - umożliwiły w terminie 24 miesięcy od dnia wejścia w życie aktów wykonawczych, o których mowa w art. 5a ust. 23 i art. 5c ust. 6, aby przynajmniej w odniesieniu do atrybutów wymienionych w załączniku VI, w przypadku gdy atrybuty te polegają na źródłach autentycznych w sektorze publicznym, wprowadzono środki umożliwiające kwalifikowanym dostawcom usług zaufania, którzy dostarczają kwalifikowane elektroniczne

				poświadczenia atrybutów, weryfikację tych atrybutów drogą elektroniczną, na żądanie użytkownika, zgodnie z prawem Unii lub prawem krajowym (zob. art. 45e rozporządzenia eIDAS), - zgłosiły do Komisji Europejskiej wnioski o włączenie atrybutów wymienionych w załączniku VI do rozporządzenia (UE) nr 910/2014 do katalogu atrybutów, w każdym przypadku gdy atrybuty te opierają się na źródłach autentycznych do celów weryfikacji przez kwalifikowanych dostawców usług zaufania w tym wskazały przestrzeń nazw dla identyfikatora atrybutów, którego wartość jest niepowtarzalna w katalogu atrybutów, semantyczny opis atrybutu, rodzaj danych atrybutu oraz punkt weryfikacji atrybutu na poziomie krajowym lub link do opisu sposobu składania wniosków o weryfikację (art. 7 rozporządzenia KE 2025/1569). Znaczy to, że państwa członkowskie nie tylko mogą, ale muszą udostępnić rejestry publiczne stanowiące jakiekolwiek źródła autentyczne w rozumieniu załącznika VI do rozporządzenia eIDAS i to w taki sposób, że wskażą nie tylko zakresy atrybutów (danych), ale też na sposób ich weryfikacji. Powyższe przepisy są główną podstawą do zapewnienia użytkownikom portfeli danych ich dotyczących. Wychodząc naprzeciw innych uwagom do projektu ustawy podobne rozwiązanie zaproponowano na szczeblu krajowym tworząc krajowy katalog schematów elektronicznych poświadczeń atrybutów. Celem tego rozwiązania jest, aby na zasadach podobnych jak europejskie umożliwić z inicjatywy podmiotu odpowiedzialnego za źródło autentyczne wydawanie elektronicznych poświadczeń atrybutów ważnych jedynie w kraju. Jeżeli chodzi o rozporządzenie Rady Ministrów, które zostanie wydane na podstawie przepisu art. 14h, to jego rola (istotna) ograniczy się do usług, które nie są elektronicznymi poświadczeniami atrybutów.
85.	Art. 6 pkt 2 – dot. art. 14h	MI	Art. 6 pkt 2 ustawy zmieniającej w odniesieniu do art. 14h ustawy o aplikacji mObywatel (ustawa zmieniana). Przepis przewiduje, że Rada Ministrów określi w rozporządzeniu zakres danych oraz wykaz rejestrów publicznych i systemów teleinformatycznych, z których będzie korzystał użytkownik europejskiego portfela tożsamości cyfrowej. Powstaje pytanie, czy wykaz ten ma mieć charakter stały, czy też będzie podlegał aktualizacji wraz ze zmianami w infrastrukturze cyfrowej i	**Uwaga wyjaśniona** Co do zasady rozporządzenia mogą i powinny być nowelizowane w miarę potrzeb nie ma potrzeby doprecyzowania tego w ustawie. Na przykład rozporządzenie Rady Ministrów w sprawie zakresu danych i wykazu rejestrów publicznych oraz systemów teleinformatycznych podmiotów publicznych, z których

			pojawianiem się nowych rejestrów lub systemów. Doprecyzowanie tej kwestii wydaje się istotne dla zapewnienia elastyczności i aktualności regulacji.	użytkownik aplikacji mObywatel może pobrać dane było już nowelizowane kilkukrotnie, a rozporządzenie Ministra Rozwoju i Finansów w sprawie sposobu przesyłania deklaracji i podań oraz rodzajów podpisu elektronicznego, którymi powinny być opatrzone - kilkunastokrotnie.
86.	Art. 6 pkt 2 – dot. art. 14f	MFiG (MF)	Odnośnie projektowanego art. 14f ustawy o usługach zaufania (…) – należy mieć na względzie, że istnieją też sprawy prywatne, które są jednocześnie związane z wykonywanym zawodem. Przykładem może być podnoszenie kwalifikacji zawodowych, sprawy dotyczące prawa jazdy osób, które kierują pojazdami prywatnie i zawodowo, i pewnie wiele innych. Właściwe wydaje się wykreślenie frazy "niezwiązanej z wykonywanym zawodem". Na przykładzie prawa jazdy - jak urząd ma stwierdzić, czy wniosek został złożony prywatnie czy zawodowo. Nie ma do tego uprawnień, a jednego prawa jazdy można używać i prywatnie, i zawodowo. Dodatkowo, aplikacja podpisująca będzie dokonywała modyfikacji podpisywanego dokumentu. Jeśli dodawany będzie znak w warstwie wizualnej, to może on uszkadzać dokument, np. zakrywać jakieś elementy, w szczególności naruszając urzędowe wzory dokumentów. Być może lepszym rozwiązaniem byłoby dodanie atrybutu do certyfikatu niż ingerowanie w dokument. Podobna sytuacja dotyczy opiekunów prawnych dorosłych osób ubezwłasnowolnionych całkowicie - oni również sprawują pieczę często identyczną jak przy opiece nad dzieckiem (projektowany art. 14g ust. 1 pkt 1 lit. d ustawy o usługach zaufania (…). Warto rozważyć dodanie ich, co może ułatwić załatwianie spraw, gdy trzeba potwierdzić fakt sprawowania opieki nad taką osobą.	**Uwagi wyjaśnione** Zakłada się, że faktyczny skutek prawny oświadczenia woli opatrzonego kwalifikowanym podpisem elektronicznym przeznaczonym do celów innych niż profesjonalne ale w celach profesjonalnych (bez względu na to czy przez omyłkę czy celowo) będzie taki sam jak podpisu własnoręcznego. Nie ma zatem powodu, aby strona ufająca była zmuszana do odróżniania podpisów "profesjonalnych" od "nieprofesjonalnych" i miała mieć z tego powodu obawy co do skuteczności wyrażenia woli. Celowo nie przewiduje się sankcji zakładając, że oznaczenie dokumentów klauzulą, która nie powoduje uszkodzenia dokumentu, że zostały opatrzone nieodpłatnym podpisem kwalifikowanym spowoduje powstanie samoregulującego się systemu. Zakłada się, że przedsiębiorcy (a tym bardziej podmioty publiczne) nie będą używali (lub będzie to zjawisko sporadyczne) nieopłatnego podpisu do celów profesjonalnych z uwagi na ich postrzeganie przez kontrahentów i klientów. Celowo nie ustala się sankcji za użycie nieodpłatnego podpisu przeznaczonego co celów innych niż profesjonalne do celów profesjonalnych. Nie zatem ma potrzeby dawania stronie ufającej możliwości nieprzyjęcia/podważenia dokumentu podpisanego z wykorzystaniem darmowego podpisu. Zakłada się, że nie powinno się obciążać stron ufających (ani sądów) koniecznością precyzyjnego odróżniania celu złożenie podpisu.
87.	Art. 8	MFiG (MRiT)	Projekt przewiduje obowiązek przyłączenia istniejących systemów podmiotów publicznych do systemu scentralizowanego dopasowywania tożsamości w terminie 6 miesięcy od wejścia ustawy w życie. Termin ten jest zbyt krótki, szczególnie dla dużych systemów oferujących wiele usług online oraz dla podmiotów posiadających ograniczone zasoby techniczne. Integracja z nowymi mechanizmami identyfikacji i dopasowywania tożsamości będzie wiązać się z koniecznością modyfikacji istniejących procesów, interfejsów, procedur bezpieczeństwa oraz testów zgodności.	**Uwaga uwzględniona** Rozporządzenie 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) wchodzi w życie 24 grudnia 2026 r. i co za tym idzie w tym terminie planuje się udostępnić system dopasowywania tożsamości. Istotnie znaczy to, że nie uda się w tym samym dniu podłączyć istniejących systemów podmiotów publicznych do systemu scentralizowanego, gdyż będzie to

			Proponuję wydłużenie terminu np. do 12 miesięcy, aby umożliwić bezpieczne i zgodne z wymogami wdrożenie.	proces wymagający spełnienia określonych wymagań dotyczących interoperacyjności i bezpieczeństwa. Dlatego też planuje się wykorzystać istniejącą infrastrukturę węzła krajowego i formaty danych w jakich węzeł ten wymienia dane, tak aby okres dostosowawczy mógł być jak najkrótszy. Z pewnością 24 grudnia 2026 nie ruszą w pełni w całej UE usługi online dla użytkowników portfeli, gdyż stanie się to dopiero gdy portfele zostaną scertyfikowane, Komisja Europejska odnotuje je we właściwym rejestrze, rejestry stron ufających zostaną oddane do użytku i zgłoszone, strony ufające zarejestrują się w tych rejestrach i uzyskają certyfikaty strony ufające portfelowi a podmioty wydające takie certyfikaty będą gotowe do ich wydawania. Nie tylko z Polsce ale w każdym z państw UE powstaną uzależnione od działania różnych podmiotów systemy dla europejskich portfeli tożsamości cyfrowej. Dlatego też postulat wydłużenia terminu do 12 miesięcy dla zapewnienia przyłączenia do systemu scentralizowanego wydaje się zasadny, mimo że może to oznaczać pojawienie się zarzutów o nieterminowe zapewnienie dopasowania tożsamości przez końcowe stronu ufające. Zakłada się, że na poziomie państwa (o czym mowa w art. 11a ust. 1 eIDAS) ten warunek będzie spełniony – w szczególności dla osób, które kiedykolwiek miały nadany numer PESEL, ale używają środka identyfikacji elektronicznej wydanego w innym państwie członkowskim UE system zapewni od razu możliwość uwierzytelniania, gdyż do końcowego dostawcy usługi zostanie wysłany oczekiwany zestaw danych w oczekiwanym formacie.
88.	Art. 10 pkt 1 i art. 11	MFiG (MF)	W projektowanym art. 11 ustawy wskazano, że ustawa wchodzi w życie z dniem 24 grudnia 2026 r. Jednocześnie przewiduje się, że zadania przewidziane w projekcie ustawy będą realizowane przez Centralny Ośrodek Informatyki, do którego będą przekazane środki z cz. 27 budżetu państwa - Informatyzacja. W roku 2026 wskazano na koszty w wysokości 45,5 mln zł. Należy zauważyć, że skoro ustawa wejdzie w życie w ostatnich dniach grudnia i w celu przekazania środków do Centralnego Ośrodka Informatyki wymagana będzie zmiana planu finansowego tej jednostki, jest bardzo mało czasu, by przeprowadzić tę zmianę z uwagi na okres świąteczny i układ kalendarza w ostatnich dniach roku. Zamknięcie roku budżetowego ogranicza możliwość dokonywania zmian. Wymaga to ponownej analizy i szczegółowego	**Uwaga uwzględniona** Projekt ustawy wraz z uzasadnieniem oraz OSR został odpowiednio zmieniony.

			odniesienia do kwestii wpływu wejścia w życie projektu ustawy na plan finansowy COI, w tym na poziom wynagrodzeń osobowych.	
89.	Uzasadnienie	MFiG (MRiT)	Rekomenduję uzupełnienie o opis powiązania aplikacji mObywatel z europejskim portfelem tożsamości cyfrowej.	**Uwaga uwzględniona** Uzasadnienie zostało uzupełnione.
90.	Uzasadnienie	MFiG (MRiT)	Projekt przewiduje możliwość pobrania podstawowych danych (imię, nazwisko, data urodzenia, numer PESEL) z europejskiego portfela tożsamości cyfrowej za pośrednictwem krajowego węzła identyfikacji elektronicznej. • Czy i kiedy przewiduje się rozszerzenie zakresu dostępnych atrybutów przekazywanych przez portfel EUDI? • Czy podmioty publiczne będą mogły samodzielnie zgłaszać potrzebę dodania nowych atrybutów?	**Uwaga wyjaśniona** Przewiduje się poszerzenie zakresu danych przesyłanych przez węzeł krajowy identyfikacji elektronicznej: - w dotychczasowym zakresie wynikającym z zestawu danych identyfikujących osobę określonym w rozporządzeniu wykonawcze 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. U. UE. L. z 2015 r. Nr 235, str. 1 z późn. zm.), - dodatkowo w zakresie danych identyfikujących osobę określonych w rozporządzeniu wykonawczym 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), - dodatkowo w zakresie przesłanie dodatkowych danych w celu dopasowania tożsamości przewidzianego w nowym art. 22a ustawy o usługach zaufanie oraz identyfikacji elektronicznej. Nie przewiduje się przesyłanie przez węzeł krajowy danych potwierdzających inne atrybuty (cechy charakterystyczne, właściwości, prawa lub zezwolenia osoby fizycznej lub prawnej lub przedmiotu) gdyż takie atrybuty co do zasady powinny znaleźć potwierdzenie w elektronicznych poświadczeniach atrybutów, a nie w środkach identyfikacji elektronicznej. Jak wynika bowiem z art. 21a ust. 2 ustawy o usługach zaufania oraz identyfikacji elektronicznej „węzeł krajowy jest rozwiązaniem organizacyjno-technicznym umożliwiającym uwierzytelnianie użytkownika systemu teleinformatycznego, korzystającego z usługi online, z wykorzystaniem środka identyfikacji elektronicznej wydanego w systemie identyfikacji elektronicznej przyłączonym do tego węzła bezpośrednio albo za pośrednictwem węzła transgranicznego”. Łącznie oznacza to że

				węzeł krajowy nie jest przeznaczony do przesyłania dodatkowych atrybutów. Służy wyłącznie do zapewnienia jednoznacznej identyfikacji osób a nie ich uprawnień, zezwoleń lub innych cech. Przesyłanie przez węzeł krajowy danych innych niż dane identyfikujące osobę – czyli danych, które wykraczają poza funkcjonalność europejskich portfeli tożsamości cyfrowej jako środków identyfikacji elektronicznej mogłoby ponadto spotkać się ze skuteczną krytyką związaną z ochroną prywatności użytkowników usług online.
91.	Uzasadnienie str. 23-24	MSWiA	W uzasadnieniu wskazano na zasadność włączenia do krajowego zestawu danych identyfikujących osobę numeru PESEL jako numeru jednoznacznie identyfikującego osobę fizyczną. Poruszono przy tym problem związany z negatywnymi skutkami polegania, w celu jednoznacznej identyfikacji osoby fizycznej, na zmiennych elementach, takich jak adres zamieszkania, adres email, czy nr telefonu komórkowego, które może spowodować uniemożliwienie ciągłego korzystania przez daną osobę z usług online po zmianie tych danych, a w szczególności uniemożliwienie dostępu do konta w systemie teleinformatycznym, w którym takie usługi są udostępniane. W ocenie projektodawcy rezygnacja z numeru PESEL, jako unikalnego identyfikatora osoby fizycznej, i poleganie w tym zakresie na elementach zmiennych, takich jak opisane powyżej, wiązałoby się nie tylko z istotnymi problemami użytkowników w dostępie do ich danych zgromadzonych w rejestrach publicznych i systemach teleinformatycznych podmiotów publicznych, ale prowadziłoby również do konieczności kosztownej przebudowy większości usług publicznych, poprzedzonej zmianami przepisów prawa regulujących funkcjonowanie tych usług. Niespójne z powyższymi wyjaśnieniami jest zawarte w uzasadnieniu sformułowanie w brzmieniu „Innym dobrze ilustrującym przykładem konsekwencji polegania na zmiennych danych są problemy z dostępem do usług online, jakie mają osoby fizyczne po zmianie numeru PESEL”. Wskazać przy tym należy, że zgodnie z art. 19 ustawy o ewidencji ludności zmiana numeru PESEL możliwa jest wyłącznie w trzech przypadkach: 1) sprostowania daty urodzenia; 2) zmiany płci; 3) nadania numeru PESEL na skutek omyłki organu administracji publicznej mającej wpływ na numer PESEL lub wprowadzenia w błąd organu administracji publicznej co do tożsamości osoby.	**Uwaga uwzględniona** Uzasadnienie zostało uzupełnione o wyjaśnienie dlaczego wskazano jako przykład zmianę numeru PESEL i że następuje to tylko w wyjątkowych sytuacjach określonych przepisami prawa.

			Numer PESEL jest zatem, co do zasady, przypisany osobie fizycznej przez całej jej życie i tylko w wyjątkowych sytuacjach określonych przepisami prawa może ulec zmianie.	
92.	OSR	MSWiA	Niezbędne jest uzupełnienie jego OSR przez ujęcie Ministra Spraw Wewnętrznych i Administracji jako podmiotu, na który wpływa projektowana zmiana ustawy, w obszarze Systemu Rejestracji Broni (SRB). Minister właściwy do spraw wewnętrznych jest administratorem SRB, który to system jest uregulowany w ustawie z dnia 13 czerwca 2019 r. o wykonywaniu działalności gospodarczej w zakresie wytwarzania i obrotu materiałami wybuchowymi, bronią, amunicją oraz wyrobami i technologią o przeznaczeniu wojskowym lub policyjnym (Dz. U. z 2023 r. poz. 1743). SRB wpisuje się w usługi zaufania, z uwagi na jego przewidziane połączenie z system PESEL, jak również ewentualne udostępnienie usługi związanej z wydawaniem zaświadczeń dla posiadaczy broni w trybie elektronicznym – w ramach planowanych usług dostępnych w aplikacji mObywatel. Biorąc powyższe pod uwagę, niezbędne jest zagwarantowanie dla MSWiA dodatkowych środków w szacowanej kwocie 2 mln. PLN, które umożliwią realizację ww. usługi.	**Uwaga wyjaśniona** Minister właściwy do spraw wewnętrznych został ujęty w OSR. Kwestia udostępnienia usługi związanej z wydawaniem zaświadczeń dla posiadaczy broni w trybie elektronicznym – w ramach planowanych usług dostępnych w aplikacji mObywatel pozostaje poza zakresem niniejszej regulacji, gdyż projektowane przepisy nie zobowiązują do udostępnienia takiej usługi.
93.	OSR	MZ	W ramach prowadzonych konsultacji publicznych i opiniowania projekt ustawy został przekazany do zaopiniowania do szeregu organizacji wskazanych jako podmioty odpowiedzialne za źródła autentyczne1, jednak na liście tej zabrakło Krajowej Rady Ratowników Medycznych. Należy podkreślić, że Krajowa Rada Ratowników Medycznych, działająca na podstawie art. 129 i art. 137 ustawy z dnia 1 grudnia 2022 r. o zawodzie ratownika medycznego oraz samorządzie ratowników medycznych (Dz. U. z 2025 r. poz. 339, z późn. zm.), prowadzi rejestr ratowników medycznych.	**Uwaga uwzględniona** OSR została uzupełniona.
94.	OSR pkt 2	KOSR	W odniesieniu do zadań, które zakłada się powierzyć ministrowi właściwemu ds. informatyzacji z możliwością wskazania wskazaną przez ten organ, jednostki podległej lub nadzorowanej do realizacji tych zadań, rekomendowane jest sprecyzowanie, jaki podmiot będzie ostatecznie realizował te czynności (pkt 2 OSR).	**Uwaga uwzględniona** OSR została uzupełniona.
95.	OSR pkt 4	MSWiA	Pod rozwagę poddaję uwzględnienie Szefa Urzędu do Spraw Cudzoziemców w części 4 Oceny Skutków Regulacji -„Podmioty, na które oddziałuje projekt”, jako podmiotu odpowiedzialnego za źródło autentyczne, w rozumieniu art. 3 pkt 47 rozporządzenia 910/2014	**Uwaga uwzględniona** OSR została uzupełniona.

			Parlamentu Europejskiego i Rady (UE) 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, a co za tym idzie jako podmiotu: - zapewniającego kwalifikowanym dostawcom usług zaufania, którzy dostarczają kwalifikowane elektroniczne poświadczenia atrybutów, możliwość weryfikacji atrybutów w źródle, za które jest odpowiedzialny, drogą elektroniczną, na żądanie użytkownika, - składającego do ministra właściwego do spraw informatyzacji wnioski zawierające informacje, o których mowa w art. 7 ust. 5 rozporządzenia wykonawczego Komisji (UE) 2025/1569 z dnia 29 lipca 2025 r. w sprawie ustanowienia zasad stosowania rozporządzenia Parlamentu Europejskiego i Rady (UE) nr 910/2014 w odniesieniu do kwalifikowanych elektronicznych poświadczeń atrybutów oraz elektronicznych poświadczeń atrybutów wydanych przez podmiot sektora publicznego odpowiedzialny za źródło autentyczne lub w jego imieniu w zakresie udostępniania informacji o tytułach pobytowych oraz dokumentach tożsamości wydawanych przez organy RP cudzoziemcom (poświadczania zezwoleń pobytowych). Należy zauważyć, że Szef Urzędu do Spraw Cudzoziemców, zgodnie z art. 449 ust. 1 ustawy z dnia 12 grudnia 2013 r. o cudzoziemcach (Dz. U. z 2025 r. poz. 1079, z późn. zm.), tworzy oraz prowadzi w systemie teleinformatycznym krajowy zbiór rejestrów, ewidencji i wykazu w sprawach cudzoziemców będący zbiorem autentycznym i referencyjnym w powyższym zakresie.	
96.	OSR pkt 6	KOSR	W zakresie wpływu na sektor finansów publicznych (pkt 6 OSR) należy: a) wskazać jaka konkretnie część kosztów zostanie zrefundowana lub sfinansowana przy udziale środków unijnych z programu FERC, a jaka ze środków krajowych. Wysokość finansowania z FERC powinna być omówiona pod tabelą pkt 6 OSR (w tabeli tylko finansowanie krajowe i wkład krajowy przy finansowaniu z FERC); b) przedstawić przyjętą metodykę i założenia obliczenia kosztów projektu (utrzymanie, budowa i rozwój systemów IT). Nie jest jasne, jakie działania wymagają poniesienia przedstawionych kosztów projektu, a także czy przedstawione wydatki związane są ze zwiększoną liczbą etatów (w takim przypadku należy przedstawić odpowiednio pracochłonność zadań).	**Uwaga uwzględniona** OSR została uzupełniona.

97.	OSR pkt 6	MFiG (MF)	Zgodnie z informacją zawartą w OSR w pkt 6. Wpływ na sektor finansów publicznych, rozwiązania przewidziane w ustawie finansowane będą z budżetu państwa z części budżetowej 27 (informatyzacja). Dodatkowo w pkt 6 OSR wskazano, że Wydatki związane z wejściem w życie rozwiązań przewidzianych w ustawie zostaną sfinansowane w ramach limitów wydatków części budżetowej 27, bez konieczności ich zwiększania w roku wejścia w życie ustawy oraz w latach kolejnych. W związku z finansowaniem przedmiotowych zadań w ramach posiadanych środków, z projektu ustawy należy usunąć art. 10, w którym określono maksymalny limit wydatków z budżetu państwa będący skutkiem wejścia w życie niniejszej ustawy.	**Uwaga wyjaśniona** W OSR zostały wprowadzone stosowne zmiany w zakresie uwzględniania zwiększenia limitu wydatków z budżetu państwa na kolejne lata następujące po 2026 r.
98.	OSR pkt 6	MFiG (MF)	W OSR wskazano, że część zadań związanych z budową i utrzymaniem europejskiego portfela tożsamości cyfrowej zostanie sfinansowanych przy udziale środków pochodzących z budżetu Unii Europejskiej z programu FERC. Jednocześnie brak jest informacji w jakiej wysokości będą to środki, oraz czy kwoty zaprezentowane w części tabelarycznej OSR obejmują wyłącznie środki krajowe, czy również środki unijne. Powyższe wymaga wyjaśnienia również w zakresie podanej informacji, że kwoty wydatków budżetu państwa ujęte w części tabelarycznej są tożsame z kwotami ujętymi w art. 10 projektu ustawy. OSR należy doprecyzować poprzez wyodrębnienie wydatków przewidzianych do sfinansowania ze środków krajowych oraz środków unijnych.	**Uwaga uwzględniona** OSR została uzupełniona.
99.	OSR pkt 6	MFiG (MF)	W pkt 6 OSR określono koszty realizacji przedmiotowego projektu na poziomie 45,5 mln zł w roku 2026 oraz 696,57 mln zł w 10-letnim okresie realizacji. Projektodawca zaznaczył również, że „Wydatki związane z wejściem w życie rozwiązań przewidzianych w ustawie zostaną sfinansowane w ramach limitów wydatków części budżetowej 27, bez konieczności ich zwiększania w roku wejścia w życie ustawy oraz w latach kolejnych. [...] Przewiduje się, że część zadań związanych z budową i utrzymaniem europejskiego portfela tożsamości cyfrowej, o którym mowa w art. 5a ust. 2 lit. a rozporządzenia 910/2014 zostanie sfinansowanych przy udziale środków pochodzących z budżetu Unii Europejskiej z programu FERC.”. W OSR w Tabeli pkt 6 zasadne byłoby dookreślenie udziału planowanych środków europejskich oraz ich ewentualny wpływ na finansowanie krajowe w poszczególnych latach (czy finansowanie krajowe będzie się zmniejszać w związku z tym).	**Uwaga uwzględniona** OSR została uzupełniona.
100.	OSR pkt 6	MFiG (MF)	W Dodatkowych informacjach zaznaczono, że: „Wydatki budżetu państwa zaprezentowane w tabeli powyżej wynikają z kosztów jakie Centralny Ośrodek Informatyki (instytucja gospodarki budżetowej) poniesie w związku z realizacją zadań wynikających z ustawy, a które następnie zostaną poniesione z budżetu państwa z części budżetowej 27 (informatyzacja).”. Należy zauważyć, że Centralny Ośrodek Informatyki to instytucja gospodarki	**Uwaga uwzględniona** OSR została uzupełniona.

			budżetowej, o której mowa w art. 24–28 ustawy o finansach publicznych. Zgodnie z art. 9 pkt 6 ustawy jednostki te należą do sektora finansów publicznych. Oznacza to, że Centralny Ośrodek Informatyki powinien być ujęty w Tabeli w pkt 6 OSR i odpowiednio zaznaczone przepływy między jednostką a budżetem państwa. Brak wyodrębnienia jednostki w Tabeli powoduje niepełne odzwierciedlenie przepływów w sektorze finansów publicznych oraz może prowadzić do nieczytelności prezentowanych danych. Należy zauważyć, że z uwagi na to, że koszty, które przewiduje się ponieść z tytułu projektowanych przepisów, ujęte są w limicie cz. 27, przepływy między budżetem państwa a Centralnym Ośrodkiem Informatyki pozostają bez wpływu na przestrzeń wydatkową wyznaczoną przez stabilizującą regułę wydatkową, o której mowa w art. 112 aa ustawy o finansach publicznych.	
101.	OSR pkt 6	MFiG (MF)	Proponujemy bardziej szczegółowo opisać jakie składniki kosztów składają się na ujęte w pkt 6 OSR w Dodatkowych informacjach kwoty w tabeli w podziale na: Utrzymanie, Budowa i Rozwój.	**Uwaga uwzględniona** OSR została uzupełniona.
102.	OSR pkt 6	MFiG (MF)	Pod tabelą wskazano, że: „Koszty w ramach utrzymania RCT (Rozwoju Cyfrowej Tożsamości) oraz Rozwoju nie zostały oszacowane z uwagi na odległy horyzont czasowy”, a zatem pytanie jakie dokładnie koszty ujęto w tabeli, a których nie ujęto. W OSR wskazano zatem, że Koszty utrzymania RCT oraz Rozwoju nie zostały oszacowane z uwagi na odległy horyzont czasowy, jednak w tabeli przedstawiono konkretne wartości w podziale na „Utrzymanie” oraz „Budowa i Rozwój”. Wymaga wyjaśnienia: czy wykazane kwoty obejmują pełny zakres kosztów, czy jedynie koszty budowy, jakie elementy kosztowe nie zostały uwzględnione. Ma to również bezpośredni związek z projektowanym art. 10 ust. 2, w którym wskazano, że: „W przypadku przekroczenia lub zagrożenia przekroczeniem przyjętego na dany rok budżetowy maksymalnego limitu wydatków określonego w ust. 1, stosuje się mechanizm korygujący polegający na ograniczeniu kosztów związanych z realizacją zadań wynikających z ustawy.”. Powstaje wątpliwość, w jaki sposób ma być stosowany wskazany w tym przepisie mechanizm korygujący. W obecnym brzmieniu przepis ma charakter blankietowy i pozostaje na dużym stopniu ogólności. Przepis nie wskazuje zasad stosowania mechanizmu korygującego, co może utrudniać jego praktyczne zastosowanie. Nie jest jasne bowiem, jakie dokładnie koszty ujęto w projektowanym art. 10 i OSR (czy tylko na budowę RCT). Wymaga to wyjaśnienia i doprecyzowania. Podkreślenia wymaga, że co do zasady mechanizm korygujący konstruowany przez projektodawcę ustawy winien polegać na obniżeniu kosztów realizacji wyznaczonych zadań, tj. powinien w sposób dokładny i konkretny określać zakres wprowadzanego ograniczenia, tak aby mógł on doprowadzić do	**Uwaga uwzględniona** OSR została uzupełniona.

			redukcji kosztów do maksymalnego limitu wydatków przyjętego na dany rok budżetowy, w przypadku zagrożenia przekroczenia tego limitu.	
103.	OSR pkt 7	KOSR	Rekomendowane jest doprecyzowanie opisu wpływu regulacji na przedsiębiorców i obywateli pod kątem praktycznym, w kontekście funkcjonowania aplikacji mObywatel (pkt 7 OSR).	**Uwaga uwzględniona** OSR została uzupełniona.
104.	OSR pkt 8	KOSR	Rekomendowane jest szersze omówienie zmian w obciążeniach regulacyjnych na skutek projektu, w szczególności omówienie obowiązków wynikających ze zmian poza bezwzględnie wymaganymi przez UE (pkt 8 OSR).	**Uwaga uwzględniona** OSR została uzupełniona.
105.	OSR pkt 10	KOSR	W pkt 10 OSR wskazano, że „ocena skutków dla ochrony danych osobowych zostanie sporządzona po ustaleniu ostatecznej treści przepisów, na późniejszym etapie". Rekomendowane jest przedstawienie takiej oceny bądź uzupełnienie oceny skutków regulacji pod kątem ochrony danych osobowych	**Uwaga uwzględniona** Ocena skutków dla ochrony danych osobowych zostanie dołączona.
106.	Uwaga ogólna	MFiG (MRiT)	Mając na uwadze, fakt, że europejski portfel tożsamości cyfrowej jest w szczególności środkiem identyfikacji elektronicznej, który będzie włączony do mObywatela, ale będzie funkcjonował obok aplikacji mObywatel, nie zastępując jej, wyjaśnienia wymaga zakres przedmiotowy usługi „Firma" dostępnej w aplikacji mObywatel w kontekście jej integracji z europejskim portfelem tożsamości cyfrowej. Zwracamy uwagę, że zgodnie z art. 3 ust. 1 ustawy z dnia 6 marca 2018 r. o Centralnej Ewidencji i Informacji o Działalności Gospodarczej przekazywanie danych i informacji do CEIDG oraz przekazywanie danych i informacji z CEIDG odbywa się za pośrednictwem systemu teleinformatycznego CEIDG lub za pośrednictwem innego, zintegrowanego z nim systemu teleinformatycznego, w szczególności za pośrednictwem systemu Punktu Informacji dla Przedsiębiorcy, o którym mowa w art. 51 ust. 1 tej ustawy. Przekazywanie danych i informacji do oraz z CEIDG za pośrednictwem systemu teleinformatycznego CEIDG polega na wykorzystaniu w tym celu systemu informatycznego, który umożliwia jednostkom administracji publicznej świadczenie usług publicznych opartych na elektronicznych kanałach komunikacji przez tzw. pojedynczy punkt dostępowy w Internecie. Zgodnie z ustawą CEIDG wnioski o wpis do CEIDG opatruje się kwalifikowanym podpisem elektronicznym, podpisem zaufanym albo podpisem osobistym, albo podpisuje w inny sposób akceptowany przez system CEIDG, umożliwiający jednoznaczną identyfikację osoby przesyłającej wniosek, czas jego przesyłania oraz zapewniający integralność danych zawartych we wniosku.	**Uwaga wyjaśniona** W związku z tym, że zgodnie z art. 5a ust. 7 rozporządzenia eIDAS pod pewnymi warunkami państwa członkowskie mogą przewidzieć, zgodnie z prawem krajowym, dodatkowe funkcje europejskich portfeli tożsamości cyfrowej, w projektowanym nowym przepisie art. 14g ust. 2 ustawy o aplikacji mObywatel przewidziano że w europejskim portfelu tożsamości cyfrowej wydawanym przez ministra właściwego do spraw informatyzacji można udostępniać inne usługi, niż określone w ust. 1, świadczone przez podmioty publiczne lub podmioty niepubliczne prowadzące rejestry publiczne, rejestry niepubliczne lub systemy teleinformatyczne. Z uwagi na to, że konstrukcja techniczna, wymagania dotyczące poziomu bezpieczeństwa dla europejskiego portfela tożsamości cyfrowej różnią od rozwiązań przyjętych dla aplikacji mObywatel, zważywszy dodatkowo, że europejski portfela tożsamości cyfrowej jest formalnie nowym narzędziem, które wcześniej nie mogło istnieć, przyjęto założenie, że nie można przenieść istniejących obecnie usług w aplikacji mObywatel z mocy ustawy do europejskiego portfela tożsamości cyfrowej. Zakłada się, że powtórzony zostanie tu zweryfikowany już w praktyce proces wnioskowy, co zostało odpowiednio przewidziane w zmienianych przepisach art. 16 ustawy o aplikacji mObywatel.

107.	Uwaga ogólna	MSWiA	Zasadniczą wątpliwość budzi brak umiejscowienia roli Ministra Spraw Wewnętrznych i Administracji, kształtującego politykę bezpieczeństwa dokumentów publicznych oraz zapewniającego funkcjonowanie systemu bezpieczeństwa dokumentów publicznych, w odniesieniu do projektowanych kwestii obejmujących dokumenty/atrybuty w formie elektronicznej. Zaznaczenia wymaga w tym miejscu, że system bezpieczeństwa dokumentów publicznych obejmuje między innymi projektowanie, wytwarzanie, przechowywanie oraz weryfikację autentyczności dokumentów publicznych, a także współpracę z międzynarodowymi instytucjami i organizacjami zajmującymi się bezpieczeństwem dokumentów publicznych. Procedowanie przywołanych kwestii powinno odbywać się przy uwzględnieniu istotnej roli Ministra Spraw Wewnętrznych i Administracji. Rozwiązanie polegające na wyłączeniu dokumentów w formie elektronicznej do odrębnego reżimu organizacyjno-prawnego, w istocie może prowadzić do utworzenia dwóch równoległych i niezależnych systemów bezpieczeństwa dokumentów emitowanych w postaci fizycznej i elektronicznej, co z kolei rodzi ryzyko negatywnego wpływu zarówno na jednolitość polityki bezpieczeństwa dokumentów publicznych jak i szczelność systemu bezpieczeństwa dokumentów służących do identyfikacji osób, rzeczy lub potwierdzających stan prawny lub prawa osób posługujących się takimi dokumentami.	**Uwaga wyjaśniona** Dokumenty publiczne nie są i nie były również wcześniej przedmiotem 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 (eIDAS) Ostatnie zmiany wprowadzone do rozporządzenia eIDAS rozporządzeniem Parlamentu Europejskiego i Rady (UE) 2024/1183 ustanowiły między innymi europejski portfel tożsamości cyfrowej i nową usługę zaufania jaką jest wydawanie elektronicznych poświadczeń atrybutów. Zarówno europejski portfel tożsamości cyfrowej jak i elektroniczne poświadczenia atrybutów zostały nie tylko zdefiniowane w rozporządzaniu eIDAS, aktach wykonawczych do tego rozporządzenia, ale również precyzyjnie opisano wymagania organizacyjne i techniczne wobec tych narzędzi wskazując na właściwe normy Europejskiego Instytutu Norm Telekomunikacyjnych (ETSI). Z pewnością zatem europejski portfel tożsamości cyfrowej, jak również elektroniczne poświadczenia atrybutów nie są dokumentami publicznymi w rozumieniu ustawy z dnia 22 listopada 2018 r. o dokumentach publicznych (t.j. Dz. U. z 2024 r. poz. 1669 z późn. zm.), jak również należą do odrębnego niezależnego reżimu organizacyjno-prawnego ustanowionego na poziomie europejskim. Nie można zatem zgodzić się z tezą, że ww. przepisy europejskie wyłączające do odrębnego reżimu prawnego określone dokumenty w postaci elektronicznej będą miały jakikolwiek negatywny wpływ na jednolitość polityki bezpieczeństwa dokumentów publicznych jak i szczelność systemu bezpieczeństwa dokumentów służących do identyfikacji osób, rzeczy lub potwierdzających stan prawny lub prawa osób posługujących się takimi dokumentami. Wprost przeciwnie, europejskie portfele tożsamości cyfrowej i elektroniczne poświadczenia atrybutów mogą i powinny stać się ważnym uzupełnieniem dokumentów publicznych w rozumieniu ustawy z dnia 22 listopada 2018 r. o dokumentach publicznych i skutecznie zastępować je w usługach online i stosownych przypadkach również w trybie offline (zob. art. 3 pkt 2, art. 5a

				ust. 4 lit. a oraz ust. 5 lit. a ppkt III eIDAS). W tym miejscu warto podkreślić, że z uwagi na kryptograficzne zabezpieczenia europejskiego portfela tożsamości cyfrowej i elektronicznych poświadczeń atrybutów ich weryfikacja przez strony ufające nie będzie wymagała znajomości zabezpieczeń, o których mowa w rozporządzeniu Ministra Spraw Wewnętrznych i Administracji z dnia 1 lipca 2022 r. w sprawie wykazu minimalnych zabezpieczeń dokumentów publicznych przed fałszerstwem (Dz. U. poz. 1456) a jedynie posiadania oprogramowania do weryfikacji ważności elektronicznego poświadczenia atrybutów lub zestawu danych identyfikujących osobę. Co do zasady z przepisów europejskich już wynika, że państwa członkowskie są zobowiązane do zapewnienia co najmniej jednego europejskiego portfela tożsamości cyfrowej (który może być zapewniony bezpośrednio przez państwo członkowskie, na podstawie upoważnienia od państwa członkowskiego lub niezależnie od państwa członkowskiego, lecz uznawane przez to państwo członkowskie). Zakładając, że zgłoszona uwaga nie podważa założenia, że europejski portfel tożsamości cyfrowej będzie wydawany przez ministra właściwego do spraw informatyzacji pozostaje wyjaśnienie sposobu zapewniania i zasad uznawania elektronicznych poświadczeń atrybutów. Rozporządzenie eIDAS wprost art. 5f ust. 1 i 2 oraz art. 6 ustanawia obowiązek transgranicznego uznawania środków identyfikacji elektronicznej w tym europejskich portfeli tożsamości cyfrowej w usługach publicznych i w części usług prywatnych. Ponadto 45b ust. 2 ustanawia, że kwalifikowane elektroniczne poświadczenie atrybutów oraz poświadczenia atrybutów wydane przez podmiot sektora publicznego odpowiedzialny za źródło autentyczne lub w jego imieniu ma taki sam skutek prawny jak poświadczenia wydane zgodnie z prawem w postaci papierowej. Celem tych przepisów jest niewątpliwie zapewnienie w całej UE wspólnej podstawy bezpiecznej interakcji elektronicznej między obywatelami, przedsiębiorstwami i organami publicznymi, co pozwoli podnieść efektywność publicznych i prywatnych usług online, e-biznesu i e-handlu w Unii, co wynika z wprost motywów 1 i 2 preambuły. Mając na uwadze, że przepisy rozporządzenia eIDAS stosuje się wprost, znaczy to że zarówno kwalifikowani dostawcy usług zaufania jak i krajowe podmioty odpowiedzialne za źródła

				autentyczne mogą wydawać elektroniczne poświadczenia atrybutów ważne w całej UE pod warunkiem, że spełnią stosowne wymagania wynikające z przepisów eIDAS i aktów wykonawczych. Dodatkowo rozporządzenie eIDAS umożliwia wyznaczenie przez państwa członkowskie podmiotu sektora publicznego, upoważnionego do wydawania takich poświadczeń atrybutów w imieniu podmiotów sektora publicznego odpowiedzialnych za źródła autentyczne. Istotne jest również, że przepisy eIDAS nie przewidują wyznaczenia do takiej roli podmiotu innego niż publiczny. Wydaj się to oczywiste z uwagi na to, że państwa członkowskie co do zasady zgodnie z art. 45e zapewniają środki umożliwiające kwalifikowanym dostawcom usług zaufania, którzy dostarczają kwalifikowane elektroniczne poświadczenia atrybutów, weryfikację atrybutów polegających na źródłach autentycznych w sektorze publicznym drogą elektroniczną, na żądanie użytkownika. Propozycja aby podmiotem który ma możliwość wydawania elektronicznych poświadczeń atrybutów w imieniu podmiotów sektora publicznego odpowiedzialnych za źródła autentyczne był minister właściwy do spraw informatyzacji nie wyklucza możliwości wydawania elektronicznych poświadczeń atrybutów przez podmioty w swoim imieniu. W związku z niepewnością w tym zakresie proponuje się stosowną zmianę w art. 22f ustawy o usługach zaufania oraz identyfikacji elektronicznej. Warto również wskazać na projektowany przepisy art. 22h ustawy o usługach zaufania oraz identyfikacji elektronicznej z których wynika że minister właściwy do spraw informatyzacji wydaje elektroniczne poświadczenia atrybutów na wniosek podmiotów zainteresowanych zawierający w szczególności odniesienie do przepisów, norm lub wytycznych, jeżeli mają zastosowanie Podsumowując, nie ma zagrożenia, że w związku z proponowanymi przepisami ucierpi szczelność systemu bezpieczeństwa dokumentów służących do identyfikacji osób, rzeczy lub potwierdzających stan prawny lub prawa osób posługujących się takimi dokumentami.
108.	Uzasadnienie	MSZ	Zgodnie z art. 11a ust. 2 rozporządzenia 910/2014 państwa członkowskie określają środki techniczne i organizacyjne w celu	**Uwaga wyjaśniona** W uzasadnieniu zostanie dodatkowo wyjaśnione jakie środki techniczne wynikają z przyjętych rozwiązań w zakresie

			zapewnienia wysokiego poziomu ochrony danych osobowych wykorzystywanych do dopasowywania tożsamości oraz w celu zapobiegania profilowaniu użytkowników. O ile w projekcie ustawy przewidziano rozwiązania dotyczące funkcjonowania systemów, weryfikacji danych oraz przetwarzania danych w różnych elementach systemu, to rozporządzenie nakłada także obowiązek określenia środków technicznych. Projektodawca powinien zatem wyjaśnić w jaki sposób zostanie zrealizowany obowiązek określenia środków technicznych w celu zapewnienia wysokiego poziomu ochrony danych osobowych.	dotyczącym funkcjonowania systemów, weryfikacji danych oraz przetwarzania danych w różnych elementach systemu i co za tym idzie wyjaśnione zostaną ewentualne wątpliwości dotyczące zapewnienia wysokiego poziomu ochrony danych osobowych.
109.	Uwaga ogólna	MSZ	Rozporządzenie 2024/1183 nakłada na państwa członkowskie szereg obowiązków informacyjnych, np.: w art. 5d ust 1– informowanie Komisji oraz grupy współpracy o europejskich portfelach tożsamości cyfrowej; w art. 12a ust. 6 – przekazywanie Komisji nazwy i adresów jednostek oceniających zgodność; w art. 45f ust. 3 – notyfikacja Komisji podmiotów sektora publicznego; w art. 46c ust. 3 – podawanie do publicznej wiadomości oraz informowanie Komisji o nazwie oraz adresach pojedynczego punktu kontaktowego; w art. 48a – zbieranie danych statystycznych. Wyjaśnienia wymaga sposób realizacji tych obowiązków, gdyż nie wynika on z projektu.	**Uwaga częściowo uwzględniona** W ramach nowego brzmienia projektowanego art. 23 ustawy o usługach zaufania oraz identyfikacji elektronicznej zostaną dodany pkt 19 w zakresie dot. obowiązku z art. 48a rozporządzenia 910/2014. Pozostałe obowiązki informacyjne już zostały uwzględnione lub zostaną uwzględnione w związki innymi uwagami MSZ.
110.	Uwaga ogólna	MFiG (MF)	W związku z wprowadzanymi w projekcie nowymi typami podpisów zaufanych (dla podmiotu publicznego i osoby reprezentującej taki podmiot) rozważenia wymaga dodanie przepisu precyzującego, że ilekroć w przepisach jest mowa o podpisie zaufanym, rozumie się przez to także te dwa nowe rodzaje PZ. Pozwoli to ograniczyć wątpliwości i ewentualną konieczność zmian w ustawach opisujących poszczególne procedury - np. Ordynacja podatkowa, Kodeks postępowania administracyjnego, ustawa o KAS i wiele innych. Kolejną uwagą dotyczącą nowego rodzaju PZ jest umieszczenie w nim daty urodzenia. Z uzasadnienia wynika, że celem utworzenia PZ dla osoby reprezentującej podmiot publiczny jest chęć umożliwianie podpisywania pism organu PZ, bez konieczności ujawniania danych osobowych (numeru PESEL) pracowników organu. Jednocześnie ten PZ zawierać ma datę urodzenia. W konsekwencji nadal istnieje ryzyko wątpliwości w kontekście ochrony danych osobowych. Już obecnie możliwe jest wydawanie podpisów kwalifikowanych, w których certyfikacie nie jest zapisany numer PESEL i taki rodzaj podpisu nie wymaga ujawniania daty urodzenia. Zamiast danych osobowych w takim certyfikacie podpisu kwalifikowanego identyfikatorem może być np. numer	**Uwaga częściowo uwzględniona** Celem projektowanych przepisów jest udostepnienie środków identyfikacji elektronicznej, a nie podpisu elektronicznego. Projektodawcy celowo nie rozróżniają profili zaufanych, gdyż wiązałoby się z koniecznością nowelizacji licznych przepisów sektorowych, w tym ustaw i rozporządzeń, które wskazują na identyfikację za pomocą profilu zaufanego. Odnośnie do daty urodzenia w PZ osoby reprezentującej podmiot publiczny – uwaga została uwzględniona (zob. art. 20ad ust. 1b ustawy zmienianej w art. 4 projektowanej ustawy.

			nadawany przez centrum autoryzacyjne. Dlatego proponujemy, aby w tym nowym rodzaju PZ przyjąć analogiczne rozwiązanie - nie umieszczać w nim daty urodzenia, lecz jakiś unikalny identyfikator nadawany przez MC podczas tworzenia PZ dla takiej osoby reprezentującej podmiot publiczny. Pozwoli to zrealizować wszystkie potrzeby opisane w uzasadnieniu do projektu (jednoznaczne zidentyfikowanie osoby reprezentującej z zachowaniem w tajemnicy jej danych osobowych w postaci daty urodzenia).	
111.	Uwaga ogólna	MSZ	do przedstawionego projektu nie została dołączona tabela zgodności. Przypominam, że zgodnie z § 30 ust. 1 pkt 1 Regulaminu pracy Rady Ministrów, w przypadku projektu ustawy mającego na celu wdrożenie prawa Unii Europejskiej lub służących stosowaniu tego prawa, organ wnioskujący dołącza do projektu tabelaryczne zestawienie przepisów prawa Unii Europejskiej, których wdrożeniu lub stosowaniu służy ta ustawa lub to rozporządzenie, oraz projektowanych przepisów prawa polskiego, zwane dalej "tabelą zgodności". Dodatkowo, jeśli projekt ustawy mającej na celu wdrożenie lub służącej stosowaniu prawa Unii Europejskiej może zawierać przepisy wykraczające poza ten cel, organ wnioskujący dołącza do projektu tabelaryczne zestawienie projektowanych przepisów ustawy, które wykraczają poza cel wdrożenia lub zapewnienia stosowania prawa Unii Europejskiej, wraz z wyjaśnieniem niezbędności objęcia ich tym projektem, zwane dalej "odwróconą tabelą zgodności" (§ 30 ust. 2 Regulaminu pracy Rady Ministrów). Mając powyższe na względzie zwracam się o uzupełnienie dokumentów do przedłożonego projektu ustawy	**Uwaga uwzględniona** Tabele zostaną dołączone.
112.	Uwaga ogólna	RCL	Przedmiotowy projekt ustawy służy stosowaniu 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, z późn. zm.), zwanego dalej „rozporządzeniem 910/2014”. W związku z wprowadzeniem do tego rozporządzenia regulacji związanych z europejskim portfelem tożsamości cyfrowej – rozporządzeniem Parlamentu Europejskiego i Rady (UE) 2024/1183 z dnia 11 kwietnia 2024 r. w sprawie zmiany rozporządzenia (UE) nr 910/2014 w odniesieniu do ustanowienia europejskich ram tożsamości cyfrowej (Dz. Urz. UE L 2024/1183 z 30.04.2024)1 – do przedmiotowego projektu ustawy powinno więc zostać dołączone dodatkowo tabelaryczne zestawienie przepisów prawa Unii Europejskiej, których stosowaniu służy przedmiotowy projekt, wraz z wyjaśnieniem określającym	**Uwaga uwzględniona** Tabele zostaną dołączone.

			przyczyny wejścia w życie ustawy oraz niektórych jej przepisów w danym terminie wraz z informacją, czy proponowane terminy wejścia w życie uwzględniają wymogi w zakresie terminów zapewnienia stosowania prawa Unii Europejskiej (§ 30 ust. 1 pkt 1 Regulaminu pracy Rady Ministrów). Ponadto, zważywszy że projekt ustawy, zgodnie z informacją zawartą w ocenie skutków regulacji oraz uzasadnieniu, ma charakter deregulacyjny i zawiera dodatkowo przepisy wykraczające poza cel służący stosowaniu prawa Unii Europejskiej, do projektu powinna zostać dołączona odwrócona tabela zgodności – tabelaryczne zestawienie projektowanych przepisów ustawy, które wykraczają poza cel zapewnienia stosowania prawa Unii Europejskiej, wraz z wyjaśnieniem niezbędności objęcia ich tym projektem.	