Uwagi zgłoszone w ramach opiniowania i konsultacji publicznych:
do projektu Projekt rozporządzenia Ministra Cyfryzacji w sprawie profilu zaufanego i podpisu zaufanego (Nr 153)

L. p.	Jednostka redakcyjna	Podmiot zgłaszający uwagę	Treść uwagi	Stanowisko MC
1.	§ 6 ust. 4	ZUS	Analiza projektowanego § 6 ust. 4 rozporządzenia wskazuje, że w trakcie rozmowy telefonicznej osoba upoważniona do potwierdzenia tymczasowego profilu zaufanego ustala z wnioskodawcą sposób i termin transmisji audiowizualnej. Z treści tego przepisu można wywnioskować, że dopuszcza się zastosowanie różnych narzędzi informatycznych do przeprowadzenia takiej transmisji. Wobec faktu, że w projekcie nie zostały wymienione wprost rodzaje tych narzędzi, istnieje w naszej ocenie ryzyko, że wybrany przez wnioskodawcę sposób transmisji może nie spełniać wymogów zapewnienia środków bezpieczeństwa. W związku z powyższym proponujemy, aby określić w projekcie rozporządzenia katalog narzędzi przeznaczonych do kontaktu z wnioskodawcą w celu przeprowadzenia zdalnego potwierdzenia tymczasowego profilu zaufanego podczas transmisji audiowizualnej, spełniających wymogi do zapewnienia środków bezpieczeństwa, bądź też określić w rozporządzeniu wymogi dotyczące konieczności zapewnienia środków bezpieczeństwa takiej transmisji.	**<u>Uwaga częściowo uwzględniona</u>** W przepisie celowo nie wskazano katalogu narzędzi do transmisji audiowizualnej. Co do zasady nie powinno się do przepisów prawa wpisywać konkretnych aplikacji. W przypadku wykrycia luk w bezpieczeństwie transmisji realizowanej za pomocą wskazanego w rozporządzeniu oprogramowania nie można byłoby go dalej stosować (natychmiast zmienić), a zmiana na inne oprogramowanie wymagałaby zmiany rozporządzenia. Dlatego minister będzie stosował takie oprogramowanie, które aktualnie będzie uznawane za bezpieczne i jednocześnie wygodne do zastosowania. W związku z uwagą Związku Powiatów Polskich dotyczącą potrzeby określenia maksymalnego terminu załatwiania sprawy, rozmowa telefoniczna zostanie zastąpiona wskazywaniem przez system najbliższych wolnych terminów do

				wyboru przez osobę wnioskującą. Po wybraniu daty i czasu zdalnego potwierdzenia tożsamości z wykorzystaniem wideoidentyfikacji wnioskodawca otrzyma pocztą elektroniczną wiadomość zawierającą pouczenie dotyczące sposobu przeprowadzenia tej transmisji (§ 5 ust. 3). Rozmowa telefoniczne będzie tylko dodatkową możliwością w przypadku, gdy transmisja audiowizualna w wybranym terminie nie dojdzie do skutku.
2.	§ 6 ust. 1	UODO	W kontekście unormowań § 6 ust. 1 projektu rozporządzenia, wyjaśnienia wymaga do jakich informacji oraz na jakich zasadach osoba potwierdzająca tymczasowy profil zaufany będzie miała dostęp do danych zawartych w rejestrze PESEL, o którym mowa w ustawie z dnia 24 września 2010 r. o ewidencji ludności (Dz. U. z 2019 r. poz. 1397, z późn. zm) oraz Rejestrze Dowodów Osobistych, o którym mowa w ustawie z dnia 6 sierpnia 2010 r. o dowodach osobistych (Dz. U. z 2020 r. poz. 332, z późn. Zm.). Z przepisów projektowanego rozporządzenia wynika (§ 6 w związku z § 13), że weryfikacji będzie podlegać jedynie imię (imiona), nazwisko, data urodzenia, numer PESEL oraz wizerunek osoby, natomiast oba rejestry zawierają zdecydowanie szersze spektrum danych. O ile w przypadku weryfikacji wykonywanej automatycznie przez system, w którym wydawany jest profil zaufany (§ 6 ust. 2), do pozyskiwania takich danych raczej nie będzie dochodzić – tak weryfikacja inna niż automatyczna może generować takie ryzyko. Należy pamiętać, że chociażby w rejestrze PESEL – gromadzona są też w powiązaniu z danymi osoby – również dane jej rodziców czy małżonka (art. 8 ustawy z dnia 24 września 2010 r. o ewidencji ludności). Dlatego bardzo istotne jest aby w ramach funkcjonalności weryfikacji wniosku, osoba weryfikująca nie miała możliwości dostępu do takich danych jak	**<u>Uwaga wyjaśniona</u>** Osoba potwierdzająca będzie miała dostęp do innych danych w rejestrach publicznych tylko w takim zakresie w jakim będzie to niezbędne do potwierdzania tożsamości to znaczy weryfikacji zgodności będą podlegać imię (imiona), nazwisko, data urodzenia, numer PESEL oraz wizerunek osoby. Dodatkowo osoba potwierdzająca będzie miała wprost informację o nr dowodu osobistego lub paszportu (jeżeli taki istnieje) osoby wnioskującej i ważności tych dokumentów. Zakłada się, że dostęp do tych danych osoba potwierdzająca ma na podstawie przepisu art. 20ca ust. 5 pkt 1 lit b ustawy.

			wskazane powyżej. Tym samym, projektodawca powinien w sposób szczegółowy przeanalizować projektowaną usługę wideoweryfikacji dla zachowania jej zgodności z zasadą zgodności z prawem, rzetelności i przejrzystości (art. 5 ust. 1 lit a RODO) Zgodnie, z którą dane osobowe muszą być przetwarzane zgodnie z prawem, rzetelnie i w sposób przejrzysty dla osoby, której dane dotyczą. oraz zasadą minimalizacji danych (art. 5 ust. 1 lit. c RODO) Zgodnie, z którą dane osobowe muszą być adekwatne, stosowne oraz ograniczone do tego co niezbędne do celów, w których są przetwarzane.	Jeżeli chodzi o dostęp do innych danych znajdujących się w tych rejestrach (takich których nie ma w warstwie graficznej dowodu osobistego) np. dane jej rodziców czy małżonka, to te dane mogą zostać udostępnione wyłącznie w trybie weryfikacji, to znaczy po podaniu ich przez osobę wnioskującą. Celem jest tu zapewnienie bezpiecznego potwierdzenia tożsamości osoby wnioskującej o tymczasowy profil zaufany co dla tak zwanego „średniego poziomu bezpieczeństwa”, o którym mowa w załączniku do *Rozporządzenia wykonawczego Komisji (UE) 2015/1502 z dnia 8 września 2015 r. w sprawie ustanowienia minimalnych specyfikacji technicznych i procedur dotyczących poziomów zaufania w zakresie środków identyfikacji elektronicznej na podstawie art. 8 ust. 3 rozporządzenia Parlamentu Europejskiego i Rady (UE) nr 910/2014,* wymaga podjęcia określonych działań w celu zminimalizowania ryzyka, że tożsamość danej osoby nie jest tożsamością deklarowaną, biorąc pod uwagę np. ryzyko utraty, kradzieży, zawieszenia, unieważnienia bądź upływu terminu ważności dokumentów. Bez podjęcia takich działań każda osoba posiadająca numer PESEL byłaby narażona na

				kradzież tożsamości, której konsekwencje są daleko większe niż potencjalne zagrożenie przetwarzaniem danych osoby, która złożyła wniosek o tymczasowy profil zaufany przez osobę upoważnioną przez Ministra Cyfryzacji. Mając na uwadze, że mamy do czynienia za zdalnym okazaniem dokumentu tożsamości celem wydania środka identyfikacji elektronicznej zabezpieczenia polegające na zminimalizowaniu ryzyka, że tożsamość danej osoby nie jest tożsamością deklarowaną są uzasadnione i zwiększają ochronę danych, a nie odwrotnie. Gdyby nie możliwość weryfikacji ważności i nr dokumentu tożsamości nie tylko na podstawie jego okazania w trakcie transmisji potencjalne zagrożenie uzyskaniem profilu zaufanego przez osobę podszywającą się pod inną osobę byłoby nieakceptowalne. Należy tez nadmienić, że profil zaufany pozwala na dostęp do danych wrażliwych w systemach ZUS i w Internetowym Koncie Pacjenta, dostęp do pełnych danych w rejestrze PESEL, do danych w Rejestrze Dowodów Osobistych do danych CEPiK itd. Niedochowanie staranności przy wydawaniu profilu zaufanego – nawet kosztem udostępnienia osobie potwierdzającej

				informacji o nr dokumentu tożsamości i jego ważności a także innych danych znajdujących się w warstwie graficznej tego dokumentu mogłoby mieć znaczące negatywne skutki nie tylko dla osób, których tożsamość zostałaby skradziona ale też dla całego systemu profilu zaufanego i co za tym idzie dla usług społeczeństwa informacyjnego. Powyższe jest zgodne z zasadą, zgodnie z którą dane osobowe muszą być adekwatne, stosowne oraz ograniczone do tego, co niezbędne do celów, w których są przetwarzane. Należy bowiem nadmienić, że przy potwierdzaniu tożsamości osoba wnioskująca okaże dokument w taki sposób, aby cała jego warstwa graficzna była widoczna i co za tym idzie wszystkie tam znajdujące się dane są przetwarzane na mocy ustawy. Dostępu do innych danych nie znajdujących się w warstwie graficznej dokumentu tożsamości, takich jak dane rodziców czy małżonka (art. 8 ustawy z dnia 24 września 2010 r. o ewidencji ludności nie przewiduje się wprost tylko w trybie weryfikacji danych zwartych w rejestrach – po podaniu ich przez wnioskodawcę. Na przykład wnioskodawca podaje nazwisko panieńskie matki, a osoba potwierdzająca wpisuje je do

				formularza w systemie i uzyskuje odpowiedź „prawda/fałsz” ale nie ma możliwości zobaczyć tych danych w systemie, jeżeli osoba wnioskująca ich nie poda.
3.	§ 6 ust. 4	UODO	Zgodnie z § 6 ust. 4 projektu rozporządzania (…) osoba upoważniona do potwierdzenia tymczasowego profilu zaufanego kontaktuje się z wnioskodawcą telefonicznie na numer telefonu podany we wniosku, podaje podczas rozmowy numer tego wniosku automatycznie nadany przez system, w którym wydawany jest profil zaufany i ustala sposób i termin transmisji audiowizualnej. Sposób i termin transmisji audiowizualnej osoba upoważniona do potwierdzenia tymczasowego profilu zaufanego potwierdza pocztą elektroniczną wysyłając stosowne zaproszenie na adres podany we wniosku o tymczasowy profil zaufany. Przepisy projektu rozporządzenia ani uzasadnienie projektu nie określą z zachowaniem jakich warunków technicznych ma się odbywać transmisja tak aby zachować zasady określone w art. 5 RODO, w szczególności celem zapewnienia integralności i poufności danych (art. 5 ust. 1 lit. f RODO) Zgodnie, z którą dane osobowe muszą być przetwarzane w sposób zapewniający odpowiednie bezpieczeństwo danych osobowych, w tym ochronę przed niedozwolonym lub niezgodnym z prawem przetwarzaniem oraz przypadkową utratą, zniszczeniem lub uszkodzeniem, za pomocą odpowiednich środków technicznych lub organizacyjnych. Nie wiadomo również na jakich zasadach i gdzie to nagranie będzie przechowywane. Ponadto konieczne jest ustalenie zasad retencji danych dla zachowania zgodności z zasadą ograniczenia przechowywania (art. 5 ust. 1 lit e RODO) Zgodnie, z którą dane osobowe muszą być przechowywane w formie umożliwiającej identyfikację osoby, której dane dotyczą, przez okres nie dłuższy, niż jest to niezbędne do celów, w których dane te są przetwarzane.	**<u>Uwaga wyjaśniona</u>** W związku z uwagą Związku Powiatów Polskich dotyczącą potrzeby określenia maksymalnego terminu załatwiania sprawy, rozmowa telefoniczna zostanie zastąpiona wskazywaniem przez system najbliższych wolnych terminów do wyboru przez osobę wnioskującą. Po wybraniu daty i czasu zdalnego potwierdzenia tożsamości z wykorzystaniem wideoidentyfikacji wnioskodawca otrzyma pocztą elektroniczną wiadomość zawierającą pouczenie dotyczące sposobu przeprowadzenia tej transmisji (§ 5 ust. 3).Rozmowa telefoniczne będzie tylko dodatkową możliwością w przypadku, gdy transmisja audiowizualna w wybranym terminie nie dojdzie do skutku. Dane osobowe zawarte we wniosku i następnie w profilu zaufanym są przechowywane w systemie teleinformatycznym, w którym wydawany jest profil zaufany przez 20 lat z zachowaniem bezpieczeństwa

				danych osobowych, w tym ochroną przed niedozwolonym lub niezgodnym z prawem przetwarzaniem oraz przypadkową utratą, zniszczeniem lub uszkodzeniem. Takie są wymogi dla każdego systemu teleinformatycznego podmiotu publicznego. 20-letni okres przechowywania danych wynika z tego, że podpis zaufany ma w niektórych zastosowaniach skutek prawny równoważy z podpisem własnoręcznym i co za tym idzie okres przechowywania dowodów wydania środka identyfikacji umożliwiającego złożenie takiego podpisu jest taki sam jak w przypadku dowodów wydania kwalifikowanego podpisu elektronicznego. Nowym dotychczas nie tworzonym dokumentem zastępującym dotychczasowy wydruk wniosku w przypadku potwierdzania profilu zaufanego w punkcie potwierdzającym jest nagranie z transmisji audiowizualnej, które ma być przechowywane zgodnie z ustawą przez okres krótszy, to znaczy przez 6 lat. Zasady przechowywania dokumentacji określają w przypadku Ministerstwa Cyfryzacji przepisy wydane na podstawie art. 6 ust. 2 ustawy z dnia 14 lipca 1983 r. o narodowym zasobie archiwalnym i archiwach

4.	§ 6 ust. 6	UODO	Zgodnie z § 6 ust. 4 projektu rozporządzenia osoba upoważniona do potwierdzania tymczasowego profilu zaufanego może w trakcie transmisji audiowizualnej zażądać wykonania gestu, który ułatwi wykrycie działania oprogramowania zakłócającego teletransmisję audiowizualną w sposób uniemożliwiający lub utrudniający potwierdzenie tożsamości wnioskodawcy. W kontekście obowiązków nakładanych na wnioskodawcę, w związku z przetwarzaniem jego danych osobowych, nie wiadomo jakie zobowiązanie z tego przepisu wynika. W szczególności nie wiadomo jakich danych osobowych oraz jakiego „gestu" może żądać osoba upoważniona od wnioskodawcy.	**<u>Uwaga wyjaśniona</u>** Chodzi o wykonanie jakiegokolwiek gestu jak np. otarcie twarzy prawą dłonią, pomachanie lewą dłonią przy prawym policzku itp. gestów, które są stosowane w celu wykrycia oprogramowania „podkładającego" twarz innej osoby do strumienia transmisji. Nie chodzi w tym przypadku o przetwarzanie dodatkowych danych osobowych. Gdyby wskazano w przepisach jakich gestów może żądać osoba potwierdzająca, to potencjalni twórcy oprogramowanie fałszującego przekazywany obraz mieliby ułatwione zadanie.
5.	§ 6 ust. 10	UODO	W odniesieniu do § 6 ust. 10 projektu rozporządzenia, w pierwszej kolejności należy wskazać, że konstrukcja przepisu nie gwarantuje osobie wnioskodawcy jakie jej dane mają być przetwarzane na zasadzie obowiązku – przepisy powinny być jednoznaczne co do tego jakie obowiązki w związku z przetwarzaniem danych nakłada się na osobę, której te dane dotyczą. Przyjęcia takiego rozwiązania przez projektodawcę wymaga zasada zgodności z prawem, rzetelności i przejrzystości (art. 5 ust. 1 pkt a) RODO). Przedmiotowy przepis nie powinien posługiwać się terminem „może zweryfikować" a „weryfikuje". Również pojęcie „dodatkowych danych dotyczących wnioskodawcy" jest nieprecyzyjne. Z przepisów projektowanego rozporządzenia nie wynika jakie miałyby być to dane – przepis w dalszej części odsyła jedynie do miejsc, których miałyby być zgromadzone (rejestry publiczne, dokumenty będące elementem akt sprawy podmiotu publicznego). Świadczy to o braku uwzględnienia przez projektodawcę ww. zasady minimalizacji danych. Także terminy „rejestry publiczne" oraz „systemy teleinformatyczne" są nieprecyzyjne, gdyż z przepisów rozporządzenia nie wynika jakich	**<u>Uwaga wyjaśniona</u>** Nie ma obowiązku weryfikacji za pomocą dodatkowych danych. Wymagana jest wideoidentyfikacja o której mowa w art. 20ca ust 5 pkt 1 ustawy. Weryfikacja wiedzy wnioskodawcy przy wykorzystaniu danych dotyczących wnioskodawcy zgromadzonych w rejestrach publicznych lub w systemach teleinformatycznych o której mowa w pkt 1 lit c , jest możliwą, ale nie wymaganą do zastosowania opcją dodatkową. Celowo nie wskazano, jakie dodatkowe dane mogłyby być weryfikowane, ponieważ może to być np. numer

			konkretnie rejestrów czy systemów ma to dotyczyć. Jeżeli miałoby to dotyczyć rejestrów dostępnych dla osoby potwierdzającej na takich zasadach jak dla każdego innego obywatela przez sieć Internet (np. Krajowy Rejestr Sądowy), to powinno to zostać wskazane w przepisach rozporządzenia. Przy tej okazji warto zwrócić uwagę projektodawcy na to, że pojęcie „rejestr publiczny" nie jest pojęciem tożsamym do „rejestru publicznie dostępnego".	paszportu (jeżeli wnioskodawca może go podać, a osoba weryfikująca zweryfikować), albo nawet numer silnika samochodu. Dodatkowo w przypadku, gdy dodatkowa weryfikacja będzie miała miejsce – wymaga się odnotowania tej czynności w systemie (§6 ust. 11)
6.	§ 6 ust. 10 pkt 2	UODO	Szczególne zaniepokojenie budzi konstrukcja § 6 ust. 10 pkt 2 projektu rozporządzenia – weryfikacja danych na podstawie dokumentu stanowiącego element akt sprawy podmiotu publicznego, który został doręczony wnioskodawcy. W takiej sytuacji będzie dochodzić do przetwarzania danych w celu innym niż zostały zgromadzone. Należy pamiętać, że rozwiązanie takie musi zostać ocenione po kątem zgodności z art. 6 ust. 4 RODO. Dopuszczalność zmiany celu, oparta na przepisach prawa, jest ograniczona wyłącznie do przypadków stanowiących w demokratycznym społeczeństwie niezbędny i proporcjonalny środek służący zagwarantowaniu celów, o których mowa w art. 23 ust. 1 RODO. Dlatego projektodawca powinien ponownie przeanalizować konstrukcję tej instytucji oraz jeśli uzna jej istnienie za niezbędne, zastanowić się nad jej ewentualną modyfikacją tak aby zapewnić poszanowanie prawa do prywatności osób wnioskujących o założenie profilu zaufanego, w szczególności poprzez ewentualne wprowadzenie unormowania, że weryfikacja w oparciu o dokumenty może odbyć się jedynie z inicjatywy wnioskodawcy oraz doprecyzowanie na podstawie jakich dokumentów i w dyspozycji jakich organów będących może następować weryfikacja. Jeżeli nie będzie to możliwe w przepisach rozporządzenia, to powinno to zostać przynajmniej wskazane w uzasadnieniu do projektu rozporządzenia. Unormowania w tym kształcie naruszają zasadę zgodności z prawem, rzetelności i przejrzystości (art. 5 ust. 1 lit a RODO) oraz minimalizacji danych (art. 5 ust. 1 lit c RODO).	**<u>Uwaga częściowo uwzględniona</u>** Proponuje się zmianę brzmienia przepisu § 6 ust.10: *„W przypadku wątpliwości odnośnie porównania wizerunku wnioskodawcy z wizerunkiem z Rejestru Dowodów Osobistych lub weryfikacji danych zawartych w warstwie graficznej dowodu osobistego albo paszportu wnioskodawcy okazanego przez niego w czasie rzeczywistym za pośrednictwem transmisji audiowizualnej, osoba upoważniona do potwierdzenia tymczasowego profilu zaufanego może zweryfikować tożsamość wnioskodawcy przy wykorzystaniu dodatkowych danych dotyczących wnioskodawcy, podanych przez niego w trakcie trwania procesu weryfikacji, których zgodność może zostać zweryfikowana z danymi zgromadzonymi w rejestrach publicznych lub w systemach teleinformatycznych prowadzonych przez ministra, w szczególności:*

				1) danych zawartych w warstwie graficznej dowodu osobistego lub paszportu widzianych w czasie rzeczywistym podczas transmisji audiowizualnej, *2) danych podanych przez wnioskodawcę w przypadku gdy chodzi o dane znajdujące się w rejestrze publicznym lub systemie teleinformatycznym prowadzonym przez ministra.”.* Wskazany przepis będzie służył samym wnioskującym, którzy w uzasadnionych przypadkach będą mogli ,pozwolić na dodatkową, szerszą weryfikację swojej tożsamości, ale tylko wtedy gdy będzie to możliwe techniczne (osoba potwierdzająca będzie mogła zweryfikować podane przez wnioskodawcę dane). Przepis należy czytać łącznie z §6 ust. 11, który wskazuje na zweryfikowanie dodatkowych danych z właściwym rejestrem publicznym i odnotowanie tej czynności w systemie, w którym wydawany jest profil zaufany. Użycie dodatkowych danych do potwierdzenia tożsamości będzie odnotowane w systemie (w uwagach do wniosku),ale nie będzie tam tych danych tylko informacja o ich użyciu.
7.	§ 7	UODO	Zgodnie z § 7 projektu rozporządzenia minister dostosuje, uwzględniając możliwości techniczne, proces potwierdzania tymczasowego profilu	**<u>Uwaga częściowo uwzględniona</u>** Przepis ma celowo charakter

			zaufanego, o którym mowa w § 6, do potrzeb osób mających szczególne potrzeby, takie jak „niemożność zrozumiałego mówienia czy głuchota”. Nie kwestionując zasadności dostosowania procesu potwierdzania tymczasowego profilu zaufanego do potrzeb osób z niepełnosprawnościami – proces potwierdzania profilu tymczasowego powinien dla tych osób zostać uregulowany na poziomie aktu wykonawczego, gdyż w obecnie projektowanej formie ma on charakter deklaratywny a nie normatywny. Jednocześnie, przy konstrukcji takiego przepisu projektodawca powinien użyć sformułowań w sposób poprawny opisujący niepełnosprawności, do których się odnosi, gdyż pojęcia „niemożność zrozumiałego mówienia czy głuchota” mają charakter potoczny.	deklaratywny, a nie normatywny, ponieważ możliwość potwierdzania tymczasowego profilu zaufanego dla osób z niepełnosprawnościami uniemożliwiającymi im przykładowo przeprowadzenie rozmowy podczas transmisji audiowizualnej może być zastąpione w różny sposób wskazany w ustawie z dnia z dnia 19 sierpnia 2011 r o języku migowym i innych środkach komunikowania się. Zwykle w przypadku wykorzystywania aplikacji przeznaczonych do połączeń konferencyjnych możliwe jest porozumiewanie się z częścią osób niemówiących na tzw. czacie, ale niektórzy mogą wymagać pomocy tłumacza. Te kwestie z uwagi na pilność potrzeby oddania do użytku takiej usługi nie zostały jeszcze rozwiązane w taki sposób, aby zapewnić osobom niepełnosprawnym bezpieczną obsługę, a z drugiej strony nie można wykluczać osób niepełnosprawnych. Bez proponowanego przepisu tymczasowy profil zaufany byłby dla nich niedostępny.
8.	§ 8 ust. 3 pkt 2	UODO	§ 8 ust. 3 pkt 2 projektu rozporządzania in fine powinien odsyłać do ust. 2 pkt. 1, w którym jest mowa o warunkach składania podpisu zaufanego, a nie ust. 1 pkt. 2.	**Uwaga wyjaśniona.** Wskazanie na ust. 1 pkt 2 jest poprawne.
9.	§ 11 ust. 5	UODO	§ 11 ust. 5 projektu rozporządzenia wskazuje, że użytkownik może używać adresu poczty elektronicznej zamiast unikatowego identyfikatora pod warunkiem, że w systemie, w którym wydawany jest profil zaufany, z tym	**Uwaga wyjaśniona`** Wielokrotne występowanie o profil zaufany i możliwość posiadania wielu

			adresem poczty powiązany jest tylko jeden identyfikator. Zgodnie z uzasadnieniem do projektu rozporządzenia, ww. przepis stał się potrzebny ze względu na to, że to udogodnienie wprowadzane w licznych systemach wymagających identyfikacji użytkowników jest dość często mylnie rozumiane przez posiadaczy profilu zaufanego jako utrudnienie. Dzieje się tak w przypadku gdy sam użytkownik założy kilka kont w systemie, w którym wydawany jest profil zaufany, co w efekcie powoduje, że nie ma możliwości przyporządkowania weryfikacji hasła, bo nie wiadomo, do jakiego konta użytkownik zamierza się logować. Przepis ma rozwiać wątpliwości w tym zakresie. Opisany wyżej fragment uzasadnienia, wskazuje na zależność profilu zaufanego od adresu poczty elektronicznej, a nie od osoby, dla której jest wystawiony profil zaufany. Takie podejście może powodować wielokrotność występowania o profil zaufany, gdyż wnioskujący może mieć wiele kont poczty elektronicznej. W przypadku gdy osoba będzie chciała pozyskać profil zaufany dla każdego identyfikatora jakim jest adres e-mail, będzie zachodzić procedura potwierdzania danych np. drogą wideoidentyfikacji, co w efekcie zwielokrotni ilość pozyskanych danych poprzez dokonania utrwalenia zawartości dokumentu tożsamości.	kont w systemie profilu zaufanego jest faktem, ponieważ taka jest konstrukcja tego systemu. Najpierw jest zakładane konto, do którego dostęp ma tylko osoba która je założyła, a dopiero potem potwierdzana jest tożsamość osoby która założyła konto. Dzięki tej metodzie nie ma potrzeby przekazywania/wydawania haseł do systemu, numerów PIN itp. zabezpieczeń – wystarczy potwierdzenie tożsamości i deklaracja osoby której potwierdza się profil zaufany, że wniosek jej dotyczy i ona będzie wyłącznie dysponować profilem. Można mieć tylko jeden profil zaufany bez względu na to,ile kont założyło się w systemie i ile adresów kont poczty elektronicznej do tych kont przyporządkowała osoba je zakładająca. Taki sposób funkcjonowania systemu powoduje jednak, że w systemie mogą znajdować się wnioski niepotwierdzone i co za tym idzie nieużywane konta osób, które z nich nie korzystają. Dostęp do tych kont maja wyłącznie osoby, które je założyły i mogą samodzielnie je usunąć. Jak pokazuje praktyka tak się nie dzieje. Dlatego przewidziano możliwość likwidacji takich kont. Powyższe nie jest związane z wielokrotnością występowania o profil

				zaufany, ponieważ jest to prawo osób wnioskujących przewidziane ustawą. Procedura wideoidentyfikacji będzie przeprowadzana tylko wtedy, gdy wnioskodawca nie będzie miał profilu zaufanego. W związku z tym, że ustawa przewiduje tylko trzy miesiące ważności tego profilu z mocy prawa, jak najbardziej należy przewidywać, że po wygaśnięciu ważności procedura może zostać powtórzona, chyba że zaistnieją warunki że: - minister przedłuży ważność tymczasowych profili zaufanych potwierdzonych - minister przestanie w ogóle udostępniać usługę.
10.	§ 13 ust. 1 pkt 5	UODO	§ 13 ust. 1 pkt 5 projektu rozporządzenia wskazuje, że niewystarczająca jakość transmisji audiowizualnej albo nagrania tej transmisji, jest przesłanką uniemożliwiającą potwierdzenie profilu zaufanego. Ponieważ możliwość potwierdzania poprzez transmisję audiowizualną dotyczy wyłącznie tymczasowego profilu zaufanego, nie zaś „zwykłego" profilu zaufanego, przepis powinien zostać przeniesiony do innego paragrafu, bądź sformułowany w taki sposób aby nie budził w tym względzie wątpliwości.	**<u>Uwaga wyjaśniona</u>** Przepis wskazuje na transmisję audiowizualną albo nagrania tej transmisji, o których mowa w § 6, zatem nie ma wątpliwości jakiej sytuacji to dotyczy.
11.	§ 15 ust. 3	UODO	§ 15 ust. 3 projektu rozporządzenia stanowi, że w toku czynności, o których mowa w ust. 2, dopuszcza się możliwość żądania od posiadacza profilu zaufanego dokonania czynności lub przekazania danych, które pozwolą na zaprzeczenie istnienia nieprawidłowości. Przepis jest nieprecyzyjny, nie wiadomo jakich czynności oraz danych można żądać od posiadacza profilu zaufanego. Przedmiotowa kwestia powinna zostać doprecyzowana (przynajmmniej na poziomie uzasadnienia do projektu rozporządzenia). Unormowania w tym kształcie naruszają zasadę zgodności z prawem,	**<u>Uwaga wyjaśniona</u>** Przepis celowo nie wskazuje o jakie czynności i dane może chodzić, aby wyjaśnić nieprawidłowości, ponieważ katalog potencjalnych nieprawidłowości, o których mowa w § 15 ust. 1 jest otwarty. Przykładowo zdarza się, że osoba potwierdzająca

			rzetelności i przejrzystości (art. 5 ust. 1 lit a RODO) oraz minimalizacji danych (art. 5 ust. 1 lit c RODO).	profil zaufany za pomocą bankowości elektronicznej wprowadziła niepoprawny adres poczty elektronicznej, który okazał się być nie jej adresem tylko kogoś innego. W takim przypadku u innej osoby (która też może mieć profil zaufany) pojawia się komunikat o potwierdzeniu profilu zaufanego. Zaniepokojona osoba, która otrzymała komunikat nieprzeznaczony dla niej w wyniku pomyłki innej osoby sygnalizuje to (do centrum pomocy użytkowników lub do IOD). Na podstawie przepisów §15 ust 2 i 3 minister może sprawdzić, czy faktycznie taka nieprawidłowość ma miejsce i wezwać osobę, która zrobiła błąd do dokonania czynności polegającej na podaniu poprawnego adresu.
12.	§ 18 ust. 1	UODO	Zgodnie § 18 ust. 1 projektu rozporządzenia na punktach potwierdzających nie ciąży obowiązek przechowywania i archiwizowania dokumentacji w postaci elektronicznej, wytworzonej w ramach procedury potwierdzania, przedłużania i unieważniania profilu zaufanego. Wyjaśnienia wymaga czy w związku z powyższym dokumenty te będą niezwłocznie usuwane z systemów teleinformatycznych tych podmiotów po zakończeniu czynności przetwarzania związanych z potwierdzaniem, przedłużaniem i unieważniania profilu zaufanego a przechowywane będą wyłączenie przez Ministra Cyfryzacji (§ 18 ust. 2). Jest to konieczne dla zachowania zgodności z zasadą ograniczenia przechowywania (art. 5 ust. 1 lit e RODO).	**<u>Uwaga wyjaśniona</u>** Wnioskowanie potwierdzanie, przedłużania i unieważnianie profilu zaufanego odbywa się specjalnie przeznaczonym do tego celu systemie teleinformatycznym utrzymywanym przez Ministra Cyfryzacji, przy użyciu którego zapewniana jest obsługa publicznego systemu identyfikacji elektronicznej, w ramach którego wydawany jest profil zaufany, a nie w systemie teleinformatycznym jakiegokolwiek innego podmiotu.
13.	§ 18 ust. 2	UODO	§ 18 ust. 2 projektu rozporządzenia powinien określać warunki	**<u>Uwaga wyjaśniona</u>**

			bezpieczeństwa przechowywania dokumentów elektronicznych przez Ministra Cyfryzacji w sposób analogiczny jak jest to uregulowane w stosunku do dokumentacji papierowej przetwarzanej przez punkty potwierdzające (§ 18 ust. 1). Rodzi się również pytanie czy Minister Cyfryzacji w ramach procedur związanych z profilem zaufanym będzie wytwarzał dokumenty papierowe. Jeżeli by tak było, to projektowane rozporządzenie również powinno regulować tę kwestię. Jest to konieczne z punktu widzenia zasady integralności i poufności (art. 5 ust. 1 lit. f RODO). W treści projektu rozporządzenia nie jest również wskazane jak i kiedy będą przeprowadzane procesy niszczenia dokumentów w wersji elektronicznej, które zgodnie z § 18 ust. 2 ma przetwarzać Minister, oraz które przejmie na postawie § 18 ust. 4. Nie wiadomo również, jak ma wyglądać proces przechowywania (przetwarzania dokumentów z danymi osobowymi), których okres ustalono na 6 lat, w chwili gdy Minister wyda decyzję o usunięciu profilu zaufanego, zgodnie z § 23 ust. 1 projektu rozporządzenia. W ekstremalnym przypadku, może zajść sytuacja gdy podmiot niepubliczny będzie w posiadaniu danych osobowych do nieistniejącego profilu zaufanego, który został usunięty z systemu decyzją ministra. Zjawisko takie może być nagminne w sytuacji opisanej w § 18 ust. 4 projektu rozporządzenia, ze względu na bezwład organizacyjny rozproszonych zbiorów danych osobowych, w zasobach do których minister nie będzie miał bezpośredniego dostępu, a które będą zmieniały administratorów. Takie sytuacje będą natomiast oznaczać przetwarzanie danych osobowych niezgodnie w zasadami dotyczącymi ich przetwarzania wynikającymi z RODO.	Wskazany przepis tak właśnie reguluje przedmiotową kwestię, to jest w sposób analogiczny, określa te warunki: *„2. Dokumenty w postaci elektronicznej w zakresie potwierdzania, przedłużania i unieważniania profilu zaufanego, z zachowaniem warunków określonych w ust. 1, przechowuje oraz archiwizuje minister.”* Minister Cyfryzacji w ramach procedur związanych z profilem zaufanym (gdy sam potwierdza profil zaufany w punkcie potwierdzającym) wytwarza dokumenty papierowe i projektowane rozporządzenie reguluje tę kwestię (§ 18 ust. 1). Dla brakowania (niszczenia) dokumentów elektronicznych w zakresie potwierdzania, przedłużania i unieważniania profilu zaufanego zastosowanie mają przepisy rozporządzenia Ministra Spraw Wewnętrznych i Administracji z dnia 30 października 2006 r. w sprawie szczegółowego sposobu postępowania z dokumentami elektronicznymi (Dz.U. z 2006 r. Nr 206, poz. 1518) - zob. §8 ust. 2 *„Brakowanie dokumentacji niearchiwalnej polega na ocenie jej przydatności do celów praktycznych, wydzieleniu dokumentacji nieprzydatnej i jej zniszczeniu w sposób właściwy dla danej technologii zapisu”*.

14.	§ 18 ust. 3	UODO	W § 18 ust. 3 projektu rozporządzenia wskazano czas przechowywania dokumentów w wersji papierowej przez podmiot niepubliczny, natomiast nie występuje jasno wyartykułowane wskazanie jak ma przebiegać proces niszczenia tejże dokumentacji po upływie czasu obowiązkowego przechowywania.	**<u>Uwaga wyjaśniona</u>** Przepis nie dotyczy czasu przechowywania dokumentów w wersji papierowej przez podmiot niepubliczny tylko przez punkt potwierdzający. Podmioty publiczne, które pełnią rolę punktów potwierdzających postępują z dokumentacją w sposób określony przepisami wydanymi na postawie ustawy z dnia 14 lipca 1983 r. *o narodowym zasobie archiwalnym i archiwach* a podmioty niepubliczne w oparciu o instrukcję określającą zasady i tryb postępowania z dokumentacją związaną z potwierdzaniem, przedłużaniem ważności i unieważnianiem profilu zaufanego której kopię przedkładają ministrowi (§ 17 ust. 3 projektu)
15.	§ 20 ust. 4 lit. a	UODO	§ 20 ust. 4 lit. a projektu rozporządzenia zakłada m. in. potwierdzanie tożsamości osoby, której udostępniono środki identyfikacji elektronicznej stosowane do uwierzytelniania w systemie teleinformatycznym podmiotu niepublicznego w trakcie nagrywanej w czasie rzeczywistym transmisji audiowizualnej dokumentu tożsamości. Takie rozwiązanie nie ma umocowania w przepisach ustawy z dnia 17 lutego 2005 r. o informatyzacji działalności podmiotów realizujących zadania publiczne (Dz. U. z 2020 r. poz. 346, z późn. zm.) i tym samym powinno zostać usunięte z projektu rozporządzenia.	**<u>Uwaga wyjaśniona</u>** Zgodnie z art. 20c ust. 1 pkt 3 ustawy, profil zaufany może być potwierdzony samodzielnie przez wnioskodawcę przy użyciu środka identyfikacji elektronicznej, wydanego przez bank krajowy lub innego przedsiębiorcę, spełniającego warunki, o których mowa w art. 20d pkt 1 tej ustawy (czyli upoważnienia do wydania niniejszego projektowanego rozporządzanie). W kwestionowanej jednostce redakcyjnej Minister Cyfryzacji nie nakłada żadnych obowiązków na obywateli, banki czy

				przedsiębiorców. W tym przepisie określone są wymogi dla ww. środków identyfikacji elektronicznej, które będą mogły być użyte przez obywatela do samodzielnego potwierdzenia profilu zaufanego. Upoważnieniem dla określenia powyższego jest art. 20d pkt 1 w związku z art. 20c ust. 1 pkt 3 ustawy.
16.	§ 21 ust. 2	UODO	W § 21 ust. 2 projektu rozporządzenia wskazano czas przechowywania przed podmiot niepubliczny nagrania audiowizualnego z procesu potwierdzenia profilu zaufanego. Nie wskazano procesu, w jaki sposób ma być przeprowadzone niszczenie tak zarejestrowanych danych, które zawierają zarówno wizerunek osoby wnioskującej, jak również dane tej osoby znajdujące się na dokumencie tożsamości, który osoba ma okazać osobie weryfikującej tożsamość wnioskodawcy.	**<u>Uwaga wyjaśniona</u>** Już obecnie banki weryfikują zdalnie tożsamość w taki sposób przy wydawaniu środków identyfikacji stosując się do wytycznych UKNF, o czym mowa w uzasadnieniu. Kwestie dotyczące procedury ustalania tożsamości (w tym w drodze wideoweryfikacji) na potrzeby wydania środków identyfikacji elektronicznej przez „bank lub innego przedsiębiorcę" regulowane są przez odrębne przepisy prawa na podstawie których funkcjonują te podmioty. Natomiast w projektowanym rozporządzeniu konieczne jest uregulowanie jakie warunki muszą spełniać ww. środki identyfikacji elektronicznej aby mogły być wykorzystane do potwierdzenia profilu zaufanego. Jeżeli „bank lub inny przedsiębiorca" ustala tożsamość obywateli w drodze wideoidentyfikacji, to uregulowań warunków przeprowadzenia takich procedur

				należy poszukiwać w wyżej wspomnianych przepisach odrębnych. Celem projektowanego rozporządzenia jest bowiem wskazanie na akceptację lub nie takich procedur w kontekście środka identyfikacji elektronicznej, który miałby służyć do potwierdzenia profilu zaufanego. Ponadto, projektowane rozporządzenie nie jest właściwym miejscem do ustalenia sposobu brakowania dokumentacji sporządzanej przez banki.
17.	§ 23 ust. 1	UODO	Zgodnie z § 23 ust. 1 projektu rozporządzenia Minister Cyfryzacji co najmniej raz na dwa lata dokonuje sprawdzenia mającego na celu ustalenie kont nieużywanych celem ich usunięcia. Doprecyzowania wymaga pojęcie „konta nieużywanego", przez jaki czas konto ma być nieużywane aby mogło zostać usunięte, gdyż nie wynika to z przepisów ani projektowanego rozporządzenia ani ustawy o informatyzacji działalności podmiotów realizujących zadania publiczne. Również w kontekście § 23 ust. 4 projektu rozporządzenia, w którym mowa o usunięciu nieużywanego konta w terminie 30 dni od przesłania drugiego powiadomienia, nasuwa się pytanie czy usunięcie tych danych następuje również z kopii zapasowych, a jeżeli nie to po jakim okresie dane są usuwane definitywnie.	**<u>Uwaga wyjaśniona</u>** Zgodnie z definicją pojęcia uregulowaną w § 2 pkt 5 projektu „konto nieużywane - konto profilu zaufanego, które nie było wykorzystywane przez użytkownika profilu zaufanego w okresie dłuższym niż 3 lata;" Kopia zapasowa jest elementem systemu teleinformatycznego i służy do jego odtworzenia po awarii. A to znaczy, że może istnieć przesunięcie w czasie w przypadku danych w kopiach zapasowych i w systemie produkcyjnym Każdy podmiot obsługujący system teleinformatyczny jest zobowiązany do tego, aby zapewnić niezawodność działania systemu zgodnie z wymogami *rozporządzenia Rady Ministrów z dnia 12 kwietnia 2012 r. w sprawie Krajowych Ram Interoperacyjności, minimalnych wymagań dla rejestrów*

				publicznych i wymiany informacji w postaci elektronicznej oraz minimalnych wymagań dla systemów teleinformatycznych (Dz.U. z 2017 r. poz. 2247). Usunięcie danych z kopii zapasowej, nastąpi w takim terminie, w jakim przewidziano dla danego systemu nadpisanie takiej kopii nowymi danymi. Kopie zapasowe co do zasady są odtwarzane tylko w przypadku awarii i nie służą innym celom.
18.	§ 24	UODO	Doprecyzowanie wymaga na czym ma polegać umowa oraz powierzenie, o których mowa w § 24 projektu rozporządzenia. Rodzi się w tym miejscu pytanie jakie relacje mają być w ten sposób budowane z punktu widzenia określenia ról w procesie przetwarzania danych osobowych. Czy powierzenie realizacji zadań oznacza, że punkt potwierdzający albo jednostka podległa lub nadzorowana przez Ministra Cyfryzacji, której powierzono realizację zadań staje się odrębnym administratorem, czy też projektodawca miał na myśli relację powierzenia przetwarzania danych. Jeśli intencją projektodawcy jest aby wykonywanie obowiązków odbywało się w drodze powierzenia w rozumieniu art. 28 RODO, to taki zapis jest niewystarczający z punktu widzenia spełnienia wszystkich warunków dla instrumentu prawnego z art. 28 RODO. Również w kontekście art. 26 RODO (jeśli w ten sposób miałaby powstawać relacja współadministrowania) ten przepis jest niewystarczający. Jako postulat de lege ferenda, wskazuję również, że materia § 24 projektu rozporządzenia powinna zostać przeniesiona na poziom ustawy.	**<u>Uwaga uwzględniona</u>** Przepis został usunięty
19.	Załącznik nr 2	UODO	Załącznik 2 do nr do projektu rozporządzenia określający zakres danych wymagany we wniosku o potwierdzenie tymczasowego profilu zaufanego nie odnosi się do danych osobowych pozyskiwanych za pośrednictwem wideoweryfikacji, takich jak niepowtarzalny numer identyfikacyjny urządzenia, na przykład IMEI, adres MAC czy adres IP. Zgodnie z motywem	**<u>Uwaga wyjaśniona</u>** Załącznik nr 2 dotyczy zakresu danych wymaganych we wniosku o potwierdzenie tymczasowego profilu zaufanego podobnie, jak załącznik nr 1

			30. RODO, przypisane osobom fizycznym identyfikatory internetowe – takie jak adresy IP, identyfikatory plików cookie – generowane przez ich urządzenia, aplikacje, narzędzia i protokoły, czy też inne identyfikatory, generowane na przykład przez etykiety RFID, w połączeniu z innymi informacjami, które pozwalają na identyfikację danej osoby, stanowią dane osobowe. O ile nie jest konieczne wymaganie od osoby samodzielnego podawania tych danych we wniosku, to dla zapewnienia przejrzystości przetwarzania, wnioskodawca powinien mieć świadomość, że dane te są od niego pobierane. Doprecyzowania wymaga również jakie wybrane „czynniki uwierzytelnienia" miał na myśli projektodawca w pkt 1 lit h załącznika nr 2 do projektu rozporządzenia.	dotyczy zakresu danych wymaganego we wniosku o potwierdzenie profilu zaufanego. Oba wnioski składa się przez Internet. Co do zasady w przepisach dotyczących zakresu danych zawartych w jakichkolwiek podaniach i wnioskach nie podaje się informacji których te wnioski nie zawierają. Zgodnie z §11 ust. 4. uwierzytelnienie z wykorzystaniem profilu zaufanego dokonywane jest w sposób zapewniający średni poziom bezpieczeństwa, przy wykorzystaniu co najmniej dwóch czynników uwierzytelnienia należących do co najmniej dwóch różnych kategorii, o których mowa w przepisach wydanych na podstawie art. 8 ust. 3 rozporządzenia 910/2014. Przepisy te to Rozporządzenie wykonawcze 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*.
20.	Dot. Przepisy art. 20ca ustawy o informatyzacji działalności	UODO	Przepisy art. 20ca ustawy o informatyzacji działalności podmiotów realizujących zadania publiczne zostały wprowadzone art. 33 ustawy z dnia 31 marca 2020 r. o zmianie ustawy o szczególnych rozwiązaniach związanych z zapobieganiem, przeciwdziałaniem i zwalczaniem COVID-19, innych chorób zakaźnych oraz wywołanych nimi sytuacji kryzysowych oraz niektórych innych ustaw (Dz. U. z 2020 r. poz. 568) w związku z trwającą epidemią. Mają więc charakter tymczasowy i nie powinny być utrzymywane	**<u>Uwaga wyjaśniona</u>** Przepisy art. 20ca ustawy o informatyzacji działalności podmiotów realizujących zadania nie mają charakteru tymczasowego. Tymczasowy jest profil zaufany wydawany na ich podstawie, jak również tymczasowa

	podmiotów realizujących zadania publiczne zostały wprowadzone art. 33 ustawy z dnia 31 marca 2020 r. o zmianie ustawy o szczególnych rozwiązaniach związanych z zapobieganiem, przeciwdziałaniem i zwalczaniem COVID-19, innych chorób zakaźnych oraz wywołanych nimi sytuacji kryzysowych oraz		dłużej niż jest to niezbędne dla ww. szczególnych celów. Projektodawca powinien więc rozważyć jak długo zamierza utrzymać instytucje tymczasowego profilu zaufanego oraz potwierdzania go w formie transmisji audiowizualnej – gdyż takie rozwiązania, jako zapewniające niższy niż dotychczasowo poziom ochrony danych osobowych powinny być utrzymane wyłącznie tymczasowo. Instytucja wideoidentyfikacji wnioskodawcy, jaką wprowadził art. 20ca ustawy o informatyzacji działalności podmiotów realizujących zadania publiczne może powodować wysokie ryzyko naruszenia praw lub wolności osób fizycznych, w tym nie tylko danych tzw. zwykłych, ale także szczególnych kategorii danych (w tym np. biometrycznych, danych dotyczących zdrowia) czy danych dotyczących krajowego numeru identyfikacyjnego. Korzystanie z technologii, która będzie umożliwiała identyfikację wizerunku, ściśle wiąże się z koniecznością zrealizowania wielu przesłanek, oceną skutków dla ochrony danych oraz ograniczeniem do minimum potencjalnie uzyskiwanych danych. Zgodnie z art. 35 RODO, każdy podmiot, także projektodawca w związku z przyjmowaniem podstawy prawnej przetwarzania danych musi ocenić, czy istnieje ryzyko naruszenia praw i wolności osób w tym poufności, integralności oraz dostępności danych. W sytuacji gdy operacje przetwarzania mogą wiązać się z wysokim ryzykiem naruszenia praw lub wolności osób fizycznych, należy zobowiązać administratora do dokonania oceny skutków dla ochrony danych w celu oszacowania w szczególności źródła, charakteru, specyfiki i powagi tego ryzyka. Wyniki oceny należy uwzględnić przy określaniu odpowiednich środków, które należy zastosować, by wykazać, że przetwarzanie danych osobowych odbywa się zgodnie z RODO. Mając na uwadze istotny poziom ryzyka związanego z wideoweryfikacją tożsamości osoby – instytucja ta powinna zostać analizie w ramach oceny skutków dla ochrony danych, o której mowa w art. 35 RODO. Unormowania ustawy o informatyzacji działalności podmiotów realizujących zadania publiczne powinna określać wymogi technicznoorganizacyjne tej procedury, ustalać jednolite standardy techniczne oraz sposoby zabezpieczenia komunikacji gwarantujące odpowiedni poziom bezpieczeństwa usługi, a także zapewniać odpowiedni	może być usługa online, o której mowa w tym przepisie, gdyż minister może, ale nie musi, udostępniać takiej usługi. Wideoweryfikacja jest to rozwiązanie przyszłościowe, które tylko pozornie jest mniej bezpieczne od potwierdzania tożsamości w trakcie fizycznej obecności w punkcie potwierdzającym. Bezpieczeństwo, o którym mowa powyżej należy rozumieć w ten sposób, że weryfikacja tożsamości osoby fizycznej, której wydaje się środek identyfikacji elektronicznej musi być niezawodna, a dowody tej weryfikacji niepodważalne. Podkreślenia wymaga, że mamy tu do czynienia nie z zagrożeniem naruszenia praw i wolności osoby fizycznej w związku z tym, że podmiot wydający środek identyfikacji elektronicznej weryfikuje tożsamość tej osoby, ale z o wiele większym zagrożeniem dla tej osoby, gdyby tego nie robił. Celem jest zapewnienie bezpiecznego potwierdzenia tożsamości osoby wnioskującej o tymczasowy profil zaufany, co dla tak zwanego średniego poziomu bezpieczeństwa, o którym mowa w załączniku do *Rozporządzenia wykonawczego Komisji (UE) 2015/1502 z dnia 8 września 2015 r. w sprawie ustanowienia minimalnych specyfikacji technicznych i procedur dotyczących*

	niektórych innych ustaw (Dz. U. z 2020 r. poz. 568) w związku z trwającą epidemią.		systemem jej wewnętrznej kontroli. Uzasadnionym jest ponowne zważenie zakresu materii regulowanej projektowanym rozporządzaniem – jako nakładającym prawa i obowiązki na adresatów tych norm, zarówno osoby, których dane dotyczą, jak i podmioty przetwarzające dane osobowe – co do konieczności uregulowania go w przepisach rangi ustawy, a nie aktu wykonawczego. Niezależnie od tego czy projektodawca przeprowadził ocenę skutków dla ochrony danych art. 20ca ustawy o informatyzacji działalności podmiotów realizujących zadania publiczne przed wprowadzeniem tego przepisu do polskiego porządku prawnego – w opinii organu nadzorczego, ocena ta powinna zostać przeprowadzona również ex post, a jej wyniki uwzględnione przy najbliższej nowelizacji tej ustawy	*poziomów zaufania w zakresie środków identyfikacji elektronicznej na podstawie art. 8 ust. 3 rozporządzenia Parlamentu Europejskiego i Rady (UE) nr 910/2014* wymaga podjęcia określonych działań w celu zminimalizowania ryzyka, że tożsamość danej osoby nie jest tożsamością deklarowaną, biorąc pod uwagę np. ryzyko utraty, kradzieży, zawieszenia, unieważnienia bądź upływu terminu ważności dokumentów. Bez podjęcia takich działań każda osoba posiadająca numer PESEL byłaby narażona na kradzież tożsamości, której konsekwencje są daleko większe niż potencjalne zagrożenie przetwarzaniem danych osoby, która złożyła wniosek o tymczasowy profil zaufany przez osobę upoważnioną przez Ministra Cyfryzacji. Mając na uwadze, że mamy do czynienia za zdalnym okazaniem dokumentu tożsamości celem wydania środka identyfikacji elektronicznej zabezpieczenia polegające na zminimalizowaniu ryzyka, że tożsamość danej osoby nie jest tożsamością deklarowaną są uzasadnione i zwiększają ochronę danych, a nie odwrotnie. Gdyby nie możliwość weryfikacji ważności i nr dokumentu tożsamości nie tylko na podstawie jego okazania w trakcie transmisji,

				potencjalne zagrożenie uzyskaniem profilu zaufanego przez oszusta byłoby nieakceptowalne. Należy też nadmienić, że profil zaufany pozwala na dostęp do danych wrażliwych w systemach ZUS i w Internetowym Koncie Pacjenta, dostęp do pełnych danych w rejestrze PESEL, do danych w Rejestrze Dowodów Osobistych do danych CEPiK, td.. Niedochowanie staranności przy wydawaniu profilu zaufanego w tym tymczasowego profilu zaufanego – nawet kosztem udostępnienia osobie potwierdzającej informacji o nr dokumentu tożsamości i jego ważności, a także innych danych znajdujących się w warstwie graficznej tego dokumentu mogłoby mieć znaczące negatywne skutki nie tylko dla osób, których tożsamość zostałaby skradziona ale też dla całego systemu profilu zaufanego i co za tym idzie do usług społeczeństwa informacyjnego. Podsumowując – paradoksalnie jest wprost przeciwnie, im większa pewność weryfikacji tożsamości osoby wnioskującej o profil zaufany tym skuteczniejsza ochrona danych tej osoby. Należy się zgodzić też z tezą, że ocena procesu zdalnego potwierdzania powinna zostać przeprowadzona również *ex post*, a jej wyniki

				uwzględnione przy najbliższej nowelizacji tej ustawy.
21.	Ogólna	ZBP	W związku z rozporządzeniem Ministra Cyfryzacji bank jako podmiot niepubliczny otrzymuje możliwość dopuszczenia do procesu zakładania Profilu Zaufanego Klienta, który zidentyfikował się w procesie wideoweryfikacji. • Czy taka zmiana jest wymagana przez Ministerstwo czy traktowana jako opcja? • Jeśli tak – to jaka jest termin realizacji zmiany narzucony przez rząd? Uzasadnienie: Taka zmiana pociąga modyfikacje w systemach teleinformatycznych banków, w których obecnie dopuszczamy do procesu zakładania Profilu Zaufanego tylko Klientów, którzy co najmniej raz zostali skutecznie zidentyfikowani fizycznie w oddziale banku.	**<u>Uwaga wyjaśniona</u>** Proponowana zmiana stwarza podmiotom mającym zgodę, o której mowa w art. 20c ust. 8 ustawy tylko możliwość i nie narzuca jakiegokolwiek terminu.
22.	Ogólna	ZBP	Zakładanie profilu zaufanego zdalnie na podstawie paszportu nie powinno być dopuszczalne, ponieważ nie ma możliwości zweryfikowania tego dokumentu w RDO. Nie ma również możliwości zweryfikowania prawdziwości innych dokumentów, które mogą wchodzić zakres pojęciowy „dokumentów tożsamości" – podkreślenia wymaga, że projekt rozporządzenia nie zawiera katalogu tych dokumentów. Uzasadnienie: Aby móc zachować należytą staranność przy zakładaniu Profilu Zaufanego w Bankach poprzez zdalne potwierdzanie tożsamości podczas transmisji audiowizualnej, Bank powinien mieć możliwość porównania wizerunku Klienta z wizerunkiem znajdującym się w Rejestrze Dowodów Osobistych. Obecne uprawienia do weryfikacji w RDO, które posiadają Banki, nie obejmują widoczności wizerunków – banki posiadają dostęp do RDO jedynie w trybie ograniczonej teletransmisji danych. Ponadto banki nie posiadają możliwości weryfikacji tożsamości w oparciu o rejestr paszportów, kart pobytu, kart repatrianta. Dodatkowo rekomendujemy dodanie zapisu określającego obowiązek weryfikacji zgodności wizerunku z Rejestrem Dowodów Osobistych w przypadku potwierdzaniu profilu zaufanego w punkcie potwierdzającym.	**<u>Uwaga wyjaśniona</u>** Zdalne potwierdzanie tożsamości na podstawie paszportu zostało dopuszczone ustawą. Rozporządzenie nie może wprowadzać ograniczeń względem przepisów ustawy wskazując katalog dokumentów jednak może ograniczyć możliwość potwierdzania tożsamości w przypadku jakichkolwiek wątpliwości dotyczących tego, czy osoba okazująca dokument jest tą za którą się podaje. Kwestia możliwości porównania wizerunku osoby fizycznej z wizerunkiem znajdującym się w Rejestrze Dowodów Osobistych zarówno w przypadku wnioskowania o środki identyfikacji elektronicznej wydawane przez bank lub innego przedsiębiorcę, jak również w punkcie

				potwierdzającym to odrębne i ważne zagadnienie wymagające rozważenia pod względem równowagi pomiędzy udostępnianiem danych dla wydania środka identyfikacji elektronicznej a ograniczaniem takiego udostępniania ze względu na ochronę danych osobowych. Mając jednak na uwadze nie tylko kwestie prawne, ale też organizacyjno-techniczne ta ważna inicjatywa wymaga szerszej analizy, w szczególności pod kątem ewentualnej konieczności dokonania zmian w przepisach rangi ustawowej, stąd też możliwość jej uwzględnienia wykracza poza przedmiotowy projekt.
23.	Ogólna	ZBP	W projekcie brak jest odniesienia się do kwestii korzystania z podpisu kwalifikowanego zawierającego parametr ograniczający odpowiedzialność wystawcy. Uzasadnienie: Banki zwracają się o potwierdzenie, czy jest to świadoma decyzja Ministerstwa.	**<u>Uwaga wyjaśniona</u>** Kwalifikowany podpis elektroniczny zgodnie z art. 25 ust. 2 rozporządzenia 915/2014 ma skutek prawny równoważny podpisowi własnoręcznemu i nie można parametryzować tego skutku.
24.	Ogólna	ZBP	Brak jest przepisu o odpowiedzialności Skarbu Państwa w przypadku, gdy dojdzie do wydania Profilu Zaufanego, który zostanie skompromitowany, a bank w procesie jego generowania zachował należytą staranność oraz działał w dobrej wierze.Bank bierze udział w wydaniu Profilu Zaufanego, czyli usługi publicznej. W związku z powyższym nie może ponosić odpowiedzialności za jego wykorzystywanie w sytuacji, w której dochował należytej staranności w trakcie procesu jego generowania - w takich sytuacjach odpowiedzialność za skutki posłużenia się skompromitowanym Profilem Zaufanym powinien ponosić Skarb Państwa. Takie mechanizmy	**<u>Uwaga wyjaśniona</u>** Rozporządzenie powinno regulować tylko te kwestie, które są już (przynajmniej ogólnie) unormowane w samej ustawie. Akt wykonawczy do ustawy nie może w sposób samoistny zmieniać ani modyfikować treści norm zawartych w aktach hierarchicznie wyższych. Zmiana albo modyfikacja

			odpowiedzialności są wdrożone w innych obszarach.	taka jest możliwa jedynie wówczas, gdy jest to wyraźnie wyrażone w przepisie upoważniającym. Rozporządzenie może jedynie wypełnić delegację ustawową i nie może być w nim uregulowanych kwestii, które poza delegację ustawową wykraczają – art. 20d nie daje podstaw do postulowanego przez ZBP działania.
25.	§ 4 ust. 3	ZBP	Proponujemy rozszerzenie katalogu możliwości podpisu wniosku o Profil Zaufany o: • kwalifikowany podpis elektroniczny; • narzędzie autoryzacyjne posiadane w Banku będącym Dostawcą Tożsamości dla Środka Identyfikacji elektronicznej (SMS, mobilna autoryzacja, kod karty TAN). Propozycja ma na celu umożliwienie digitalizacji procesu w oddziałach Banku, gdzie wypełnienie wniosku jest w formie elektronicznej, a klient zatwierdza wniosku o PZ narzędziem elektronicznym – kwalifikowanym, jak mSzafir, lub aktualnym bankowym, jak SMS, mobilna autoryzacja, kod z karty TAN.	**<u>Uwaga wyjaśniona</u>** Cel uwagi jest niejasny. Przepis §4 ust. 3 odnosi się do podpisania wydruku wniosku (dokumentu utrwalonego w postaci papierowej). Każdy posiadacz kwalifikowanego podpisu elektronicznego może go użyć do samodzielnego potwierdzenia profilu zaufanego na podstawie art. 20c ust. 1 pkt 2 ustawy i nie jest do tego potrzebna wizyta w oddziale banku. Jeżeli uwaga odnosi się do możliwości, o której mowa w art. 20c ust. 1 pkt 3 ustawy, to stosowne wymagania wskazane są w §20 projektu rozporządzenia i nie zawierają żadnych ograniczeń dotyczących wykorzystania środka identyfikacji elektronicznej wydanego w systemie teleinformatycznym banku krajowego lub innego przedsiębiorcy poza spełnieniem wymogów dla średniego poziomu bezpieczeństwa o którym mowa w rozporządzeniu wykonawczym 2015/1502. W praktyce oznacza to, że

				osoba fizyczna korzystająca bankowości elektronicznej w banku krajowym może użyć środka identyfikacji elektronicznej wydawanego w systemie banku do samodzielnego potwierdzenia profilu zaufanego pod warunkiem, że środek ten: 1) spełnia wymagania dla poziomu średniego, co znaczy, że tożsamość jest odpowiednio zweryfikowana, są wykorzystywane co najmniej dwa czynniki uwierzytelniania, a uwierzytelnianie jest dynamiczne 2) dodatkowo jeżeli potwierdzenie tożsamości było zdalne, to sporządzane jest nagranie. Bank powinien to udokumentować w sposób określony w § 20 ust. 2 .
26.	§ 4 ust. 5 oraz § 6 ust. 8	ZBP	Rozważenia może wymagać rozszerzenie wskazanych przepisów o następujące punkty: pkt 3) kwalifikowanym certyfikatem pieczęci elektronicznej; pkt 4) podpisem osobistym. Z uwagi na wprowadzony przez Rząd RP dowód osobisty z warstwą elektroniczną (tzw. eDowód) oraz posiadane możliwości technologiczne należy rozważyć dodanie wskazanych rozwiązań.	**<u>Uwaga wyjaśniona</u>** Nie można opatrzyć dokumentu elektronicznego kwalifikowanym certyfikatem pieczęci elektronicznej (można opatrzyć kwalifikowaną pieczęcią elektroniczną). Nie może tego jednak uczynić osoba potwierdzająca, ponieważ osoby fizyczne co do zasady posługują się podpisami elektronicznymi, a nie pieczęciami elektronicznymi. Nie przewidziano możliwości wykorzystanie podpisu osobistego we wskazanym celu ponieważ uznano obecne możliwości za wystarczające.

27.	§ 6 ust. 1	ZBP	W § 6 ust. 1. proponujemy obok weryfikacji osoby uprawnionej dodanie narzędzia biometrii behawioralnej rozpoznawania twarzy. Scoring ze wskazanego narzędzia byłby wkładem do podjęcia decyzji osoby upoważnionej do potwierdzania tymczasowego profilu zaufanego	**<u>Uwaga wyjaśniona</u>** Propozycja jest warta rozważenia wobec wielokrotnie podkreślanego, kluczowego w całym procesie wydawania środka identyfikacji elektronicznej procesu weryfikacji tożsamości osoby fizycznej. Takie rozwiązania będą rozważane w ramach oceny funkcjonowania obecnego tymczasowego profilu zaufanego.
28.	§ 6 ust. 4	ZBP	Rozważania wymaga czy porównanie wizualne ma się ograniczyć tylko do stwierdzenia że w RDO jest zdjęcie osoby wnioskującej. Mogą wystąpić sytuacje, w których jakość zdjęcia jest słaba lub jest ono bardzo nieaktualne. Wyjaśnienia wymaga, czy w takich przypadkach wniosek zostanie rozpoznany pozytywnie. Uwaga ma na celu zwiększenie bezpieczeństwa procesu.	**<u>Uwaga uwzględniona</u>** W przypadku potwierdzania tymczasowego profilu zaufanego osoba potwierdzająca nie może zweryfikować niektórych cech dowodu osobistego, których weryfikacja jest możliwa do sprawdzenia tylko w przypadku obecności fizycznej (dotyk, ultrafiolet), jednakże w zamian ma dostęp do wizerunku osoby fizycznej w rejestrze dowodów osobistych oraz sporządzane jest nagranie audiowizualne, które może stanowić ważny dowód w ewentualnej sprawie o podawanie się wnioskodawcy za osobę, którą ten wnioskodawca w rzeczywistości nie jest. Takie nagranie pełni istotną rolę odstraszającą potencjalnych przestępców zamierzających ukraść tożsamość innej osoby.
29.	§ 6 ust. 5	ZBP	Doświadczenia banków wskazują, że warunków do poprawnej weryfikacji powinno być znacznie więcej: dobre łącze komputerowe, kamera o wysokiej	**<u>Uwaga wyjaśniona</u>** Takie szczegółowe wymagania znajdują

			rozdzielczości, tło rozmówcy powinno być statyczne, okazanie dowodu pod różnymi kątami itp. Ponadto wyjaśnienia wymaga, czy osoba upoważniona do potwierdzania tymczasowego profilu zaufanego będzie należycie przeszkolona z weryfikacji drogą zdalną żądanych danych i oceny wiarygodności przedstawionych dowodów osobistych. Dodatkowo proponuje się dodanie następujących treści: 5) zwraca się o okazanie dowodu osobistego lub paszportu w sposób umożliwiający weryfikację znaków zabezpieczających dowód osobisty tj. …… lub paszportu; 6) zwraca się o okazanie dowodu osobistego lub paszportu w sposób umożliwiający weryfikację krawędzi dowodu osobistego – dłuższej i krótszej. Uwaga ma na celu zwiększenie bezpieczeństwa procesu.	się w ciągle uzupełnianej i rozwijanej instrukcji dla osoby potwierdzającej, która jest na bieżąco dostosowywana do wniosków wynikających z gromadzonych doświadczeń. Celowo wymagania te nie są wprost wyliczone w rozporządzeniu, tylko zostały ujęte ogólnie w przepisach dotyczących jakości połączenia i nagrania oraz możliwości zażądania wykonania gestu, który ułatwi wykrycie działania oprogramowania zakłócającego teletransmisję audiowizualną w sposób uniemożliwiający lub utrudniający potwierdzenie tożsamości wnioskodawcy. Gdyby tak nie było, to wprowadzenie dodatkowych zabezpieczeń wynikających z wykrytych prób oszustwa byłoby niemożliwe bez zmiany rozporządzenia.
30.	§ 6 ust. 5 pkt 1	ZBP	Wnioskodawca powinien być poinformowany również jaki jest zakres przetwarzania danych osobowych, biometrycznych i jak długo jest przechowywane nagranie. Uwaga doprecyzowująca.	**<u>Uwaga wyjaśniona</u>** Nie ma takiej potrzeby ponieważ: 1. Wynika to z przepisów prawa, 2. Przy składaniu wniosku wnioskodawca jest o tym informowany za pomocą odpowiedniej klauzuli informacyjnej udostępnianej w ramach usługi online pozwalającej na wniesienie wniosku o potwierdzenie profilu zaufanego”.
31.	§ 6 ust. 5 pkt 3	ZBP	Rozważanie wymaga dodanie w procedurze zdalnej weryfikacji tożsamości obywatela możliwości wykorzystania danych z warstwy elektronicznej e-Dowodu, a nie tylko weryfikacji na podstawie okazania dokumentu	**<u>Uwaga wyjaśniona</u>** Osoba posiadająca dowód osobisty z warstwą elektroniczną w ogóle nie musi

			tożsamości. Z uwagi na wprowadzony przez Rząd RP dowód osobisty z warstwą elektroniczną (tzw. eDowód), należy rozważyć dodanie wskazanych rozwiązań.	wnioskować o profil zaufany, tylko może samodzielne potwierdzić profil zaufany od razu. Zob. https://pz.gov.pl/pz/registerMainPage i dalej e-dowód
32.	§ 6 ust. 6	ZBP	Niejasne jest sformułowanie "wykonanie gestu, który ułatwi wykrycie działania oprogramowania zakłócającego teletransmisję audiowizualną w sposób uniemożliwiający lub utrudniający potwierdzenie tożsamości wnioskodawcy". Prośba o doprecyzowanie.	**Uwaga wyjaśniona** W zamierzeniu projektodawcy stwierdzenie to ma się odnosić do działań osoby potwierdzającej, których celem jest wykrycie potencjalnego użycia oprogramowania, które jedynie symulowałoby w czasie rzeczywistym prezentację osoby fizycznej w takcie transmisji audiowizualnej. Działanie takiego oprogramowania wykluczałoby zarejestrowanie faktycznego wizerunku wnioskodawcy oraz okazywanego dokumentu tożsamości.
33.	§ 6 ust. 9	ZBP	Wątpliwości budzi na czym polegać automatyzm weryfikacji jakości nagrania i czy bezpieczniejszym rozwiązaniem nie byłaby weryfikacja jakości nagrania przez człowieka. Prośba o wyjaśnienie.	**Uwaga wyjaśniona** To tylko możliwość, a nie wymóg. Jeżeli przykładowo będzie możliwa automatyczna weryfikacja nagrania, która pozwoli na weryfikację wizerunku przy wykorzystaniu narzędzia biometrii behawioralnej i danych z warstwy graficznej dowodu osobistego to przeglądanie nagania przez człowieka może nie być konieczne.
34.	§ 6 ust. 10	ZBP	Wideoidentyfikacja ma zastąpić spotkanie „twarzą w twarz” - w związku z tym rozważenia wymaga zasadność zastępowania jej zadawaniem pytań. W przypadku wątpliwości porównywania wizerunku, wnioskodawca powinien być skierowany do punktu potwierdzającego. W związku z tym proponujemy rezygnację z ustępów 10 i 11 w obecnym	**Uwaga wyjaśniona** Zadanie pytań, które jest fakultatywne, nie zastępuje wideoidentyfikacji. Przepis zostanie zmieniony w związku z uwagą PUODO. Proponuje się

			brzmieniu z uwagi na brak skutecznej i jednolitej oceny.W przedstawionym projekcie dokonuje się próby wideoweryfikacji/identyfikacji Wnioskodawcy za pomocą wideorozmowy, gdzie weryfikujący w czasie sesji ma dokonać porównania wizerunku twarzy Wnioskującego ze zdjęciem na dokumencie stwierdzającym tożsamość oraz zweryfikować dokument tożsamości czy jest prawdziwy, co wydaje się często niemożliwe w zależności od jakości połączenia i jest subiektywne. Problematyczna jest możliwość zadania pytań w przypadku wątpliwości odnośnie porównywania wizerunku wnioskodawcy z wizerunkiem z RDO – będzie to tylko i wyłącznie subiektywna decyzja oceniającego. Wizerunek osoby w procesie uwierzytelnienia jest jednym z podstawowych elementów tego procesu i jego podważenie może zachwiać zaufanie do weryfikacji profilu zaufanego.	brzmienie: *„10. W przypadku wątpliwości odnośnie porównania wizerunku wnioskodawcy z wizerunkiem z Rejestru Dowodów Osobistych lub weryfikacji danych zawartych w warstwie graficznej dowodu osobistego albo paszportu wnioskodawcy okazanego przez niego w czasie rzeczywistym za pośrednictwem transmisji audiowizualnej, osoba upoważniona do potwierdzenia tymczasowego profilu zaufanego może zweryfikować tożsamość wnioskodawcy przy wykorzystaniu dodatkowych danych dotyczących wnioskodawcy, podanych przez niego w trakcie trwania procesu weryfikacji, których zgodność może zostać zweryfikowana z danymi zgromadzonymi w rejestrach publicznych lub w systemach teleinformatycznych prowadzonych przez ministra, w szczególności:* *1) danych zawartych w warstwie graficznej dowodu osobistego lub paszportu widzianych w czasie rzeczywistym podczas transmisji audiowizualnej,* *2) danych podanych przez wnioskodawcę w przypadku gdy chodzi o dane znajdujące się w rejestrze publicznym lub systemie teleinformatycznym prowadzonym*

				przez ministra. *11. W przypadku, o którym mowa w ust. 10, osoba upoważniona do potwierdzenia tymczasowego profilu zaufanego dokonuje potwierdzenia, po zweryfikowaniu dodatkowych danych z właściwym rejestrem publicznym lub systemem teleinformatycznym i odnotowaniu tej czynności w systemie, w którym wydawany jest profil zaufany."*
35.	§ 7	ZBP	Prośba o wskazanie planowanego terminu wydania wytycznych dostosowujących proces do potrzeb osób mających szczególne potrzeby, takie jak niemożność zrozumiałego mówienia czy głuchota.	**<u>Uwaga wyjaśniona</u>** Przepis ma celowo charakter deklaratywny, a nie normatywny, ponieważ możliwość potwierdzania tymczasowego profilu zaufanego dla osób z niepełnosprawnościami uniemożliwiającymi im przykładowo przeprowadzenie rozmowy podczas transmisji audiowizualnej może być zastąpione w różny sposób wskazany w ustawie wskazanymi w ustawie z dnia z dnia 19 sierpnia 2011 r o języku migowym i innych środkach komunikowania się. Zwykle w przypadku wykorzystywania aplikacji przeznaczonych do połączeń konferencyjnych możliwe jest porozumiewanie się z częścią osób niemówiących na tzw. czacie, ale niektórzy mogą wymagać pomocy tłumacza. Te kwestie z uwagi na pilność potrzeby oddania do użytku takiej

				usługi nie zostały jeszcze rozwiązane w taki sposób, aby zapewnić osobom niepełnosprawnym bezpieczną obsługę, a z drugiej strony nie można wykluczać osób niepełnosprawnych. Bez proponowanego przepisu
36.	§ 11 ust. 4 i w konsekwencji § 11 ust. 7 oraz § 16 ust. 3 (lista dopuszczalnych czynników uwierzytelnienia)	ZBP	Rozważania może wymagać dodanie czynnika z kategorii „kim jestem" – biometrii. Warto dodać do Rozporządzenia możliwość wykorzystania również czynnika z kategorii „kim jestem" – czyli rozwiązań opartych na biometrii.	**<u>Uwaga wyjaśniona</u>** Przepisy § 11 nie wykluczają możliwości stosowania czynnika uwierzytelniania na podstawie cech przyrodzonych. Wymagają co najmniej dwóch czynników, ale nie wykluczają trzeciego.
37.	§ 11 ust. 5	ZBP	Ryzykowne jest używanie adresu email jako drugiego faktora. Nie jest on niezależny od identyfikatora i hasła i może być łatwo skompromitowany (podsłuchiwanie komunikatów na komputerze obywatela). Uwaga ma na celu podniesienie bezpieczeństwa procesu.	**<u>Uwaga wyjaśniona</u>** Przepis nie ustanawia adresu email jako czynnika uwierzytelniania (jeżeli tak należy rozumieć „drugi faktor"). Adres email może być podany podczas logowanie zamiast identyfikatora (loginu). Niezależnie od tego czy podany zostanie identyfikator, czy adres e-mail, wymaganym jest podanie hasła, które stanowi czynnik uwierzytelniania oparty na wiedzy.
38.	§ 12 ust. 2 oraz ust. 3	ZBP	Wątpliwości budzi brak możliwości przedłużania profilu zaufanego przez systemy bankowości elektronicznej. Wyjaśnienia wymaga, czy jest to celowe zamierzenie Ministerstwa.	**<u>Uwaga wyjaśniona</u>** Zgodnie z art. 20c ust 1a ustawy „Przedłużenie ważności profilu zaufanego może nastąpić w sposób, o którym mowa w ust. 1 pkt 1, 2 i 4, albo

				przy wykorzystaniu profilu zaufanego.”, to jest: - w punkcie potwierdzającym, - samodzielnie przy wykorzystaniu kwalifikowanego podpisu elektronicznego, - samodzielnie przy wykorzystaniu profilu osobistego. - samodzielnie przy wykorzystaniu profilu zaufanego. Powyższe znaczy, że osoba posiadająca ważny profil zaufany może go przedłużyć wykorzystując czynniki uwierzytelniania w systemie bankowości elektronicznej, jeżeli te są przez nią wykorzystywane. Kluczowe w tych przepisach jest to, że to posiadacz profilu zaufanego decyduje w jaki sposób go przedłuży.
39.	§ 14 ust. 2	ZBP	Czy automatyczne tworzenie Profilu Zaufanego następuje w ramach autoryzacji zmian e-mail/nr telefonu danych w Profilu Zaufanym? Prośba o wyjaśnienie.	**Uwaga wyjaśniona** System zachowuje się w taki sposób, że w przypadku takiej zmiany technicznie tworzony jest nowy profil zaufany z nowymi danymi powiązany z tym samym kontem profilu zaufanego. Dla tego nowego profilu zaufanego od nowa liczy się termin jego ważności.
40.	§ 15 ust. 1	ZBP	Wyjaśnienia wymaga, kto jest odpowiedzialny za wykrywanie i monitorowanie nieprawidłowości po wydaniu Profilu. W szczególności dotyczy to tymczasowego Profilu Zaufanego. Profile przyznane w trybie wideoweryfikacji powinny podlegać ścisłemu monitorowaniu ich aktywności i przeciwdziałaniu potencjalnym fraudom. Rozporządzenie nie wskazuje jednak, do jakiego podmiotu należało będzie monitorowanie wykorzystywania PZ.	**Uwaga wyjaśniona** Zgodnie z art. 20aa ustawy minister właściwy do spraw informatyzacji odpowiada za funkcjonowanie systemu teleinformatycznego, w którym wydawany jest profil zaufany. Wszelkie profile zaufane (nie tylko

				potwierdzone w trybie wideoweryfikacji) powinny podlegać ścisłemu monitorowaniu ich aktywności i przeciwdziałaniu potencjalnym fraudom. Prowadzone są bieżące analizy systemu pod tym kątem jak również przygotowywane rozwiązania wzmacniające możliwości ochrony użytkowników profilu zaufanego potencjalnie zagrożonych „przejęciem" profili zaufanego na przykład przez osobę dysponującą kontem bankowym. założonym na cudze dane osobowe, co stanowiłoby istotne zagrożenie dla wiarygodności potwierdzanych profili zaufanych.
41.	§ 18 ust. 3	ZBP	Proponujemy dodanie na końcu zdania „licząc od końca roku, w którym wcześniej wymienione zdarzenie miało miejsce". Doprecyzowanie terminu – brak wskazania momentu, od którego należy liczyć termin 6 lat.	**<u>Uwaga wyjaśniona</u>** Zasady obliczania czasu przechowywania dokumentacji wynikają z przepisów Rozporządzenia Ministra Spraw Wewnętrznych i Administracji z dnia 30 października 2006 r. *w sprawie szczegółowego sposobu postępowania z dokumentami elektronicznymi* (Dz.U. z 2006 r. Nr 206, poz. 1518)
42.	§ 21 ust.2	ZBP	Należałoby wskazać od jakiego momentu należy liczyć termin 6 lat. Ponadto zaproponowany termin powinien podlegać ocenie w kontekście przepisów RODO. Doprecyzowanie terminu.	**<u>Uwaga wyjaśniona</u>** Zaproponowany termin jest taki sam jak dla nagrań przechowywanych przez ministra przy potwierdzaniu tymczasowego profilu zaufanego. Celem jest dostosowanie okresu przechowywania nagrania do terminu

				przedawnienia, o którym mowa w art. 118 Kodeksu cywilnego i jednocześnie wzięcie pod uwagę zasady planowania przepisów w taki sposób aby nie przechowywać danych osobowych (w tym przypadku wizerunku) dłużej niż to jest konieczne. Proponowany okres zapewnia równowagę pomiędzy potrzebą zapewnienia podstawy dla bezpiecznej interakcji elektronicznej z wykorzystaniem profilu zaufanego a zasadami ochrony danych osobowych. Sposób liczenia okresu przetwarzania przez banki informacji stanowiących tajemnicę bankową, o których mowa w art. 105a ust. 5 ustawy z dnia 29 sierpnia 1997 r. - Prawo bankowe (Dz.U. z 2019 r. poz. 2357) nie został w tej ustawie ani w rozporządzeniu wydanym na podstawie art. 105a ust. 7 tej ustawy mimo, że w przepisach tych ustalono okresy przechowywania danych.
43.	§ 23 ust. 2	ZBP	Proponujemy, aby dodać również powiadomienie przy użyciu wiadomości SMS.	**<u>Uwaga wyjaśniona</u>** Celowo nie jest zamierzone powiadamianie smsem, ponieważ chodzi o konta porzucone, a celem jest nie tylko zwolnienie zasobów systemu, ale też zakończenie przetwarzania danych osobowych, które znajdują się w systemie, ale nie ma powodu dalszego ich przechowywania.
44.	§6 ust. 10	Konfederacja	§6 ust. 10 proponujemy dodać pkt. 3) o treści: „3) z danymi posiadanymi	**<u>Uwaga wyjaśniona</u>**

		Lewiatan	przez bank krajowy, w którym wnioskodawca posiada rachunek płatniczy, udostępnionymi za pośrednictwem usługi polecenia przelewu lub usługi dostępu do informacji o rachunku, o których mowa w art. 3 ust. 1 pkt 2 lit. c) i pkt 8) ustawy z dnia 19 sierpnia 2011 r. o usługach płatniczych.”	Nieuzasadnionym jest wprowadzenie postulowanych zmian, ponieważ zgodnie z art. 20c ust 8, Minister właściwy do spraw informatyzacji, na wniosek banku krajowego lub innego przedsiębiorcy, udziela zgody na nieodpłatne wykorzystywanie środków identyfikacji elektronicznej stosowanych do uwierzytelniania w systemie teleinformatycznym banku krajowego lub innego przedsiębiorcy do potwierdzania profilu zaufanego w sposób, o którym mowa w ust. 1 pkt 3, oraz do uwierzytelnień i autoryzacji związanych z jego wykorzystaniem po spełnieniu przez bank krajowy lub innego przedsiębiorcę warunków, o których mowa w przepisach wydanych na podstawie art. 20d pkt 1.
45.	§ 11 po ust. 7	Konfederacja Lewiatan	W § 11 po ust. 7 proponujemy dodanie ust. 8 o treści jak niżej, a kolejne ustępy tego § powinny otrzymać zaktualizowaną numerację. „8. Profil zaufany, w tym tymczasowy profil zaufany może być wykorzystywany przez posiadacza profilu zaufanego w stosunkach z jednostkami administracji publicznej lub podmiotami prywatnymi.”	**<u>Uwaga wyjaśniona</u>** Propozycja wykracza poza zakres upoważnienia ustawowego.
46.	§ 13 ust. 1	Konfederacja Lewiatan	W § 13 ust. 1 proponujemy dodać pkt 10 o treści: „10) wątpliwości co do autentyczności dokumentu tożsamości okazywanego przez wnioskodawcę w trakcie transmisji audiowizualnej, o której mowa w § 6.”	**<u>Uwaga wyjaśniona</u>** Propozycja mieści się w zakresie przepisu § 13 ust. 1 pkt 1
47.	§11 ust. 4-5	PIIT	Izba rekomenduje uzupełnienie §11 ust. 4-5 Projektu o dodatkowe czynniki uwierzytelniania, które odpowiadają zawartym w standardzie Mobile Connect mechanizmom uwierzytelnienia dwuskładnikowego. W standardzie Mobile Connect pierwszym składnikiem uwierzytelniania (czynnikiem uwierzytelniania) jest wiedza o numerze telefonu	**<u>Uwaga częściowo uwzględniona</u>** Przepis § 11 ust. 5 otrzyma brzmienie: *„5. Zamiast identyfikatora użytkownika, o którym mowa w ust. 4 pkt 1 lit. a, użytkownik może używać adresu poczty*

			komórkowego oraz o nadanym przez użytkownika kodzie PIN (czynnik uwierzytelniania - „coś, co wiem”). Drugim ze składników (czynników) uwierzytelniania w standardzie Mobile Connect jest karta SIM, do której przypisany jest pojedynczy numer telefonu komórkowego oraz kod PIN nadany przez użytkownika Dostęp do konta Profilu Zaufanego nie będzie możliwy, jeżeli użytkownik: • nie posługuje się telefonem komórkowym z konkretną kartą SIM, powiązaną z numerem telefonu wykorzystywanym w koncie Profilu Zaufanego. • Nie posługuje się numerem PIN, który nadał i tylko on zna. Karta SIM jest zatem „ustaloną uprzednio rzeczą”, którą użytkownik musi posiadać w czasie oraz w celu dostępu do konta Profilu Zaufanego lub autoryzacji usługi online (czynnik uwierzytelniania - „coś, co mam”). Rekomendowane poniżej uzupełnienia w Projekcie (tekst pogrubiony) zapewnią współpracę konta Profilu Zaufanego ze standardem Mobile Connect w ramach dostępu do konta oraz autoryzacji usług online. Dotyczą one bowiem włączenia do Projektu dodatkowych czynników uwierzytelniania. Propozycja zmian w Projekcie: „§11 ust. 4. Uwierzytelnienie z wykorzystaniem profilu zaufanego dokonywane jest w sposób zapewniający średni poziom bezpieczeństwa, przy wykorzystaniu co najmniej dwóch czynników uwierzytelnienia, należących do co najmniej dwóch rożnych kategorii, o których mowa w przepisach wydanych na podstawie art. 8 ust. 3 rozporządzenia 910/2014, przy czym: 1) jeden czynnik stanowi: a) identyfikator użytkownika i hasło do konta profilu zaufanego albo b) inny czynnik uwierzytelniania wymagający od osoby podlegającej uwierzytelnieniu określonej, znanej tylko tej osobie wiedzy albo, c) dane posiadacza profilu zaufanego zweryfikowane za pomocą kwalifikowanego certyfikatu podpisu elektronicznego; 2) drugi czynnik stanowi: a) hasło jednorazowe przesyłane na wskazany przez użytkownika numer telefonu komórkowego albo b) inny czynnik uwierzytelniania wymagający	*elektronicznej lub numeru telefonu komórkowego, pod warunkiem, że w systemie, w którym wydawany jest profil zaufany z tym adresem poczty lub tym numerem telefonu komórkowego powiązany jest tylko jeden identyfikator.”* Pozostałe proponowane zmiany nie są potrzebne, gdyż także bez nich możliwe jest wykorzystanie technologii MobileConnect.

			od posiadacza profilu zaufanego wykazania się posiadaniem ustalonej uprzednio rzeczy, w szczególności karty SIM, lub urządzenia niezbędnego dla wykorzystania tego czynnika. 5. Zamiast identyfikatora użytkownika, o którym mowa w ust. 4 pkt 1 lit. a, użytkownik może używać adresu poczty elektronicznej lub numeru telefonu komórkowego, pod warunkiem, że w systemie, w którym wydawany jest profil zaufany z tym adresem poczty lub numerem telefonu komórkowego powiązany jest tylko jeden identyfikator. W przypadku korzystania z numeru telefonu komórkowego, zamiast identyfikatora użytkownika użytkownik nadaje temu numerowi telefonu komórkowego czterocyfrowy kod PIN, spełniający funkcję hasła".	
48.	§11	PIIT	Konsekwencją uzupełnienia §11 Projektu o dodatkowe czynniki uwierzytelniania jest wprowadzenie na grunt Projektu pojęcia karty SIM. Choć jest to termin powszechnie znany i używany, to Izba uznaje za adekwatne zdefiniowanie pojęcia „karty SIM" w ramach Projektu, w celu usunięcia wątpliwości dotyczących natury czynnika uwierzytelniania, o którym mowa w §11 ust. 4 pkt 2 lit. b Projektu. Propozycja zmian w Projekcie: „karta SIM - karta czipowa, powiązana z pojedynczym numerem telefonu komórkowego wykorzystywanym w koncie profilu zaufanego zamiast identyfikatora użytkownika"	**<u>Uwaga wyjaśniona</u>** Nieuzasadnionym jest używanie tego pojęcia w rozporządzeniu
49.	Ogólna	PIIT	W świetle rozmów prowadzonych przez Ministra Cyfryzacji z Izbą w odniesieniu do potencjalnego uzupełnienia konta Profilu Zaufanego o funkcjonalności Mobile Connect, PIIT rekomenduje także uzupełnienie przepisów prawa o podstawę do udostępnienia dostawcom Mobile Connect danych osobowych zawartych w koncie Profilu Zaufanego. Takie udostępnienie miałoby miejsce wyłącznie w przypadku wyrażenia przez użytkownika zamiaru korzystania ze standardu Mobile Connect w ramach Profilu Zaufanego oraz wyłącznie na potrzeby uruchomienia standardu dla danego użytkownika. Stworzenie podstawy prawnej do udostępnienia danych osobowych użytkownika wobec dostawcy standardu Mobile Connect pozwoli na łatwiejsze i szybsze powiązanie konta Profilu Zaufanego ze standardem	**<u>Uwaga wyjaśniona</u>** Propozycja wykracza poza zakres upoważnienia ustawowego.

			Mobile Connect (tj. bez potrzeby zbierania dodatkowej zgody użytkownika w procesie powiązania konta Profilu Zaufanego z Mobile Connect), co pozytywnie wpłynie na: zwiększenie bezpieczeństwa; • uniknięcie potencjalnych błędów przy wprowadzaniu danych do formularza; • polepszenie doświadczeń użytkownika (ang. User experience); • zapewnienie spójności i unikatowości danych w obu systemach: Profilu Zaufanym i Mobile Connect. Izba rekomenduje, aby przedmiotowe udostępnienie objęło następujące dane: imię i nazwisko, numer telefonu komórkowego, adres poczty elektronicznej oraz numer PESEL.	