| **Lp.** | **Podmiot wnoszący uwagę** | **Jednostka redakcyjna, do której wnoszona jest uwaga** | **Treść uwagi** | **Propozycja brzmienia przepisu** |
| --- | --- | --- | --- | --- |
| **A545 – wnoszenie pism za pośrednictwem PI** | | | | |
| 1. | RCL | § 4 ust. 6, załącznik nr 1, załącznik nr 3 | Po dodatkowej analizie projektu poddaje się pod rozwagę odstąpienie od wskazywania w projekcie konkretnych formatów plików obsługiwanych przez portal i zastąpienie takiego wyliczenia tych formatów opisem cech funkcjonalnych dokumentu elektronicznego, jaki może być przyjmowany i wysyłany w portalu. Powyższe regulacje projektu mogą bowiem budzić wątpliwości w kontekście zasady równego traktowania różnych technologii informatycznych przez władze publiczne (zasada neutralności technologicznej).  Ponadto należy wskazać, że wśród formatów dokumentów elektronicznych wymieniono także standard podpisu elektronicznego PAdES, który nie stanowi formatu dokumentu, lecz sposób jego podpisania. | **Uwaga uwzględniona częściowo**.  Zrezygnowano z wymienienia w § 4 ust. 6 standard podpisu elektronicznego PAdES.  **W pozostałym zakresie uwaga nie uwzględniona**.  Ze względów bezpieczeństwa konieczne jest wskazanie w projekcie konkretnych formatów plików obsługiwanych przez portal informacyjny. Istotnie nie przyjęliśmy wszystkich formatów z KRI (nie ma np. zip).  ZIP jest uznawany za niebezpieczny, ponieważ stanowi kontener, a nie „przezroczysty” dokument. Po pierwsze, ukrywa rzeczywistą zawartość – do momentu rozpakowania nie da się jednoznacznie stwierdzić, jakie pliki się w nim znajdują (formaty, liczba plików, ich nazwy). Po drugie, archiwa ZIP mogą zawierać złośliwe oprogramowanie albo mechanizmy utrudniające analizę (np. wielopoziomowe archiwa, tzw. zip bomb), co stwarza ryzyko dla systemów teleinformatycznych. Po trzecie, ZIP utrudnia automatyczne przetwarzanie, indeksowanie i kontrolę zgodności z wymogami technicznymi (np. długości nazw plików, formatów, dostępności cyfrowej), dlatego w obrocie urzędowym i sądowym bywa wyłączany lub ograniczany. Również inne sądowe systemy teleinformatyczne ograniczają możliwość wnoszenia plików do konkretnych formatów. Ma to również znaczenie dla możliwości ich odczytania i wykorzystania w sądzie. |
| 2. | MC | § 4 | Proponuje się dodać ust. 5a w brzmieniu:  „5a.Pliki odwzorowywane cyfrowo spełniają minimalne wymogi dostępności cyfrowej określone w załączniku do ustawy z 4 kwietnia 2019 r. o dostępności cyfrowej stron internetowych i aplikacji mobilnych podmiotów publicznych (Dz. U. z 2023 r. poz. 1440).” | **Uwaga nieuwzględniona.**  PI jako system teleinformatyczny spełnia wymogi tej ustawy, ustawa reguluje dostępność cyfrową stron internetowych i aplikacji mobilnych podmiotów publicznych a nie dokumentów składanych przez radców i adwokatów. Proponowany przepis nie wprowadza nowej treści normatywnej. |
| 3. | MC | zał. nr 1 | W załączniku nr 1 zawarte są formaty danych, które są określone w załączniku nr 2 do rozporządzenia Rady Ministrów z dnia 22 maja 2024 r. w sprawie Krajowych Ram Interoperacyjności, minimalnych wymagań dla rejestrów publicznych i wymiany informacji w postaci elektronicznej oraz minimalnych wymagań dla systemów teleinformatycznych (Dz. U. poz. 773), zwanego dalej rozporządzeniem KRI.  W związku z tym, że ustawa z dnia 17 lutego 2005 r. o informatyzacji działalności podmiotów realizujących zadania publiczne (Dz. U. z 2025 r. poz. 1703) w art. 13 ust. 1 wskazuje, że podmiot publiczny używa do realizacji zadań publicznych systemów teleinformatycznych spełniających minimalne wymagania dla systemów teleinformatycznych oraz zapewniających interoperacyjność systemów na zasadach określonych w Krajowych Ramach Interoperacyjności i tym samym określa podstawowe kierunki rozwiązań w zakresie interoperacyjności systemów, minimalnych wymagań dla rejestrów publicznych i dla systemów teleinformatycznych używanych do realizacji zadań publicznych oraz wymiany danych z podmiotami publicznymi, które są uszczegółowione w przepisach rozporządzenia KRI, konieczne jest zapewnienie zgodności tych formatów z formatami określonymi w załączniku nr 2 rozporządzenia KRI. W celu realizacji ww. celu należy usunąć załącznik nr 2 z projektowanego rozporządzenia i jednocześnie w projekcie rozporządzenia dodać przepis, zgodnie z którym formaty danych są zgodne z formatami danych określonymi w przepisach wydanych na podstawie ustawy z dnia 17 lutego 2005 r. o informatyzacji działalności podmiotów realizujących zadania publiczne (czyli rozporządzenia KRI). | **Uwaga nieuwzględniona.**  Ze względów bezpieczeństwa konieczne jest wskazanie w projekcie konkretnych formatów plików obsługiwanych przez portal informacyjny. Istotnie nie przyjęliśmy wszystkich formatów z KRI (nie ma np. zip).  ZIP jest uznawany za niebezpieczny, ponieważ stanowi kontener, a nie „przezroczysty” dokument. Po pierwsze, ukrywa rzeczywistą zawartość – do momentu rozpakowania nie da się jednoznacznie stwierdzić, jakie pliki się w nim znajdują (formaty, liczba plików, ich nazwy). Po drugie, archiwa ZIP mogą zawierać złośliwe oprogramowanie albo mechanizmy utrudniające analizę (np. wielopoziomowe archiwa, tzw. zip bomb), co stwarza ryzyko dla systemów teleinformatycznych. Po trzecie, ZIP utrudnia automatyczne przetwarzanie, indeksowanie i kontrolę zgodności z wymogami technicznymi (np. długości nazw plików, formatów, dostępności cyfrowej), dlatego w obrocie urzędowym i sądowym bywa wyłączany lub ograniczany. Również inne sądowe systemy teleinformatyczne ograniczają możliwość wnoszenia plików do konkretnych formatów. Ma to również znaczenie dla możliwości ich odczytania i wykorzystania w sądzie. Wszystkie przewidziane formaty znajdują się w załączniku nr 2 do rozporządzenia Rady Ministrów z dnia 22 maja 2024 r. w sprawie Krajowych Ram Interoperacyjności, minimalnych wymagań dla rejestrów publicznych i wymiany informacji w postaci elektronicznej oraz minimalnych wymagań dla systemów teleinformatycznych. Pod tym względem projektowane rozporządzenie jest zgodne z tym aktem prawnym. Nie przewiduje innych formatów danych, aniżeli te przewidziane w wymienionym załączniku.  Po drugie Załącznik nr 2 jest konieczny, gdyż brak jednolitych zasad nazewnictwa i struktury plików prowadzi do realnych ryzyk technicznych, takich jak: niemożność zapisania lub odczytania pliku w określonych systemach operacyjnych, błędy podczas automatycznego przetwarzania dokumentów, utrata dokumentów lub ich niewłaściwe przyporządkowanie do spraw,  problemy z długoterminowym przechowywaniem i migracją danych. |
| 4. | MC | zał. nr 3 | Proponuje się uzupełnić załącznik przez dodanie poniższej informacji:  „Pliki odwzorowywane cyfrowo spełniają minimalne wymogi dostępności cyfrowej określone w załączniku do ustawy z 4 kwietnia 2019 r. o dostępności cyfrowej stron internetowych i aplikacji mobilnych podmiotów publicznych (Dz. U. z 2023 r. poz. 1440).”. | **Uwaga nieuwzględniona.**  PI jako system spełnia wymogi tej ustawy, ustawa reguluje dostępność cyfrową stron internetowych i aplikacji mobilnych podmiotów publicznych a nie dokumentów składanych przez radców i adwokatów. |
| **A546 – wzajemne bezpośrednie doręczanie pism między pełnomocnikami przez PI** | | | | |
| 1. | RCL | § 4 ust. 6 oraz załączniki nr 1 i 3 do projektowanego rozporządzenia | Po dodatkowej analizie projektu poddaje się pod rozwagę odstąpienie od wskazywania w projekcie konkretnych formatów plików obsługiwanych przez portal, i zastąpienie takiego wyliczenia tych formatów opisem cech funkcjonalnych dokumentu elektronicznego, jaki może być przyjmowany i wysyłany w portalu. Powyższe regulacje projektu mogą bowiem budzić wątpliwości w kontekście zasady równego traktowania różnych technologii informatycznych przez władze publiczne (zasada neutralności technologicznej).  Ponadto należy wskazać, że wśród formatów dokumentów elektronicznych wymieniono także standard podpisu elektronicznego PAdES, który nie stanowi formatu dokumentu, lecz sposób jego podpisania. | **Uwaga uwzględniona częściowo**.  Zrezygnowano z wymienienia w § 4 ust. 6 standard podpisu elektronicznego PAdES.  **W pozostałym zakresie uwaga nie uwzględniona**.  Ze względów bezpieczeństwa konieczne jest wskazanie w projekcie konkretnych formatów plików obsługiwanych przez portal informacyjny. Istotnie nie przyjęliśmy wszystkich formatów z KRI (nie ma np. zip).  ZIP jest uznawany za niebezpieczny, ponieważ stanowi kontener, a nie „przezroczysty” dokument. Po pierwsze, ukrywa rzeczywistą zawartość – do momentu rozpakowania nie da się jednoznacznie stwierdzić, jakie pliki się w nim znajdują (formaty, liczba plików, ich nazwy). Po drugie, archiwa ZIP mogą zawierać złośliwe oprogramowanie albo mechanizmy utrudniające analizę (np. wielopoziomowe archiwa, tzw. zip bomb), co stwarza ryzyko dla systemów teleinformatycznych. Po trzecie, ZIP utrudnia automatyczne przetwarzanie, indeksowanie i kontrolę zgodności z wymogami technicznymi (np. długości nazw plików, formatów, dostępności cyfrowej), dlatego w obrocie urzędowym i sądowym bywa wyłączany lub ograniczany.  Również inne sądowe systemy teleinformatyczne ograniczają możliwość wnoszenia plików do konkretnych formatów. Ma to również znaczenie dla możliwości ich odczytania i wykorzystania w sądzie. |
| 2. | MC | § 3 | Proponuje się dodać ust. 3 w brzmieniu:  „3. Portal informacyjny spełnia minimalne wymogi dostępności cyfrowej określone w załączniku do ustawy z 4 kwietnia 2019 r. o dostępności cyfrowej stron internetowych i aplikacji mobilnych podmiotów publicznych (Dz. U. z 2023 r. poz. 1440).” | **Uwaga nieuwzględniona.**  PI jako system spełnia wymogi tej ustawy, ustawa reguluje dostępność cyfrową stron internetowych i aplikacji mobilnych podmiotów publicznych a nie dokumentów składanych przez radców i adwokatów. |
| 3. | MC | § 4 | Proponuje się dodać ust. 5a w brzmieniu:  „5a. Pliki odwzorowywane cyfrowo spełniają minimalne wymogi dostępności cyfrowej określone w załączniku do ustawy z 4 kwietnia 2019 r. o dostępności cyfrowej stron internetowych i aplikacji mobilnych podmiotów publicznych (Dz. U. z 2023 r. poz. 1440).” | **Uwaga nieuwzględniona.**  PI jako system spełnia wymogi tej ustawy, ustawa reguluje dostępność cyfrową stron internetowych i aplikacji mobilnych podmiotów publicznych a nie dokumentów składanych przez radców i adwokatów. |
| 4. | MC | zał. nr 1 | W załączniku nr 1 zawarte są formaty danych, które są określone w załączniku nr 2 do rozporządzenia Rady Ministrów z dnia 22 maja 2024 r. w sprawie Krajowych Ram Interoperacyjności, minimalnych wymagań dla rejestrów publicznych i wymiany informacji w postaci elektronicznej oraz minimalnych wymagań dla systemów teleinformatycznych (Dz. U. poz. 773), zwanego dalej rozporządzeniem KRI.  W związku z tym, że ustawa z dnia 17 lutego 2005 r. o informatyzacji działalności podmiotów realizujących zadania publiczne (Dz. U. z 2025 r. poz. 1703) w art. 13 ust. 1 wskazuje, że podmiot publiczny używa do realizacji zadań publicznych systemów teleinformatycznych spełniających minimalne wymagania dla systemów teleinformatycznych oraz zapewniających interoperacyjność systemów na zasadach określonych w Krajowych Ramach Interoperacyjności i tym samym określa podstawowe kierunki rozwiązań w zakresie interoperacyjności systemów, minimalnych wymagań dla rejestrów publicznych i dla systemów teleinformatycznych używanych do realizacji zadań publicznych oraz wymiany danych z podmiotami publicznymi, które są uszczegółowione w przepisach rozporządzenia KRI, konieczne jest zapewnienie zgodności tych formatów z formatami określonymi w załączniku nr 2 rozporządzenia KRI. W celu realizacji ww. celu należy usunąć załącznik nr 2 z projektowanego rozporządzenia i jednocześnie w projekcie rozporządzenia dodać przepis, zgodnie z którym formaty danych są zgodne z formatami danych określonymi w przepisach wydanych na podstawie ustawy z dnia 17 lutego 2005 r. o informatyzacji działalności podmiotów realizujących zadania publiczne (czyli rozporządzenia KRI). | **Uwaga nieuwzględniona.**  Ze względów bezpieczeństwa konieczne jest wskazanie w projekcie konkretnych formatów plików obsługiwanych przez portal informacyjny. Istotnie nie przyjęliśmy wszystkich formatów z KRI (nie ma np. zip).  ZIP jest uznawany za niebezpieczny, ponieważ stanowi kontener, a nie „przezroczysty” dokument. Po pierwsze, ukrywa rzeczywistą zawartość – do momentu rozpakowania nie da się jednoznacznie stwierdzić, jakie pliki się w nim znajdują (formaty, liczba plików, ich nazwy). Po drugie, archiwa ZIP mogą zawierać złośliwe oprogramowanie albo mechanizmy utrudniające analizę (np. wielopoziomowe archiwa, tzw. zip bomb), co stwarza ryzyko dla systemów teleinformatycznych. Po trzecie, ZIP utrudnia automatyczne przetwarzanie, indeksowanie i kontrolę zgodności z wymogami technicznymi (np. długości nazw plików, formatów, dostępności cyfrowej), dlatego w obrocie urzędowym i sądowym bywa wyłączany lub ograniczany. Również inne sądowe systemy teleinformatyczne ograniczają możliwość wnoszenia plików do konkretnych formatów. Ma to również znaczenie dla możliwości ich odczytania i wykorzystania w sądzie.  Po drugie Załącznik nr 2 jest konieczny, gdyż brak jednolitych zasad nazewnictwa i struktury plików prowadzi do realnych ryzyk technicznych, takich jak: niemożność zapisania lub odczytania pliku w określonych systemach operacyjnych, błędy podczas automatycznego przetwarzania dokumentów, utrata dokumentów lub ich niewłaściwe przyporządkowanie do spraw,  problemy z długoterminowym przechowywaniem i migracją danych. |
| 5. | MC | zał. nr 3 | Proponuje się uzupełnić załącznik przez dodanie poniższej informacji:  „Pliki odwzorowywane cyfrowo spełniają minimalne wymogi dostępności cyfrowej określone w załączniku do ustawy z 4 kwietnia 2019 r. o dostępności cyfrowej stron internetowych i aplikacji mobilnych podmiotów publicznych (Dz. U. z 2023 r. poz. 1440).”. | **Uwaga nieuwzględniona.**  PI jako system spełnia wymogi tej ustawy, ustawa reguluje dostępność cyfrową stron internetowych i aplikacji mobilnych podmiotów publicznych a nie dokumentów składanych przez radców i adwokatów. |
| **B936 – doręczanie pism za pośrednictwem PI** | | | | |
| 1. | MC | § 1 pkt 3 | Dla konkretnego celu przetwarzania niezbędne jest przewidzenie zamkniętego, precyzyjnego katalogu danych osobowych, w ramach otwartego katalogu ustawowego. Obywatel powinien wiedzieć, jakie konkretnie dane znajdą się na potwierdzeniu odbioru, a zakres ten nie może być domniemywany ani rozszerzany w drodze interpretacji. Niewłaściwe jest też zbieranie danych osobowych „na zapas”. Argumentacja projektodawcy o „ewentualnej potrzebie przyszłych modyfikacji” czy „uwarunkowaniach technologicznych” stanowi nieproporcjonalność i budzi wątpliwości w zakresie zgodności z zasadami ograniczenia celu, przejrzystości i minimalizacji danych (art. 5 ust. 1 lit. a, b i c RODO). Prawo nie powinno zezwalać na przetwarzanie nieokreślonego zakresu danych tylko dlatego, że mogą one okazać się przydatne w przyszłości. Jeżeli zajdzie potrzeba zmiany zakresu danych ze względu na przyszły, nieokreślony postęp technologiczny lub cyberbezpieczeństwo, wówczas należy odpowiednio i sprawnie znowelizować przepisy rozporządzenia, a nie tworzyć in blanco możliwość pozyskiwania nieokreślonych danych osobowych.  W związku z powyższym wnosi się o usunięcie z § 1 pkt 3 projektu rozporządzenia, zmieniającego § 4 ust. 3 nowelizowanego rozporządzenia, słów: ''w szczególności'' i ew. rozbudowanie tego przepisu o precyzyjne inne dane osobowe.  W przypadku gdy projektodawcy nie chodzi w ramach innych danych o dane osobowe, proponuje się po usunięciu słów w szczególności dodać fragment np: „(...) oraz inne informacje nie stanowiące danych osobowych”. | **Uwaga uwzględniona.**  Projekt został odpowiednio zmodyfikowany poprzez wykreślenie wyrazów: „w szczególności” i dodania fragmentu: „(...) oraz inne informacje nie stanowiące danych osobowych”. |
| **B937 – w sprawie PI** | | | | |
| 1. | RCL | § 2 pkt 7 | W przepisie definiującym pojęcie „likwidacji konta” określono de facto skutki takiej likwidacji – którymi ma być m.in. pozostawienie „minimalnego zestawu danych pozwalającego na zachowanie rozliczalności działań”. Regulacja w tym zakresie me jednak charakter materialny, a nie wyłącznie definicyjny, i tym samym powinna zostać zamieszczona w przepisach materialnych projektu.  Takie brzmienie ww. przepisu nie precyzuje przy tym katalogu danych, które będą przechowywane po likwidacji konta – co budzi istotne wątpliwości; rozważenia wymaga określenie co najmniej przykładowego katalogu takich nadal przechowywanych danych. | **Uwaga uwzględniona częściowo.**  Definicja została uzupełniona o wskazanie zakresu danych pozostałych po likwidacji konta, a są to dane obejmujące informacje w zakresie: imienia, drugiego imienia, nazwiska, nr PESEL oraz czy konto było założone dla obcokrajowca.  W zakresie uwagi co do zawarcia skutku likwidacji konta w przepisach materialnych a nie w definicji, należy zauważyć, że wprowadzenie przepisu materialnego w tym zakresie prowadziłoby do powielenia treści definicji, co w ocenie projektodawcy nie jest zasadne. |
| 2. | RCL | § 2 pkt 15 | Z treści przepisu projektowanego rozporządzenia nie wynika jaka jest podstawa prawna oraz charakter prawny systemu ROBUS; proponuje się co najmniej wskazanie, że system ten jest systemem teleinformatycznym i działa na podstawie art. 175 da § 2 ustawy upoważniającej – z jednoczesnym wskazaniem jego przedmiotu lub (jak obecnie) celu jego funkcjonowania. | **Uwaga uwzględniona.**  Projekt został zmieniony poprzez dodanie w definicji, że ROBUS jest sądowym systemem teleinformatycznym i działa na podstawie art. 175 da § 2, przedmiot i cel jest obecnie w pkt 15 |
| 3. | RCL | § 5 ust. 8  § 15 ust. 2 | Jakkolwiek zasadne jest zapewnienie, aby (jak podano w wyjaśnieniach projektodawcy dotyczących uwag RCL zgłoszonych w uzgodnieniach) na podstawie projektowanych przepisów nie dochodziło dublowania kont dla tych samych jednostek organizacyjnych, i tym samym aby w systemie jednostki te nie mogły występować w kilku postaciach (np. jako gmina, burmistrz, urząd gminy), to zauważa się, że mająca ten skutek zapewnić regulacja § 5 ust. 8 de facto wyłącza wskazane w niej podmioty z posiadania kont w portalu informacyjnym – co budzi wątpliwości co do zgodności z zakresem upoważnienia ustawowego. | **Uwaga uwzględniona.**  W ocenie MS wbrew stanowisku RCL zaproponowana regulacja § 5 ust. 8 nie wyłącza organów i urzędów z posiadania kont w PI, a jedynie determinuje, że te organy i urzędy są obsługiwane / działają poprzez konto założone dla jednostki samorządu terytorialnego, związku międzygminnego, związku powiatów, związku powiatowo-gminnego, związku metropolitalnego oraz państwowych albo samorządowych jednostek organizacyjnych.  Precyzując jednak brzmienie przepisu, aby lepiej oddać intencje projektodawcy, proponujemy następujące brzmienie:  Konto zakłada się dla jednostki samorządu terytorialnego, związku międzygminnego, związku powiatów, związku powiatowo-gminnego, związku metropolitalnego oraz państwowych albo samorządowych jednostek organizacyjnych. Konto to jest wspólne dla organów tych jednostek i urzędów je obsługujących. |
| 4. | PUODO | § 6 | Zgodnie z **§ 6 ust. 1 i 2 projektu** weryfikacja polega na potwierdzeniu, że dane składającego wniosek o założenie konta w portalu informacyjnym są zgodne z danymi wskazanymi we wniosku, a weryfikacja ta odbywa się m. in. na podstawie danych z właściwych rejestrów lub ewidencji. Z projektowanego przepisu powinno wprost wynikać, w oparciu o dane osobowe z jakich konkretnych rejestrów lub ewidencji ma następować ww. weryfikacja oraz że weryfikacja polega na potwierdzeniu poprawności danych w zakresie niezbędnym do dokonania przedmiotowej weryfikacji. Pozwoli to zapewnić zgodność z wynikającymi z rozporządzenia 2016/679 zasadami zgodności z prawem, rzetelności i przejrzystości oraz minimalizacji. Należy też wskazać, że przetwarzanie danych osobowych na podstawie projektowanego przepisu oparte będzie na przesłance legalizującej z art. 6 ust. 1 lit. c) rozporządzenia 2016/679, tj. niezbędności przetwarzania do realizacji obowiązku prawnego ciążącego na administratorze. W takim przypadku, zgodnie z art. 6 ust. 3 tego rozporządzenia, regulacja krajowa będąca podstawą przetwarzania powinna określać rejestr (ewidencję) z jakiej pozyskiwane są dane, tryb pozyskiwania, zakres danych niezbędny do weryfikacji, a ta podstawa prawna powinna wynikać z aktu rangi ustawy, a nie rozporządzenia służącego jej wykonaniu.  Co więcej, z projektowanego § 6 nie wynika, **jak dokonywana jest ww. weryfikacja**, tzn. czy odbywa się ona w taki sposób, że w przypadku niepotwierdzenia poprawności dane niepoprawne nie są udostępniane. Czy jest dokonywana przez pracownika podmiotu odpowiedzialnego za prowadzenie portalu, czy też w inny sposób.  Ponieważ kwestia ta jest bezpośrednio związana z przetwarzaniem danych osobowych, w tym z koniecznością nieudostępniania danych niepoprawnych to powinna ona zostać dookreślona w projekcie, co jest istotne z punktu widzenia nie tylko zasady prawidłowości danych, zgodnie z którą dane osobowe muszą być prawidłowe i w razie potrzeby uaktualniane [art. 5 ust. 1 lit. d) rozporządzenia 2016/679], ale i wyrażonej w rozporządzeniu 2016/679 zasady rozliczalności. Zastrzeżenia te dotyczą wykonawców norm – zarówno administratora potwierdzającego poprawność danych we wniosku, jak i administratora potwierdzającego poprawność danych będącego dysponentem rejestru czy ewidencji.  Analogiczną uwagę należy odnieść **§ 6 ust. 5 oraz § 10 ust. 6 projektu** odnoszących się do weryfikacji użytkownika będącego pełnomocnikiem zawodowym, komornikiem sądowym, biegłym sądowym lub mediatorem, za pomocą systemu ROBUS. | **Uwaga uwzględniona częściowo.** Uzupełniono przepis deklarując, o jakie systemy i rejestry mogą być wykorzystywane do weryfikacji. Sprecyzowanie ma charakter ogólny, ponieważ wymienienie tych systemów z nazwy ograniczałyby możliwości rozwoju PI (chodzi o systemy i rejestry, które są dostępne dla sądów na podstawie szczególnych przepisów, są sądowymi systemami informatycznymi lub są ogólnie dostępne – mogą to być systemy udostępniane przez państwa obce). Weryfikacja polega na sprawdzeniu danych przekazanych przez użytkownika portalu informacyjnego. Zakres danych weryfikowanych wynika więc z danych podawanych we wniosku o założenie konta. Przewidziane rozwiązanie realizuje rozwiązania ustawowe związane ze sprawowaniem wymiaru sprawiedliwości. Ogólna podstawa dotycząca przetwarzania danych związana z funkcjonowaniem sądowych systemów teleinformatycznych znajduje się w art. 175da ustawy z dnia 27 lipca 2001 r. Prawo o ustroju sądów powszechnych (t.j. Dz. U. z 2024 r. poz. 334 z późn. zm.). |
| 5. | PUODO | § 13 ust. 6 w zw. z § 2 pkt 7 | Zgodnie z **§ 13 ust. 6 projektu** dane osobowe użytkownika związane z kontem są usuwane po upływie 5 lat od dnia zlikwidowania konta. Z kolei zgodnie z **§ 2 pkt 7 projektu** przez likwidację konta rozumie się „usunięcie danych konta, profili zależnych oraz użytkowników kont powiązanych z kontem, skutkujące brakiem możliwości uwierzytelnienia na koncie i pozostawieniem minimalnego zestawu danych pozwalających na zachowanie rozliczalności działań podejmowanych w ramach portalu przez użytkownika konta, podmiot lub podmiot publiczny”.  Po pierwsze, nie jest jasne, **co należy rozumieć przez „minimalny zestaw danych**” pozostawianych na koncie użytkownika i czy obejmuje on również dane o charakterze osobowym. Ze względu na ww. zasadę minimalizacji z projektu powinno wprost wynikać, jaki jest zakres danych pozostawianych na koncie po jego likwidacji.  Po drugie treść § 2 pkt 7, z której wynika, że likwidacja konta jest równoznaczna z usunięciem danych z tego konta (z zastrzeżeniem ww. „minimalnego zestawu danych”) wydaje się być sprzeczna z § 13 ust. 6 projektu i wynikającym z niego okresie czasu, po którym dane są  usuwane – powstaje pytanie, czy dane te są usuwane wraz ze zlikwidowaniem konta użytkownika, czy też dopiero po upływie 5 lat od likwidacji. Co więcej, jeżeli ww. okres 5 lat odnosi się do danych pozostawianych na koncie zgodnie z § 2 pkt 7 to również powinno wynikać to wprost z projektowanych regulacji. Postulowane doprecyzowanie ww. przepisów jest istotne ze względu na zasadę ograniczenia przechowywania, a także ww. zasady zgodności z prawem, rzetelności i przejrzystości. | Uwaga uwzględniona w zakresie doszczegółowienia „minimalnego zestawu danych” poprzez wskazanie, że chodzi o dane obejmujące informacje w zakresie: imienia, drugiego imienia, nazwiska, nr PESEL oraz czy konto było założone dla obcokrajowca.  W pozostałym zakresie, dotyczącym 5 letniego okresu, po którym dane są usuwane należy wskazać, że z przepisu § 13 ust. 6 wprost wynika, że chodzi o 5 lat liczone „od dnia zlikwidowania konta”. |