Uwagi do projektu rozporządzenia Rady Ministrów w sprawie szczegółowych sposobów realizacji obowiązków w zakresie Krajowych Ram Interoperacyjności, minimalnych wymagań dla rejestrów publicznych, minimalnych wymagań dla systemów teleinformatycznych używanych do realizacji zadań publicznych i wymiany danych z podmiotami publicznymi (RD313) UZGODNIENIA				
Lp.	**Jednostka redakcyjna, której uwaga dotyczy/ Uzasadnienie/ pkt OSR**	**Podmiot zgłaszający**	**Uwaga/Propozycja zmian zapisu**	**Stanowisko MC**
Uwagi ogólne				
1.	**Uwaga ogólna**	**RCL**	Zgodnie z upoważnieniem ustawowym zawartym w art. 18 ustawy z dnia 17 lutego 2005 r. o informatyzacji działalności podmiotów realizujących zadania publiczne (Dz. U. z 2025 r. poz. 1703 oraz z 2026 r. poz. 160), zwanej dalej „ustawą" – w wersji obowiązującej od dnia 23 lutego 2027 r. – przedmiotowe rozporządzenie powinno określać szczegółowe sposoby realizacji, przez podmiot realizujący zadania publiczne, obowiązków, o których mowa w art. 13 ust. 1 pkt 1 i 2 oraz art. 14 ust. 1 ustawy, tj. szczegółowe sposoby używania przez ten podmiot, do realizacji ww. zadań: a) systemów teleinformatycznych spełniających minimalne wymagania dla systemów teleinformatycznych używanych do realizacji zadań publicznych i wymiany danych z podmiotami publicznymi, b) systemów teleinformatycznych zapewniających interoperacyjność zgodnie z Krajowymi Ramami Interoperacyjności obejmującymi określone zagadnienia, c) rejestrów publicznych prowadzonych zgodnie z minimalnymi wymaganiami dla tych rejestrów. W tym kontekście zauważenia wymaga, że projekt rozporządzenia, w części swojej regulacji, nie tyle wskazuje na sposoby realizacji ww. obowiązków, a określa np. minimalne wymagania dla rejestrów publicznych (np. § 5 ust. 1 projektu) bądź minimalne wymagania dla systemów teleinformatycznych (np. § 12 ust. 1 projektu) – na wzór przepisów dotychczasowych. Projekt wymaga więc stosownego przeformułowania pod kątem właściwej realizacji upoważnienia ustawowego, w jego zmienionym brzmieniu.	**Uwaga uwzględniona** Projekt uległ niezbędnemu przeformułowaniu pod kątem właściwej realizacji upoważnienia ustawowego wskazując sposoby realizacji, przez podmiot realizujący zadania publiczne, obowiązków, o których mowa w art. 13 ust. 1 pkt 1 i 2 oraz art. 14 ust. 1 ustawy. W szczególności zmianie uległy przepisy w zakresie Krajowych Ram Interoperacyjności: § 3 ust. 3 pkt 2, ust. 4 pkt 1-4, ust. 5-7 projektu, minimalnych wymagań dla rejestrów publicznych: § 5 ust. 1, § 6 ust. 2, § 7 i § 9 projektu, minimalnych wymagań dla systemów teleinformatycznych: § 10 - § 17 projektu.

2.	**Uwaga ogólna**	**MKiŚ**	Uprzejmie wskazuję, że przedstawiony projekt wymaga dalszego dopracowania merytorycznego i redakcyjnego. W projekcie nie określono jednoznacznie charakteru normatywnego poszczególnych załączników oraz wzajemnych relacji między tymi załącznikami a przepisami zasadniczej części rozporządzenia. W obecnym brzmieniu nie jest możliwe jednoznaczne ustalenie, które wymagania mają charakter obligatoryjny, które stanowią wymagania minimalne, a które należy traktować jako rekomendacje lub przykłady. Wątpliwości budzi również szczegółowość regulacji technicznych zawartych w załącznikach. W przypadku uznania wskazanych w projekcie formatów, standardów i technologii za obowiązkowe może dojść do kolizji z wymaganiami wynikającymi z przepisów prawa Unii Europejskiej, w tym aktów wykonawczych Komisji Europejskiej, lub powszechnie stosowanych standardów międzynarodowych. Pełna ocena skutków projektowanych regulacji będzie możliwa po uporządkowaniu i przeredagowaniu załączników oraz jednoznacznym określeniu zakresu ich stosowania i charakteru.	**Uwaga wyjaśniona** Wszystkie załączniki stanowią część rozporządzenia i z tego względu mają charakter normatywny. W przepisach rozporządzenia wskazano jednoznaczne odwołania do załączników. Wszystkie wymagania w rozporządzeniu mają charakter obligatoryjny. Minimalne wymagania dla rejestrów publicznych, a także minimalne wymagania dla systemów teleinformatycznych używanych do realizacji zadań publicznych i wymiany danych z podmiotami publicznymi oznaczają zestawy wymagań, które podmiot realizujący zadania publicznie musi spełniać na poziomie wskazanym w wymaganiach, a fakultatywnie - na poziomie wyższym, niż określony w wymaganiach. Projekt rozporządzenia nie narusza ani nie ogranicza stosowania przepisów prawa Unii Europejskiej, w tym aktów wykonawczych Komisji Europejskiej ustanawiających szczególne wymagania dotyczące interoperacyjności, wymiany danych lub stosowania określonych standardów technicznych. Określone w projekcie formaty i standardy służą zapewnieniu interoperacyjności podmiotów realizujących zadania publiczne i uwzględniają regulacje wynikające z rozporządzenia Parlamentu Europejskiego i Rady (UE) 2024/903 z dnia 13 marca 2024 r. w sprawie ustanowienia środków na rzecz wysokiego poziomu interoperacyjności sektora publicznego na terytorium Unii (akt w sprawie Interoperacyjnej Europy) (Dz. Urz. UE L 2024/903 z 22.03.2024).
Uwagi szczegółowe				
3.	**§ 2**	**MNiSW**	W odniesieniu do art. 19 projektu rozporządzenia proponuję uzupełnienie katalogu definicji zawartego w art. 2 o definicję „istotnej zmiany systemu teleinformatycznego”. Jej wprowadzenie	**Uwaga nieaktualna** Dotychczasowy § 19 został usunięty z projektu rozporządzenia.

			jest zasadne z uwagi na potrzebę zapewnienia jednolitej interpretacji i stosowania przepisów, w szczególności w zakresie rozumienia pojęcia zmiany istotnej dla funkcjonowania systemu teleinformatycznego. Proponuję następujące brzmienie definicji: „istotna zmiana systemu teleinformatycznego" – zmiana dotycząca architektury, funkcjonalności związanych z podstawowym celem systemu, sposobu wymiany danych, sposobu realizacji zabezpieczeń; istotna zmiana nie obejmuje zmian eksploatacyjnych, niwelowania błędów systemu lub aktualizacji środowiska systemu	
4.	**§ 2**	**MFiG (MF)**	po pkt 24) występuje pkt 26); brak punktu 25)	**Uwaga uwzględniona**
5.	**§ 2 pkt 14**	**MRiRW**	**<u>Projektowane brzmienie § 2 pkt 14:</u>** „14) pielęgnowalność - stopień, w jakim system teleinformatyczny może być modyfikowany w celu poprawy, korekty błędów lub dostosowania do zmian środowiska i wymagań;" **<u>Proponowane brzmienie § 2 pkt 14:</u>** „14) **modyfikowalność** - stopień, w jakim system teleinformatyczny może być modyfikowany w celu poprawy, korekty błędów lub dostosowania do zmian środowiska i wymagań;" Termin „pielęgnowalność" nie występuje powszechnie w polskiej praktyce inżynierii oprogramowania ani w dokumentacji projektowej systemów teleinformatycznych. Proponowane określenie „modyfikowalność" jest zgodne z terminologią stosowaną w normie ISO/IEC 25010 i ogranicza ryzyko rozbieżności interpretacyjnych podczas projektowania, odbioru i audytowania systemów. .	**Uwaga wyjaśniona** W normie ISO/IEC 25010 „maintainability" oznacza „pielęgnowalność" (inaczej „utrzymywalność"). Modyfikowalność jest aspektem pielęgnowalności, a tym samym nie jest pojęciem z nim tożsamym. Pielęgnowalność obejmuje szerszy zakres cech, m.in.: • modularność, • możliwość ponownego użycia, • analizowalność, • testowalność, • modyfikowalność. W związku z tym terminologia projektu została dostosowana do nazewnictwa określonego w normie ISO/IEC 25010.
6.	**§ 2 pkt 20**	**Minister – Koordynator Służb Specjalnych**	Jednocześnie proponuję wprowadzenie w projekcie rozporządzenia następujących zmian mających na celu uwzględnienie potrzeb służb specjalnych w ramach projektowanych regulacji. W tym zakresie proponuję wprowadzenie zmian w definicji pojęcia „rozliczalność" (§ 2 pkt 20 projektu rozporządzenia), które uwzględnią specyfikę zadań realizowanych przez służby specjalne w ramach organizowanych dostępów do zasobów informacyjnych podmiotów publicznych, pozwalające na ochronę danych identyfikacyjnych	**Uwaga wyjaśniona** Ochrona danych identyfikacyjnych funkcjonariuszy wynika z przepisów ustawowych. Przepisy te podlegają uwzględnieniu przy realizacji wymagań określonych w projekcie. Nie zachodzi zatem potrzeba modyfikowania definicji „rozliczalności" na potrzeby poszczególnych kategorii podmiotów.

			funkcjonariuszy, co wynika z przepisów ustawowych. W tym zakresie proponuję rozważenie wdrożenie tzw. użytkownika instytucjonalnego, bowiem uregulowanie takiego rodzaju „użytkownika'" na poziomie rozporządzenia ułatwi realizację przez służby specjalne ich ustawowych zadań, a podmioty publiczne udostępniające posiadane dane nie będą miały obaw co do ewentualnego zarzutu naruszenia przepisów. Wskazać należy, że takie regulacje zapewnią rozliczalność po stronie gestora zasobu na poziomie instytucji, gdzie widoczne będą jedynie dane instytucji przesyłającej zapytanie, pozostawiając jednocześnie rozliczalność co do konkretnych użytkowników, która będzie możliwa poprzez wewnętrzne rozwiązania. W tym miejscu należy nadmienić, że art. 34 ust. 2a ustawy z dnia 24 maja 2002 r. o Agencji Bezpieczeństwa Wewnętrznego oraz Agencji Wywiadu przewiduje już taką sytuację i stanowi, że administrator zbioru danych udostępnia Szefowi Agencji Bezpieczeństwa Wewnętrznego w drodze teletransmisji informacje zgromadzone w zbiorach danych bez konieczności każdorazowego przedstawiania imiennego upoważnienia wydanego przez Szefa Agencji Bezpieczeństwa Wewnętrznego, okazywanego przez funkcjonariusza Agencji Bezpieczeństwa Wewnętrznego wraz z legitymacją służbową, jeżeli jednostka organizacyjna Agencji Bezpieczeństwa Wewnętrznego będąca odbiorcą informacji spełnia łącznie następujące warunki: 1) posiada urządzenia umożliwiające odnotowanie w systemie, kto, kiedy, w jakim celu oraz jakie dane uzyskał; 2) posiada zabezpieczenia techniczne i organizacyjne uniemożliwiające wykorzystanie danych niezgodnie z celem ich uzyskania; 3) specyfika lub zakres wykonywanych zadań uzasadnia takie udostępnienie. W związku z powyższym proponuję rozważenie nadania § 2 pkt 20 projektu rozporządzenia następującego brzmienia: „20) rozliczalność - właściwość systemu teleinformatycznego pozwalającą przypisać określone działanie w tym systemie do podmiotu, osoby fizycznej lub procesu oraz umiejscowić je w czasie; ”.	
7.	**§ 3 ust. 4 pkt 3**	**MRiRW**	**<u>Projektowane brzmienie § 3 ust. 4 pkt 3:</u>** „4. Interoperacyjność na poziomie semantycznym osiągana jest przez: (……)	**Uwaga wyjaśniona** Proponowane uzupełnienie nie jest konieczne. Przetwarzanie danych osobowych w ramach prowadzenia rejestrów publicznych oraz wymiany

			3) stosowanie w rejestrach publicznych odwołań do rejestrów publicznych zawierających dane referencyjne w zakresie niezbędnym do realizacji zadań publicznych;" **<u>Proponowane brzmienie § 3 ust. 4 pkt 3:</u>** „4. Interoperacyjność na poziomie semantycznym osiągana jest przez: (……) 3) stosowanie w rejestrach publicznych odwołań do rejestrów publicznych zawierających dane referencyjne w zakresie niezbędnym do realizacji zadania publicznego, **z uwzględnieniem przepisów o ochronie danych osobowych, w przypadku, gdy dane referencyjne stanowią dane osobowe."** Przepis nie zawiera żadnego mechanizmu ograniczania zakresu danych pobieranych z rejestrów referencyjnych. Może to prowadzić do np. pobierania szerszego zakresu danych niż jest niezbędny. Proponowane brzmienie nie ogranicza zasady interoperacyjności ani możliwości wykorzystywania danych referencyjnych pomiędzy rejestrami publicznymi. Jego celem jest zapewnienie, aby wymiana i wykorzystywanie danych odbywały się w sposób zgodny z obowiązującymi przepisami prawa, w szczególności w zakresie ochrony danych osobowych. Zmiana ma zatem charakter doprecyzowujący i porządkujący oraz służy zapewnieniu właściwego wyważenia pomiędzy potrzebą zapewnienia interoperacyjności rejestrów publicznych a obowiązkiem ochrony praw osób, których dane są przetwarzane.	danych pomiędzy rejestrami podlega przepisom o ochronie danych osobowych niezależnie od ich wyraźnego przywołania w projektowanym przepisie. Ponadto projektowany § 3 ust. 4 pkt 3 ogranicza wykorzystywanie danych referencyjnych do zakresu niezbędnego do realizacji zadania publicznego, co pozostaje spójne z zasadą minimalizacji danych. Ponadto zgodnie z Zasadami techniki prawodawczej nie powtarza się w przepisach rozporządzenia norm wynikających bezpośrednio z aktów wyższego rzędu. Obowiązek przestrzegania RODO i przepisów krajowych o ochronie danych osobowych obowiązuje niezależnie od tego, czy zostanie powtórzony w rozporządzeniu.
8.	**§ 3 ust. 4 pkt 1 i 3 oraz OSR**	**MKiŚ**	Projekt przewiduje obowiązek stosowania modelu danych CPSV-AP do opisu usług publicznych w formacie nadającym się do odczytu maszynowego (pkt 1). Dodatkowo wskazuje, że opisy procedur są publikowane i uaktualniane na BIP danego podmiotu (pkt 3). Wątpliwości budzi, czy na BIP mają być publikowane usługi opisane w modelu CPSV-AP, czy w innym miejscu (np. w repozytorium interoperacyjności). Dodatkowo wyjaśnienia wymaga relacja między opisami usług, które mają być publikowane na BIP urzędów, a opisami usług funkcjonującymi obecnie w ramach kart usług www.gov.pl (w niektórych przypadkach jeden opis usługi dotyczy wielu urzędów realizujących tę samą usługę).	**Uwaga częściowo uwzględniona** **Wyjaśnienie** **Uwaga odnosi się do § 3 ust. 3 pkt 1 i 3 rozporządzenia.** Zgodnie z przepisami rozporządzenia <u>opisy procedur</u> obowiązujących przy załatwianiu spraw z zakresu jego właściwości za pomocą środków komunikacji elektronicznej mają być publikowane i uaktualniane na stronie podmiotowej w Biuletynie Informacji Publicznej. Z kolei <u>informowanie o elektronicznych usługach publicznych</u> świadczonych przez podmiot następuje m.in. w formacie nadającym się do odczytu maszynowego, wskazanym

			1. Należy doprecyzować, które opisy usług lub opisy procedur i w jakim modelu publikowane są na BIP, a jakie w repozytorium interoperacyjności. 2. Należy wyjaśnić relację między istniejącymi już opisami usług na www.gov.pl dotyczących usług realizowanych przez wiele urzędów, a opisami usług, które miałyby być publikowane na BIP indywidualnego urzędu.	w załączniku do rozporządzenia. § 3 ust. 3 pkt 1 uzupełniono określając, że ww. informacje mają być opublikowane na stronie podmiotowej w BIP. Projekt rozporządzenia nie zakłada publikowania opisów procedur ani informacji o usługach w repozytorium interoperacyjności.
9.	**§ 3 ust. 4 pkt 4**	**MKiŚ**	§ 3 ust. 4 pkt 4 wskazuje, że interoperacyjność na poziomie semantycznym jest osiągana przez stosowanie formatów plików określonych w załącznikach nr 2 i 3 do rozporządzenia. Wprowadzanie wymogu, by podmiot publiczny w celu osiągnięcia interoperacyjności na poziomie semantycznym musiał umożliwić odczyt wskazanych w załączniku nr 3 zamkniętych, komercyjnych formatów plików, jest sprzeczne z ogólną zasadą wspierania neutralności technologicznej projektu wskazaną w § 3 ust. 2. Usunięcie w § 3 ust. 4 pkt 4 odniesienia do załącznika nr 3 – pozostawienie wyłącznie odniesienia do załącznika nr 2. Proponowane nowe brzmienie: „4) stosowanie formatów plików określonych w załączniku nr 2 do rozporządzenia.”	**Uwaga uwzględniona** Załącznik nr 3 został usunięty z projektu.
10.	**§ 3 ust. 6**	**MKiŚ**	Zasadne jest doprecyzowanie zakresu procesów podlegających obowiązkowi dokumentowania zgodnie ze standardem notacji i modelu procesu biznesowego (ang. Business Process Model and Notation, BPMN). Obecne brzmienie może być interpretowane jako obejmujące wszystkie procesy realizowane przy wykorzystaniu środków komunikacji elektronicznej, niezależnie od ich skali, stopnia automatyzacji i znaczenia dla interoperacyjności. Warto wskazać kryteria określające procesy objęte tym obowiązkiem.	**Uwaga wyjaśniona** Rozporządzenie jest aktem wykonawczym do ustawy z dnia 17 lutego 2005 r. o informatyzacji działalności podmiotów realizujących zadania publiczne (Dz. U. z 2026 r. poz. 1241). Z tego względu podmioty powinny tworzyć modele dla tych procesów, które służą realizacji zadań publicznych za pomocą środków komunikacji elektronicznej - z uwzględnieniem konieczności zapewnienia poprawnej współpracy podmiotów realizujących zadania publiczne, w tym efektywnej wymiany danych. W związku z tym proponowane uzupełnienie nie jest konieczne.
11.	**§ 3 ust. 6**	**MRiRW**	**<u>Projektowane brzmienie ust. 6</u>:** „6. Procesy, o których mowa w ust. 3 pkt 2, dokumentuje się zgodnie ze standardem notacji i modelu procesu biznesowego (ang. Business Process Model and Notation, BPMN) określonym przez normę ISO/IEC 19510.”	**Uwaga wyjaśniona** Rozporządzenie jest aktem wykonawczym do ustawy o informatyzacji działalności podmiotów realizujących zadania publiczne. Z tego względu podmioty powinny tworzyć modele dla procesów, które służą realizacji zadań publicznych za

			<u>Proponowane brzmienie ust. 6:</u> „6. Procesy, o których mowa w ust. 3 pkt 2, mające znaczenie dla zapewnienia interoperacyjności pomiędzy podmiotami realizującymi zadania publiczne, dokumentuje się zgodnie ze standardem notacji i modelu procesu biznesowego BPMN określonym przez normę ISO/IEC 19510." 'Obecne brzmienie może być rozumiane jako obowiązek dokumentowania w BPMN wszystkich procesów związanych z realizacją zadań publicznych za pomocą środków komunikacji elektronicznej. W dużych organizacjach liczba takich procesów i podprocesów jest bardzo duża, natomiast znaczna ich część ma charakter wewnętrzny i nie wpływa na współpracę z innymi po 4 podmiotami. Z punktu widzenia celu KRI zasadne byłoby objęcie tym obowiązkiem przede wszystkim procesów istotnych dla interoperacyjności. Proponowane brzmienie ust. 6 ma na celu doprecyzowanie jakich procesów dotyczy obowiązek dokumentowania zgodnie z BPMN.	pomocą środków komunikacji elektronicznej – z uwzględnieniem konieczności zapewnienia poprawnej współpracy podmiotów realizujących zadania publiczne, w tym efektywnej wymiany danych. Obecnie każde zadanie publiczne realizowane przez jeden podmiot może potencjalnie służyć realizacji zadań innego podmiotu, poprzez ponowne wykorzystanie danych zgodnie z przepisem art. 220 Kodeksu postępowania administracyjnego. W związku z tym proponowane uzupełnienie nie jest konieczne.
12.	**§ 3 ust. 6, § 11 ust. 3, § 11 ust. 8, § 14 ust. 4**	**Minister – Koordynator Służb Specjalnych**	Projekt rozporządzenia w swojej treści odsyła do norm ISO/IEC albo ETSI dotyczących: modelowania procesów (§ 3 ust. 6 projektu rozporządzenia), zarządzania usługami (§ 11 ust. 3 projektu rozporządzenia), zarządzania ciągłością działania (§ 11 ust. 8 projektu rozporządzenia) oraz dostępności cyfrowej (§ 14 ust. 4 projektu rozporządzenia) poprzez wskazanie konkretnej normy. Natomiast w § 13 ust. 1 projektu rozporządzenia projektodawca odsyła do normy dotyczącej kodowania znaków - ISO/IEC 10646 wraz ze zmianami lub normy je zastępujące. W związku z powyższym proponuję we wszystkich przepisach odsyłających do konkretnych norm zamieścić wskazanie, że przedmiotową normę stosuje się „wraz ze zmianami lub normą ją zastępującą". Przedmiotowa zmiana ma pozwolić na stosowanie najnowszych norm bez potrzeby dokonywania nowelizacji projektowanego rozporządzenia	**Uwaga uwzględniona** W przepisach zostało zapisane, że przedmiotową normę stosuje się wraz ze zmianami lub normą ją zastępującą.
13.	**§ 4**	**MRiRW**	W § 4 projektowanego rozporządzenia po ust. 2 proponuje się dodać ust. 3 i 4 w następującym brzmieniu: „3. Obowiązek przeprowadzenia oceny interoperacyjności krajowej, o której mowa w ust. 1, stosuje się do projektów dotyczących utworzenia nowego albo istotnej zmiany istniejącego systemu teleinformatycznego, rejestru publicznego lub elektronicznej usługi publicznej, jeżeli zmiana ta może mieć	**Uwaga wyjaśniona** Obowiązek przeprowadzania ocen interoperacyjności krajowej wynika z art. 12n ustawy o informatyzacji. Zgodnie przepisami ustawy o informatyzacji podmiot realizujący zadania publiczne przeprowadza ocenę interoperacyjności krajowej każdorazowo przed

			istotny wpływ na interoperacyjność z innymi systemami lub rejestrami publicznymi. 4. Oceny, o której mowa w ust. 1, nie przeprowadza się w przypadku zmian o charakterze technicznym, utrzymaniowym, bezpieczeństwa, aktualizacji oprogramowania lub innych zmian, które nie powodują istotnej zmiany sposobu wymiany danych albo procesu realizacji zadania publicznego.” Projekt przewiduje ocenę interoperacyjności krajowej, jednak moim zdaniem konieczne jest jednoznaczne wskazanie, kiedy ocena jest faktycznie wymagana. Brak wyłączenia zmian nieistotnych może prowadzić do sytuacji, w której każda modernizacja, aktualizacja czy modyfikacja systemu będzie wymagała przeprowadzenia pełnej procedury oceny. Będzie to szczególnie problematyczne dla ARiMR, która posiada ponad 100 systemów.	wprowadzeniem zmian w systemie teleinformatycznym używanym do realizacji zadań publicznych lub w rejestrze publicznym, a taka ocena interoperacyjności krajowej zawiera opis wpływu zmian wprowadzanych w systemie teleinformatycznym używanym do realizacji działań publicznych lub w rejestrze publicznym na podmioty publiczne, opis działań podjętych oraz planowanych do podjęcia w celu minimalizacji lub usunięcia negatywnego wpływu zmian na podmioty publiczne, informację o negatywnym wpływie zmian na podmioty publiczne, który nie zostanie usunięty w ramach podjętych działań. Przepisy ustawy już wyraźnie wskazują, że takiej oceny nie przygotowuje się, w przypadku wprowadzania zmian i działań prowadzonych w stosunku do systemów teleinformatycznych używanych do realizacji zadań publicznych oraz do rejestrów publicznych niewpływających na ich interoperacyjność, w szczególności do konserwacji oprogramowania, aktualizacji w zakresie bezpieczeństwa lub aktualizacji technicznych.
14.	**§ 4, § 12, § 16, § 19–20 + zał. nr 4 i 5**	**MFiG (MF)**	w opinii MF – Bezpieczeństwo API i systemów – dostęp anonimowy do API powinien być dopuszczalny tylko po ocenie ryzyka; należy zapewnić możliwość jego całkowitego wyłączenia w systemach wymagających ochrony, a wymagania interoperacyjności powinny być podporządkowane bezpieczeństwu, rozliczalności, ciągłości działania i ochronie danych.	**Uwaga wyjaśniona** Ministerstwo co do zasady zgadza się z opinią MFiG. Jednakże projekt nie wymaga zapewnienia anonimowego dostępu do API. Dobór środków bezpieczeństwa pozostaje uzależniony od analizy ryzyka i charakteru świadczonych usług. Należy podkreślić, że wymagania interoperacyjności, wynikające z przepisów prawa powszechnie obowiązującego, powinny być rozpatrywane łącznie z analogicznymi wymaganiami prawnymi z zakresu bezpieczeństwa, rozliczalności, ciągłości działania i ochrony danych. Ponadto zgodnie z Zasadami techniki prawodawczej nie powtarza się w przepisach

				rozporządzenia norm wynikających bezpośrednio z aktów wyższego rzędu.
15.	**§ 5 ust. 1 i 2**	**RCL**	Zgodnie z projektowanym § 5 ust. 1 rozporządzenia w rejestrach publicznych wyróżnia się w szczególności następujące typy obiektów: osobę fizyczną, podmiot i obiekt przestrzenny. Natomiast zgodnie z przepisem ust. 2 – dla każdego obiektu, o którym mowa w ust. 1, nadaje się unikatowy identyfikator. Wyjaśnienia zatem wymaga, mając na uwadze otwarty katalog przepisu ust. 1, czy obowiązek nadawania identyfikatora dotyczy także innych obiektów niż te wymienione w ust. 1, a dodatkowo – jakie to mogą być obiekty i czy możliwe jest ich wymienienie, a tym samym – zamknięcie katalogu obiektów.	**Uwaga wyjaśniona** W rejestrach publicznych są przetwarzane różnorodne typy obiektów. Obiektami wyróżnionymi, ze względu na ich walor referencyjności, są obiekty wskazane w projektowanym § 5 ust. 1 rozporządzenia. Właśnie ze względu na ich referencyjność nadaje się im obowiązkowo unikatowy identyfikator, co pozwala na jednoznaczne identyfikowanie obiektu tego typu w różnych publicznych systemach teleinformatycznych i rejestrach publicznych, a także niepublicznych zbiorach danych. Jednakże, jak wspomniano powyżej, w setkach występujących rejestrów publicznych przetwarza się różnorodne typy obiektów. Ich liczba jest o rzędy wielkości większa, niż wskazane w § 5 ust. 1 projektu rozporządzenia. Należy podkreślić, że w istniejących rejestrach publicznych może dochodzić do zmiany zakresu przetwarzanych danych, co może skutkować zmianą liczby typów obiektów w nich przetwarzanych. Co więcej - z biegiem czasu powstają nowe rejestry publiczne, w których mogą występować typy obiektów aktualnie nie występujące. Z tego względu katalog typy obiektów w rejestrach publicznych nie może być zamknięty. Odnośnie obowiązku nadawania unikatowego identyfikatora, to zachodzi on wyłącznie w przypadku referencyjnych typów obiektów określonych w przywołanym przepisie. Przykładowo: w Powszechnym Elektronicznym Systemie Ewidencji Ludności (PESEL) przetwarzane są m.in. dane osób fizycznych i powiązane z nimi dane adresowe. I tak, zgodnie z załącznikiem nr 1 do projektu rozporządzenia obiektowi typu "Osoba fizyczna posiadająca

				nadany numer PESEL" nadaje się unikatowy identyfikator "Numer PESEL". Pozwala to na jednoznaczną identyfikację obiektów tego typu, czyli osób fizycznych, przez niepowtarzalny numer. Z kolei z osobą fizyczną powiązany jest obiekt typu "adres zameldowania", posiadający różnorodne atrybuty (jak ulica, nr domu czy miejscowość), ale nie posiadający i dla którego nie jest wymagane posiadanie unikatowego identyfikatora. Nie ma natomiast przeciwskazań, aby gestor rejestru publicznego nadawał unikatowe identyfikatory także typom obiektów innym, niż wskazane w § 5 ust. 1 projektu rozporządzenia.
16.	**§ 5 ust. 1–3, zał. nr 1**	**MFiG (MRiT)**	§ 5 ust. 2 nakazuje nadanie unikatowego identyfikatora każdemu obiektowi, w tym obiektowi przestrzennemu, natomiast § 5 ust. 3 ogranicza zakres załącznika nr 1 – w części dotyczącej obiektów przestrzennych – do punktu adresowego i działki ewidencyjnej. Budynek, będący obiektem podstawowym rejestrów prowadzonych np. CEEB, CRChEB jest zatem objęty obowiązkiem bez wskazanego wzorca identyfikatora. Zasadnym jest uzupełnienie załącznika nr 1 o pozycję „budynek” wraz ze wskazaniem rejestru zawierającego dane referencyjne i struktury identyfikatora (Baza Budynków i Lokali GUNB).	**Uwaga uwzględniona**
17.	**§ 5 ust. 4 i § 14 ust. 3**	**RCL**	mając na uwadze informacyjny charakter projektowanego § 5 ust. 4 rozporządzenia, zgodnie z którego wynika nakaz stosowania przepisów wydanych na podstawie art. 19 ust. 1 pkt 6–10 i ust. 1a, art. 24b ust. 4, art. 26 ust. 2 oraz art. 47b ust. 5 ustawy z dnia 17 maja 1989 r. – Prawo geodezyjne i kartograficzne (Dz. U. z 2024 r. poz. 1151, z późn. zm.) – projektowaną regulację należy usunąć z rozporządzenia, a ewentualną informację o wzajemnych relacjach przedmiotowego projektu i wskazanych aktów wykonawczych wydanych na podstawie ustawy z dnia 17 maja 1989 r. – Prawo geodezyjne i kartograficzne należy umieścić w uzasadnieniu projektu. Powyższa uwaga dotyczy także projektowanego § 14 ust. 3 rozporządzenia w zakresie zgodności z wymogami dostępności cyfrowej określonymi w ustawie z dnia 4 kwietnia 2019 r. o dostępności cyfrowej stron internetowych i	**Uwaga częściowo uwzględniona** **Wyjaśnienie** Z projektu usunięty został § 5 ust. 4. Paragraf 14 ust. 3 projektu rozporządzenia regulować ma wymogi dostępności cyfrowej dla wskazanych formatów plików określonych w załączniku nr 1 do rozporządzenia (zmiana numeracji załączników w projekcie). Wymogi dostępności wobec stron internetowych są określone w ustawie z dnia 4 kwietnia 2019 r. o dostępności cyfrowej stron internetowych i aplikacji mobilnych podmiotów publicznych. Przepisy przywołanego artykułu nie wprowadzają wyjątków od stosowania przepisów ww. ustawy

			aplikacji mobilnych podmiotów publicznych (Dz. U. z 2023 r. poz. 1440), z tym że ponownej analizy i wyjaśnienia wymaga wprowadzenie w przedmiotowym przepisie (w wyliczeniu) wyjątków od stosowania niektórych przepisów ww. ustawy – co, jak się wydaje, nie powinno następować aktem niższego rzędu;	w odniesieniu do stron internetowych oraz aplikacji mobilnych, które stanowią zakres przedmiotowy ustawy. Przepisy § 14 ust. 3 projektu rozporządzenia nakładają natomiast obowiązki stosowania dostępności cyfrowej wobec ww. plików w takim samym zakresie, jakie ustawa o dostępności cyfrowej nakłada na strony internetowe - lecz z wyłączeniem pozycji wymagań, które nie mają zastosowania do plików z załącznika nr 2 do rozporządzenia. Jak wskazuje uzasadnienie projektu KRI zgodnie z definicją z ustawy o informatyzacji „minimalne wymagania dla systemów teleinformatycznych” obejmują również wymagania, których spełnienie przez system teleinformatyczny używany do realizacji zadań publicznych zapewnia dostęp do danych udostępnianych za pomocą tego systemu. Dane te są udostępniane w plikach, których formaty określono w projekcie rozporządzenia. Sama zgodność plików z wymaganymi formatami nie gwarantuje jednak realnego dostępu do zawartych w nich danych. Aby odbiorca mógł faktycznie zapoznać się z treścią dokumentu, konieczne jest również zapewnienie dostępności cyfrowej takiego dokumentu. Brak ustanowienia w rozporządzeniu wymagań dotyczących dostępności cyfrowej dokumentów może prowadzić do sytuacji, w której urzędy - korzystając z poczty elektronicznej lub doręczeń elektronicznych - przekazują pisma w sposób zgodny formalnie, lecz niemożliwy do samodzielnego odczytania przez część obywateli. Dotyczy to także korespondencji między urzędami, ponieważ odbiorcą dokumentu w jednostce może być osoba potrzebująca dostępności cyfrowej do skutecznego odczytu treści.

				Wprowadzenie ust. 3 i 4 eliminuje to ryzyko, ponieważ wiąże minimalne wymagania nie tylko z formatami danych, lecz również z obowiązkiem zapewnienia dostępności cyfrowej, a więc faktycznego dostępu do danych dla wszystkich użytkowników - do czego zobowiązują minimalne wymagania dla systemów teleinformatycznych. Dla dokumentów zastosowano rozwiązanie analogiczne do wymagań wobec stron internetowych podmiotów publicznych.
18.	**§ 6 ust. 1**	**MRiRW**	**<u>Projektowane brzmienie § 6 ust. 1:</u>** „1. Podmiot prowadzący rejestr publiczny dokumentuje oraz standaryzuje procesy i reguły zarządzania danymi dla zbierania i aktualizacji danych w rejestrze publicznym. Reguły zarządzania danymi zawierają reguły kontroli, korekty, anonimizacji, wprowadzania i synchronizacji oraz integracji danych, których celem jest zapewnienie kompletności, spójności i jednolitości danych.” **<u>Proponowane brzmienie § 6 ust. 1:</u>** „1. Podmiot prowadzący rejestr publiczny dokumentuje oraz standaryzuje procesy i reguły zarządzania danymi dla zbierania i aktualizacji danych w rejestrze publicznym. Reguły zarządzania danymi zawierają reguły kontroli, korekty, wprowadzania, synchronizacji, integracji danych, których celem jest zapewnienie kompletności, spójności i jednolitości danych **oraz zasady anonimizacji lub pseudonimizacji danych osobowych, w przypadkach, gdy zastosowanie tych środków jest odpowiednie z uwagi na cele przetwarzania i ryzyko praw lub wolności osób, których dane dotyczą.”** Proponuje się doprecyzowanie kiedy i dla jakich danych anonimizacji lub pseudonimizacja powinna być stosowana. W projektowanym brzmieniu przepisu anonimizacja została wskazana jako jedna z reguł zarządzania danymi, bez uwzględnienia charakteru i celu przetwarzania danych oraz konieczności dokonania oceny, czy zastosowanie danego środka jest w konkretnym przypadku właściwe. Proponowane brzmienie pozwala na bardziej elastyczne i adekwatne podejście do przetwarzania danych osobowych, poprzez wskazanie zarówno anonimizacji, jak i pseudonimizacji, z uwzględnieniem celów	**Uwaga częściowo uwzględniona** **Wyjaśnienie** Zmieniono przepis na „Reguły zarządzania danymi zawierają reguły kontroli, korekty, anonimizacji lub pseudoanonimizacji, wprowadzania i synchronizacji oraz integracji danych, których celem jest zapewnienie kompletności, spójności i jednolitości danych.” Brak jest podstaw do doprecyzowania w rozporządzeniu, kiedy i dla jakich danych anonimizacji lub pseudonimizacja powinna być stosowana, ponieważ wynika to już przepisów dotyczących ochrony danych osobowych.

			przetwarzania oraz ryzyka dla praw i wolności osób, których dane dotyczą.	
19.	**§ 7**	**Minister – Koordynator Służb Specjalnych**	Pragnę także zwrócić uwagę na potrzebę uwzględnienia wymagań dotyczących wymiany danych, w szczególności w odniesieniu do kwestii zasad wymiany danych, skoncentrowanych na ograniczeniu ich zakresu do niezbędnego minimum oraz unikania w miarę możliwości kopiowania lub powielania danych. Tego rodzaju regulacja jest zawarta w § 13 obowiązującego rozporządzenia i stanowi, że: „§ 13. 1. Wymiana danych dokonywana pomiędzy rejestrami publicznymi obejmuje jedynie informacje niezbędne do prawidłowego funkcjonowania tych rejestrów. 2. Wymiana danych odbywa się przez bezpośrednie odwołanie się do danych referencyjnych przez rejestr inicjujący wymianę. 3. Jeśli wymiana danych w trybie, o którym mowa w ust. 2, jest niemożliwa lub znacznie utrudniona, dopuszcza się wymianę danych w innym trybie, w tym przez kopiowanie danych przez rejestr inicjujący wymianę. ". Regulacje przytoczone powyżej powinny znaleźć się również w projektowanym rozporządzeniu.	**Uwaga wyjaśniona** Treść dotychczasowego § 13 ust 1 rozporządzenia ws. KRI jest już zaadresowana przez przepis art. 15 ust. 1 ustawy o informatyzacji „ Podmiot prowadzący rejestr publiczny zapewnia podmiotowi publicznemu albo podmiotowi niebędącemu podmiotem publicznym, realizującym zadania publiczne na podstawie odrębnych przepisów albo na skutek powierzenia lub zlecenia przez podmiot publiczny ich realizacji, nieodpłatny dostęp do danych zgromadzonych w prowadzonym rejestrze, w zakresie niezbędnym do realizacji tych zadań.” Informacje niezbędne do funkcjonowania rejestrów to dane w zakresie niezbędnym do realizacji zadań publicznych. Zagadnienie wymiany danych pomiędzy rejestrami jest zaadresowane w szczególności przez § 12 ust. 1 projektowanego rozporządzenia „Podmiot realizujący zadania publiczne wyposaża system teleinformatyczny używany do realizacji zadań publicznych w interfejsy programistyczne aplikacji, zgodne ze specyfikacją, określoną w załączniku nr 5 do rozporządzenia.” - w połączeniu z przepisem art. 15 ust. 2 ustawy o informatyzacji „Dane, o których mowa w ust. 1, powinny być udostępniane za pomocą środków komunikacji elektronicznej i mogą być wykorzystane wyłącznie do realizacji zadań publicznych.” Ponadto w § 3 określono, że „4. Interoperacyjność na poziomie semantycznym osiągana jest przez: (…) 3) stosowanie przez podmiot realizujący zadania publiczne w rejestrach publicznych odwołań do rejestrów

				publicznych zawierających dane referencyjne w zakresie niezbędnym do realizacji zadań publicznych", co adresuje kwestię odwoływania się do danych referencyjnych w rejestrach publicznych. Ustawa o informatyzacji, a za nią projekt rozporządzenia, wskazują domyślne techniczne metody dostępu do danych rejestru publicznego prowadzonego przy pomocy systemu teleinformatycznego - poprzez API systemu teleinformatycznego, co jest konsekwencją stosowania określonego w rozporządzeniu modelu usługowego dla publicznych systemów teleinformatycznych. Zgodnie z § 10 ust. 2 projektowanego rozporządzenia w udokumentowanych przypadkach - uzasadnionych specyfiką podmiotu realizującego zadania publiczne lub świadczonych przez niego elektronicznych usług publicznych - podmiot może jednak stosować inny model architektury systemu teleinformatycznego, niż model usługowy. Może zatem zapewniać dostęp do danych rejestru publicznego w innym trybie, niż opisany powyżej, w szczególności w trybie kopiowania danych poza API. Zapisy ustawy o informatyzacji i projektowanego rozporządzenia skutkują brakiem uzasadnienia dla utrzymania przepisu z § 13 obecnie obowiązującego rozporządzenia ws. KRI. W związku z tym proponowane uzupełnienie nie jest konieczne.
20.	**§ 8 ust. 1**	**MFiG (MRiT)**	Rozliczalność każdego odczytu przy rejestrach o dużym wolumenie generuje zapisy audytowe wielokrotnie przewyższające sam rejestr. Wnosimy o zastosowanie zasady proporcjonalności (powiązanie zakresu z analizą ryzyka, jak w § 16 ust. 3) oraz doprecyzowanie,	**Uwaga uwzględniona** Rejestr publiczny jest zbiorem danych służącym do realizacji zadań publicznych i prowadzonym na podstawie przepisów ustawowych**.** Z tego względu jest źródłem danych publicznych o najwyższym stopniu zaufania, co skutkuje

			czy wymagany jest zapis każdego rekordu, czy operacji dostępu wraz z kryteriami.	wymogiem zapewnienia rozliczalności operacji na danych tego rejestru publicznego. Odpowiedź na uwagę została rozpatrzona łącznie z odpowiedzią na uwagę nr 21.
21.	**§ 8 ust. 1**	**MRiRW**	**<u>Projektowane brzmienie § 8 ust. 1:</u>** „1. Podmiot prowadzący rejestr publiczny przy użyciu systemu teleinformatycznego zapewnia rozliczalność wszystkich operacji na danych tego rejestru publicznego.” **<u>Proponowane brzmienie § 8 ust. 1:</u>** „1. Podmiot prowadzący rejestr publiczny przy użyciu systemu teleinformatycznego zapewnia rozliczalność operacji na danych rejestru publicznego w zakresie niezbędnym do ustalenia podmiotu lub procesu wykonującego operację, jej rodzaju oraz czasu wykonania, z uwzględnieniem charakteru danych oraz przepisów odrębnych.” W dużych rejestrach znaczna część operacji jest wykonywana automatycznie przez integracje, procesy wsadowe, mechanizmy synchronizacji, raportowania czy przetwarzania technicznego. Literalne rozumienie obowiązku rejestrowania wszystkich operacji może prowadzić do gromadzenia bardzo dużych ilości informacji technicznych, bez istotnego zwiększenia rozliczalności. Warto jednoznacznie wskazać cel i wymagany zakres takiego rejestrowania. Dlatego też proponuje się doprecyzowanie zakresu pojęcia „wszystkich operacji na danych rejestru publicznego”, w szczególności w odniesieniu do operacji technicznych i automatycznych.	**Uwaga uwzględniona** Pojęcie rozliczalności służy przede wszystkim zapewnieniu możliwości ustalenia: • kto (człowiek, system) wykonał działanie, • jakie działanie wykonano, • kiedy je wykonano, • ewentualnie na jakiej podstawie i z jakim skutkiem. Z tego względu wprowadzono następującą zmianę w przepisie projektu rozporządzenia „Podmiot prowadzący rejestr publiczny przy użyciu systemu teleinformatycznego zapewnia rozliczalność operacji na danych tego rejestru publicznego przez utrwalanie danych umożliwiających ustalenie podmiotu wykonującego operację, a w przypadku operacji wykonywanych automatycznie również systemu teleinformatycznego wykonującego operację, rodzaju operacji oraz czasu jej wykonania.”.
22.	**§ 8 ust. 1**	**MKiŚ**	Należy rozważyć ograniczenie zakresu obowiązku zapewnienia rozliczalności wszystkich operacji na danych rejestru publicznego albo uzależnienie zakresu rejestrowanych operacji od charakteru danych, rodzaju operacji i analizy ryzyka. Objęcie obowiązkiem wszystkich operacji, w tym masowych i automatycznych odczytów realizowanych za pośrednictwem API, może prowadzić do generowania bardzo dużych wolumenów logów oraz istotnego wzrostu zapotrzebowania na zasoby infrastrukturalne potrzebne do ich przechowywania i analizy.	**Uwaga częściowo uwzględniona** Wyjaśnienie podano w odpowiedzi na uwagę nr 21.
23.	**§ 8 ust. 2**	**MFiG (MRIT)**	Daty utworzenia rekordów historycznych często nie da się wiarygodnie odtworzyć. Treść Rozporządzenia powinna definiować ograniczenie obowiązku do rekordów tworzonych i modyfikowanych po dniu dostosowania rejestru.	**Uwaga uwzględniona/wyjaśniona** Projekt nie nakłada obowiązku odtwarzania informacji, które nie są dostępne w rejestrze publicznym. W związku z tym brak jest potrzeby wprowadzania dodatkowego wyłączenia

				obejmującego rekordy utworzone przed dostosowaniem rejestru do wymagań rozporządzenia. Jednakże w celu uniknięcia wątpliwości interpretacyjnych do uzasadnienia zostało dodane następujące zdanie: „Wymagania, o którym mowa w § 8, związane z oznaczaniem rekordów i danych w rejestrze publicznym datą i czasem ich utworzenia oraz datą i czasem ich modyfikacji lub usunięcia, dotyczą danych i rekordów w rejestrze publicznym utworzonych po wejściu w życie obowiązków związanych z minimalnymi wymaganiami dla rejestrów publicznych, wynikających z ustawy o informatyzacji, w stosunku do podmiotów zobowiązanych do ich realizacji."
24.	**§ 8 ust. 2**	**MFiG (MRiT)**	MRiT proponuje - co koresponduje z ust. 1 gdzie podmiot zapewnia rozliczalność wszystkich operacji na danych prowadzonego rejestru publicznego - uzupełnić ust. 2 dodając słowa 'lub - o ile dotyczy - ich usunięcia'. Propozycja doprecyzuje wymóg rozliczalności z ust. 1 (jednocześnie nie wskazuje na obowiązek przechowywania usuniętych danych) poprzez zapewnienie możliwości ustalenia daty i czasu usunięcia rekordu lub danych, jeżeli taka operacja jest przewidywana i wykonalna w danym rejestrze. Usunięcie, podobnie jak utworzenie i modyfikacja stanowi operację na danych, która powinna być możliwa do odtworzenia w ramach historii operacji np. na potrzeby audytu. Propozycja zapisu: 2. Podmiot prowadzący rejestr publiczny przy użyciu systemu teleinformatycznego zapewnia, że rekordy lub dane w rejestrze publicznym są oznaczane datą i czasem ich utworzenia oraz modyfikacji lub - o ile dotyczy - ich usunięcia.	**Uwaga uwzględniona**
25.	**§ 8 ust. 3**	**MFiG (MRiT)**	Pojęcie „czasu rzeczywistego" nie jest zdefiniowane. Należy wskazać dopuszczalne opóźnienia albo określić wymaganie funkcjonalne oraz wyraźnie wskazać, których rejestrów dotyczy.	**Uwaga uwzględniona** W praktyce architektury systemów teleinformatycznych „informowanie w czasie rzeczywistym" jest zwykle rozumiane jako bez

				celowego opóźnienia, automatycznie po wystąpieniu zdarzenia. Przepis dotyczy rejestrów publicznych właściwych dla danych referencyjnych, w zakresie tych danych. Wskutek zgłoszonej uwagi wprowadzono jednak zmianę z „w czasie rzeczywistym” na „niezwłocznie po dokonaniu zmiany”.
26.	**§ 8 ust. 3**	**MRiRW**	Proponuje się doprecyzowanie pojęcia „w czasie rzeczywistym”. Proponowane brzmienie: „(...) zapewnia mechanizmy informowania o zmianach danych referencyjnych bez zbędnej zwłoki, w czasie odpowiednim do charakteru danych i wymagań procesów korzystających z tych danych.” Określenie „w czasie rzeczywistym” nie wskazuje mierzalnego parametru i może być różnie interpretowane. W zależności od charakteru danych wymagany czas propagacji zmiany może być różny. Obecne brzmienie może również sugerować konieczność stosowania mechanizmów zdarzeniowych nawet wtedy, gdy aktualizacja danych z niewielkim opóźnieniem jest wystarczająca dla realizowanego zadania publicznego.	**Uwaga uwzględniona** Wyjaśnienie udzielono na odpowiedzi na uwagę nr 25.
27.	**§ 8 ust. 3**	**MRiRW**	„3. Dla danych referencyjnych przetwarzanych w rejestrze publicznym, prowadzonym przy użyciu systemu teleinformatycznego, podmiot prowadzący ten rejestr zapewnia mechanizmy informowania o zmianach danych referencyjnych w czasie rzeczywistym **z uwzględnieniem zasad ochrony danych osobowych, w przypadku gdy dane te stanowią dane osobowe,** przy pomocy interfejsów programistycznych aplikacji systemów teleinformatycznych, przy użyciu których zapewniany jest dostęp do rejestru publicznego.” Przekazany do zaopiniowania przepis nie określa: komu dane mogą być przekazywane, jakie dane mogą być przekazywane oraz czy wszystkie zmiany podlegają ogłoszeniu, dlatego też zostało dodane ogólna sformułowanie: „z uwzględnieniem zasad ochrony danych osobowych, w przypadku gdy dane te stanowią dane osobowe”	**Uwaga wyjaśniona** Przetwarzanie danych osobowych w związku z prowadzeniem rejestrów publicznych podlega przepisom o ochronie danych osobowych niezależnie od ich wyraźnego przywołania w projektowanym przepisie. Projektowany § 8 ust. 3 określa obowiązek zapewnienia mechanizmów informowania o zmianach danych referencyjnych i nie stanowi samodzielnej podstawy prawnej do udostępniania danych. Zakres, cele oraz zasady przetwarzania danych wynikają z przepisów regulujących prowadzenie poszczególnych rejestrów publicznych oraz z przepisów o ochronie danych osobowych. Dodanie proponowanego zastrzeżenia jest zatem zbędne i prowadziłoby do powtórzenia norm obowiązujących na podstawie przepisów odrębnych, co nie jest zgodne z Zasadami techniki prawodawczej.

28.	**§ 8 ust. 3**	**MKiŚ**	W świetle wskazanego w przedmiotowym przepisie sformułowania „w czasie rzeczywistym” nie jest jasne, czy wystarczające jest udostępnienie aktualnego stanu danych przez API, czy też wymagany jest mechanizm aktywnego powiadamiania odbiorców, np. subskrypcja lub mechanizm push.	**Uwaga wyjaśniona** Zastosowane rozwiązanie powinno być podyktowane specyfiką systemów teleinformatycznych służących do udostępniania danych rejestru publicznego, a także zdiagnozowanymi potrzebami i możliwościami uprawnionych odbiorców danych. Przepis określa wymagany rezultat, a nie sposób jego osiągnięcia. Dobór rozwiązań technicznych, w tym wykorzystanie mechanizmów API, subskrypcji, powiadomień lub innych środków, pozostawiono podmiotowi prowadzącemu rejestr publiczny.
29.	**§ 8 ust. 3 + zał. Nr 5**	**MFiG (MF)**	w opinii MF – Elastyczny model synchronizacji danych – zastąpienie obligatoryjnego „czasu rzeczywistego” wymogiem zapewnienia odpowiedniej aktualności danych oraz dopuszczenie mechanizmów synchronicznych i asynchronicznych.	**Uwaga wyjaśniona** Wyjaśnienie udzielono w odpowiedzi na uwagę nr 25.
30.	**§ 10 ust. 1 i 2**	**MRiRW**	Proponuje się doprecyzowanie, że wymaganie dotyczące modelu usługowego odnosi się do sposobu udostępniania funkcjonalności systemu, a nie do jego całej wewnętrznej architektury. Proponowane brzmienie: „W zakresie funkcjonalności udostępnianych innym systemom teleinformatycznym stosuje się rozwiązania oparte na modelu usługowym.” Systemy wykorzystywane do realizacji zadań publicznych mają różną architekturę i przeznaczenie. W przypadku części systemów, w szczególności rozwiązań istniejących od wielu lat, systemów analitycznych lub przetwarzających dane wsadowo, wymaganie stosowania SOA jako modelu całego systemu może być nieadekwatne. Dla zapewnienia interoperacyjności istotniejszy jest sposób udostępniania funkcji i danych na styku z innymi systemami. Poza tym aktualne brzmienie przepisu wskazuje na konkretny model architektoniczny, co może być postrzegane jako ograniczenie zasady neutralności technologicznej. W praktyce współczesne systemy teleinformatyczne wykorzystują również architektury mikroserwisowe, zdarzeniowe oraz rozwiązania chmurowe zapewniające ten sam cel interoperacyjności.	**Uwaga wyjaśniona** Na propozycję zgłoszoną przez wnioskodawcę odpowiada już § 10 ust. 2 projektu rozporządzenia, który pozwala na stosowanie – w uzasadnionych przypadkach - modelu architektury systemu teleinformatycznego innego, niż model usługowy. Neutralność technologiczna to zasada równego traktowania przez władze publiczne technologii teleinformatycznych i tworzenia warunków do ich uczciwej konkurencji, w tym zapobiegania możliwości eliminacji technologii konkurencyjnych przy rozbudowie i modyfikacji eksploatowanych systemów teleinformatycznych lub przy tworzeniu konkurencyjnych produktów i rozwiązań. Model architektury systemu teleinformatycznego nie jest technologią teleinformatyczną. Dodatkowe wyjaśnienie znajduje się w odpowiedzi na uwagę 31.
31.	**§ 10 ust. 2**	**RCL**	niejasny pozostaje projektowany § 10 ust. 2 rozporządzenia, zgodnie z którym w uzasadnionych przypadkach dopuszcza się	**Uwaga wyjaśniona**

			„inny model architektury systemu teleinformatycznego”. Zaznaczyć należy, że przepis § 2 pkt 9 projektu definiuje jedynie pojęcie „modelu usługowego” architektury, a zawarta w § 2 pkt 1 projektu definicja „architektury systemu teleinformatycznego” nie wskazuje na rodzaje „modeli” tej architektury – przepis § 10 ust. 2 wymaga więc wyjaśnienia i ewentualnie doprecyzowania;	Zgodnie z definicją "model usługowy" to "model architektury systemu teleinformatycznego, w którym zdefiniowano, stanowiące odrębną całość, funkcje systemu teleinformatycznego oraz opisano sposób korzystania z tych funkcji przy pomocy interfejsów programistycznych aplikacji, zgodnie z architekturą zorientowaną na usługi (ang. Service Oriented Architecture, SOA)". W informatyce występują także inne modele architektury systemu teleinformatycznego, niż model usługowy. Przykładowo systemy teleinformatyczne mogą być projektowane i budowane w oparciu o model mikrousługowy, model komponentowy, model warstwowy, model zdarzeniowy, model procesowy, model zorientowany na dane i inne. Z biegiem czasu powstają także inne modele. Ze względu na zróżnicowaną perspektywę na system teleinformatyczny modele te nie są możliwe do łącznego scharakteryzowania. Część z nich kładzie nacisk na strukturę systemu, część na sposób integracji a inne na główne obiekty modelowania. Jednak w celu zaadresowania zgłoszonej uwagi uzupełniono przepis § 10 ust. 2: "W udokumentowanych przypadkach uzasadnionych specyfiką podmiotu realizującego zadania publiczne lub świadczonych przez niego elektronicznych usług publicznych dopuszcza się inny model architektury systemu teleinformatycznego, niż model usługowy."
32.	**§ 10**	**MRiRW**	**Projektowane brzmienie § 10 ust. 1:** „1. Dla systemów teleinformatycznych używanych do realizacji zadań publicznych stosuje się rozwiązania oparte na modelu usługowym.” **Proponowane brzmienie:** „1. Dla nowo projektowanych i wdrażanych systemów teleinformatycznych używanych do realizacji zadań publicznych stosuje się rozwiązania oparte na modelu usługowym.	**Uwaga wyjaśniona** Przepis dotyczący stosowania modelu usługowego dla publicznych systemów teleinformatycznych obowiązuje od 2012 roku. Został określony w rozporządzeniu 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

			1a. W przypadku systemów istniejących obowiązek dostosowania do modelu usługowego stosuje się przy ich istotnej przebudowie, modernizacji lub wymianie, o ile dostosowanie jest technicznie możliwe i ekonomicznie uzasadnione.” Proponowany wymóg modelu usługowego jest racjonalny dla systemów budowanych po wejściu w życie projektowanego rozporządzenia, natomiast jego automatyczne zastosowanie do istniejących systemów może oznaczać konieczność przebudowy całej architektury systemu. W ARiMR funkcjonują systemy projektowane wiele lat temu, często dostarczane jako rozwiązania monolityczne, których przebudowa do modelu usługowego może być kosztowniejsza niż ich stopniowa wymiana.	minimalnych wymagań dla systemów teleinformatycznych (Dz.U. z 2012 r. poz. 526). Natomiast zgodnie z § 10 ust. 2 projektu rozporządzenia w udokumentowanych przypadkach uzasadnionych specyfiką podmiotu realizującego zadania publiczne lub świadczonych przez niego elektronicznych usług publicznych dopuszcza się inny model architektury systemu teleinformatycznego, niż model usługowy.
33.	**§ 11 ust. 1**	**MI**	Wnoszę o zmianę § 11 ust. 1 w brzmieniu: „1. Systemy teleinformatyczne używane do realizacji zadań publicznych projektuje się, wdraża oraz eksploatuje w sposób zapewniający ich funkcjonalność, niezawodność, użyteczność, wydajność, przenoszalność i pielęgnowalność niezbędne do realizacji zadań publicznych, przy zastosowaniu norm oraz uznanych w obrocie profesjonalnym standardów i metodyk, z uwzględnieniem analizy ryzyka cyberbezpieczeństwa.”. Projekt rozporządzenia określa wymagania dotyczące projektowania architektury systemów teleinformatycznych, jednak nie odnosi się on do konieczności uwzględniania bezpieczeństwa już na etapie projektowania i rozwoju systemów. Tymczasem podejście takie stanowi jeden z podstawowych kierunków europejskiej polityki cyberbezpieczeństwa. Dyrektywa Parlamentu Europejskiego i Rady (UE) 2022/2555 z dnia 14 grudnia 2022 r. w sprawie środków na rzecz wysokiego wspólnego poziomu cyberbezpieczeństwa na terytorium Unii, zmieniająca rozporządzenie (UE) nr 910/2014 i dyrektywę (UE) 2018/1972 oraz uchylająca dyrektywę (UE) 2016/1148 (dyrektywa NIS 2) zobowiązuje podmioty kluczowe i ważne do stosowania odpowiednich oraz proporcjonalnych środków technicznych, operacyjnych i organizacyjnych opartych na analizie ryzyka, obejmujących cały cykl życia systemów informacyjnych. Analogiczne wymagania wynikają z Rozporządzenia Parlamentu Europejskiego i Rady (UE) 2024/2847 z dnia 23 października 2024 r. w sprawie horyzontalnych wymagań w zakresie cyberbezpieczeństwa w odniesieniu do produktów z elementami	**Uwaga wyjaśniona** Podmioty realizujące zadania publiczne uznane za podmioty kluczowe lub ważne w rozumieniu ustawy z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa (Dz. U. z 2026 r. poz. 20, z późn. zm.) są zobowiązanie na mocy tych przepisów ustawowych do wdrożenia systemu zarządzania bezpieczeństwem informacji w systemie informacyjnym wykorzystywanym w procesach wpływających na świadczenie usługi przez te podmioty.

			cyfrowymi oraz w sprawie zmiany rozporządzeń (UE) nr 168/2013 i (UE) 2019/1020 i dyrektywy (UE) 2020/1828 (akt o cyberodporności) (Cyber Resilience Act), zgodnie z którym produkty z elementami cyfrowymi powinny być projektowane z uwzględnieniem bezpieczeństwa przez cały okres ich eksploatacji. Z kolei ustawa z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa (Dz. U. z 2026 r. poz. 20, z późn.zm.) w art. 2 pkt 19 definiuje zarządzanie ryzykiem jako skoordynowane działania w zakresie cyberbezpieczeństwa odnoszące się do całego systemu informacyjnego oraz w art. 3 wskazuje, że celem krajowego systemu cyberbezpieczeństwa jest zapewnienie odpowiedniego poziomu bezpieczeństwa systemów informacyjnych. Uzupełnienie przepisu pozwoli zachować spójność pomiędzy Krajowymi Ramami Interoperacyjności a ustawą z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa oraz zapewni zgodność z wymaganiami normy ISO/IEC 27001:2022, która wymaga uwzględnienia bezpieczeństwa na etapie projektowania i zarządzania zmianą. Biorąc pod uwagę powyższe proponuję w § 11 ust. 1 po wyrazach: „uznanych w obrocie profesjonalnym standardów i metodyk” dodać wyrazy: „z uwzględnieniem analizy ryzyka cyberbezpieczeństwa.”	
34.	**§ 11 ust. 1**	**MRIRW**	**<u>Projektowane brzmienie § 11 ust. 1:</u>** „1. Systemy teleinformatyczne (...) projektuje się, wdraża oraz eksploatuje w sposób zapewniający ich funkcjonalność, niezawodność, użyteczność, wydajność, przenoszalność i pielęgnowalność (...).” **<u>Proponowane brzmienie § 11 ust. 1:</u>** „1. Systemy teleinformatyczne (...) projektuje się, wdraża oraz eksploatuje w sposób zapewniający ich funkcjonalność, niezawodność, użyteczność, wydajność, przenoszalność i modyfikowalność (...).”. Zmiana ma charakter dostosowujący do proponowanej zmiany § 2 pkt 14 i zapewnia spójność terminologiczną rozporządzenia.	**Uwaga wyjaśniona** Wyjaśnienie znajduje się w odpowiedzi na uwagę nr 5.
35.	**§ 11 (zmiana poprzez dodanie kolejnej**	**MRiRW**	W § 11 proponuję dodanie kolejnego ustępu w brzmieniu: „3a. Wymagania uznaje się za spełnione, jeżeli podmiot wdrożył i stosuje udokumentowane procesy odpowiadające zakresowi wymagań określonych w normach, o których mowa w ust. 3”. Projektowany przepis wymaga doprecyzowania w zakresie tego,	**Uwaga wyjaśniona** Projekt rozporządzenia nie zakłada obowiązku uzyskania certyfikacji zgodności z żadną z norm przywołanych w rozporządzeniu.

	jednostki redakcyjnej)		czy jego celem jest stosowanie wymagań określonych w odpowiednich normach, czy też uzyskanie formalnej certyfikacji zgodności z tymi normami. Proponowane dodanie ust. 3a jednoznacznie wskazuje, że spełnienie wymagań dotyczących zarządzania usługami nie wymaga uzyskania certyfikacji zgodności z normą ISO/IEC 20000-1 ani ISO/IEC 20000-2.	
36.	**§ 11 ust. 1**	**Minister – Koordynator Służb Specjalnych**	Dodatkowo w ww. zakresie postuluję rozszerzenie projektowanego § 11 poprzez wskazanie, że cechy systemów teleinformatycznych, w tym „funkcjonalność", mają służyć realizacji potrzeb wszystkich interesariuszy, w szczególności w zakresie „zapewnienia podmiotom uprawnionym do realizacji zadań wynikających z odrębnych przepisów". W związku z powyższym proponuję nadanie § 11 ust. 1 projektu rozporządzenia następującego brzmienia: „§ 11. 1. Systemy teleinformatyczne używane do realizacji zadań publicznych projektuje się, wdraża oraz eksploatuje w sposób zapewniający ich funkcjonalność, niezawodność, użyteczność, wydajność, przenoszalność i pielęgnowalność niezbędne do realizacji zadań publicznych oraz zapewnienia podmiotom uprawnionym realizacji zadań wynikających z odrębnych przepisów, przy zastosowaniu norm oraz uznanych w obrocie profesjonalnym standardów i metodyk.". Jednocześnie wynikiem przyjęcia powyższej uwagi powinna być również zmiana w § 2 projektowanego rozporządzenia polegająca na dodaniu definicji pojęcia „funkcjonalność" systemów teleinformatycznych, analogicznie jak w przypadku innych cech systemów teleinformatycznych wymienionych w § 11 ust. 1 projektu rozporządzenia.	**Uwaga częściowo uwzględniona** Projektowany § 11 określa ogólne wymagania dotyczące systemów teleinformatycznych używanych do realizacji zadań publicznych. Wskazane w przepisie cechy, takie jak przydatność funkcjonalna, niezawodność, użyteczność, wydajność, przenoszalność i pielęgnowalność, odnoszą się do sposobu projektowania, wdrażania i eksploatacji systemów teleinformatycznych oraz mają zapewnić możliwość skutecznej realizacji zadań publicznych. Proponowane uzupełnienie przepisu o odwołanie do „zapewnienia podmiotom uprawnionym realizacji zadań wynikających z odrębnych przepisów" nie jest konieczne. Uprawnienia poszczególnych podmiotów do dostępu do danych, korzystania z systemów teleinformatycznych lub realizacji określonych czynności wynikają bowiem z przepisów szczególnych. To te przepisy określają zakres zadań realizowanych przez poszczególne podmioty oraz związane z nimi obowiązki i uprawnienia, a także wprowadzają wymagania w zakresie odpowiedniego dostosowania publicznych systemów teleinformatycznych. Podmioty realizujące zadania publiczne tworzą co do zasady systemy teleinformatyczne służące realizacji ich zadań publicznych. Uwzględnienie wymogu „zapewnienia podmiotom uprawnionym realizacji zadań wynikających z odrębnych przepisów" wymagałoby od podmiotu

				projektującego, wdrażającego oraz eksploatującego system teleinformatyczny przeglądu przepisów prawa, nakładających obowiązki na wszystkie inne podmioty i uwzględnienie ich w procesie projektowania systemu, co jest niewykonalne. Podmiot powinien zaprojektować system do realizacji swojego zadania publicznego oraz udostępniać z niego dane z użyciem mechanizmów określonych w przepisach ustawy o informatyzacji lub innych ustaw. Dodano definicję „przydatności funkcjonalnej" systemu teleinformatycznego (pochodzącej z ISO/IEC 25010) do słowniczka pojęć rozporządzenia.
37.	**§ 11 ust. 1-3**	**Minister – Koordynator Służb Specjalnych**	Ponadto w projekcie rozporządzenia doprecyzowania wymagają zagadnienia dotyczące obszaru cyberbezpieczeństwa. gdyż projektowane regulacje pomijają wymagania dotyczące obowiązku wdrożenia systemu zarządzenia bezpieczeństwem informacji. W tym zakresie proponuję rozważenie uzupełnienia projektowanych regulacji dotyczących zarządzania usługami (§ 11 ust. 1-3 projektu rozporządzenia) oraz zarządzania ciągłością działania (§ 11 ust. 4-8 projektu rozporządzenia) poprzez sformułowanie przepisu odsyłającego do przepisów zawartych np. w art. 8 ustawy z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa (Dz. U. z 2026 r. poz. 20, z późn. zm.), który reguluje tego rodzaju kwestie. Jednocześnie projektowane rozporządzenie powinno również wskazywać na obowiązek spełniania przez systemy teleinformatyczne obowiązków wynikających z ww. ustawy.	**Uwaga wyjaśniona** Projekt rozporządzenia, zgodnie z upoważnieniem ustawowym, zawartym w art. 18ustawy z dnia 17 lutego 2005 r. o informatyzacji działalności podmiotów realizujących zadania publiczne, reguluje wyłącznie szczegółowe sposoby realizacji obowiązków wynikających z przepisów ustawowych, tj. art. 13 ust. 1 pkt 1 i 2 oraz art. 14 ust. 1 ustawy o informatyzacji. Treść rozporządzenia bezpośrednio nie wpływa na treść obowiązków wynikających z przepisów innych ustaw, w tym ustawy z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa.
38.	**§ 11 ust. 3**	**MI**	Zgodnie z § 11 ust. 3 projektu rozporządzenia, wymagania określone w ust. 1 i 2 uznaje się za spełnione, jeśli projektowanie, wdrażanie, eksploatowanie, monitorowanie, przeglądanie, utrzymanie i udoskonalanie zarządzania usługami systemów teleinformatycznych odbywają się w oparciu o normy ISO/IEC 20000-1 i ISO/IEC 20000 2. Należy stwierdzić, że przywołane normy referencyjne, tj. ISO/IEC 20000-1 oraz ISO/IEC 20000-2, w wykazie norm Polskiego Komitetu Normalizacyjnego występują	**Uwaga wyjaśniona** Normy ISO/IEC 20000-1 oraz ISO/IEC 20000-2 są normami obowiązującymi. Wycofane zostały polskie wersje tych norm, tj. PN-ISO/IEC 20000-1 oraz PN-ISO/IEC 20000-2.

			jako normy wycofane (https://www.gov.pl/web/ia/standardy-krajowych-ram interoperacyjnoscikri). Tym samym zasadne jest wskazanie, która edycja normy wyszczególniona w projekcie rozporządzenia jest aktualnie obowiązująca (np.: PN-EN ISO/IEC20000-1:2018-10 oraz ISO/IEC 20000-2:2019).	
39.	**§ 11 ust. 5 pkt 1**	**MI**	Wnoszę o zmianę § 11 ust. 5 pkt 1 w brzmieniu: „5. Przy tworzeniu planu ciągłości świadczenia oraz planu przywracania po awarii, o których mowa w ust. 4, uwzględnia się: 1) wyniki przeprowadzonych analiz ryzyka, w tym ryzyka wynikającego z incydentów cyberbezpieczeństwa oraz zagrożeń dla bezpieczeństwa systemów teleinformatycznych;”. Projekt rozporządzenia przewiduje obowiązek uwzględniania wyników analiz ryzyka przy opracowywaniu planów ciągłości działania, jednak nie wskazuje wprost ryzyk wynikających z incydentów cyberbezpieczeństwa. Uzupełnienie w tym zakresie jest istotne, ponieważ ustawa z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa w art. 2 pkt 8 i 18 definiuje incydent oraz zarządzanie incydentem jako podstawowe elementy zapewnienia bezpieczeństwa systemów informacyjnych. Ponadto dyrektywa NIS2 oraz dyrektywa Parlamentu Europejskiego i Rady (UE) 2022/2557 z dnia 14 grudnia 2022 r. w sprawie odporności podmiotów krytycznych i uchylająca dyrektywę Rady 2008/114/WE wskazują konieczność uwzględniania zagrożeń cyfrowych i hybrydowych przy zapewnianiu odporności podmiotów krytycznych. Z kolei norma ISO 22301 wymaga identyfikacji wszystkich zagrożeń mogących zakłócić realizację procesów biznesowych. Mając powyższe na uwadze proponuję w § 11 ust. 5 pkt 1 po wyrazach: „wyniki przeprowadzonych analiz ryzyka” dodać wyrażenie w brzmieniu: „w tym ryzyka wynikającego z incydentów cyberbezpieczeństwa oraz zagrożeń dla bezpieczeństwa systemów informacyjnych.”	**Uwaga wyjaśniona** Wyjaśnienie znajduje się w odpowiedzi na uwagę nr 33.
40.	**§ 11 ust. 5 pkt 2**	**MFiG (MF)**	po wyrazie realizacji występuje przecinek i średnik - proponuje się usunąć przecinek	**Uwaga uwzględniona**
41.	**§ 12**	**MI**	Projekt rozporządzenia nie wskazuje jednoznacznie, czy obowiązek udostępniania danych przez API obejmuje wszystkie dane prezentowane publicznie przez system teleinformatyczny, czy jedynie dane rejestrów publicznych oraz dane niezbędne do realizacji interoperacyjności pomiędzy podmiotami publicznymi. Portale informacyjne zawierają również	**Uwaga wyjaśniona** Zgodnie z art. 13 ust. 5 ustawy o informatyzacji podmiot realizujący zadania publiczne przygotowuje i publikuje w repozytorium interoperacyjności określone w ustawie informacje o API systemu teleinformatycznego

			dane przetworzone, wizualizacje, produkty eksperckie, analizy i prezentacje danych źródłowych. Nie jest jasne, czy wszystkie te elementy miałyby podlegać obowiązkowi udostępniania poprzez API. Przedmiotowa kwestia wymaga jednoznacznego uregulowania w projekcie rozporządzenia albo wyjaśnienia w uzasadnieniu.	używanego do realizacji zadań publicznych. Udostępnianie interfejsów programistycznych aplikacji oraz informacji o nich ma służyć osiąganiu interoperacyjności. Obejmuje to w szczególności dane z rejestrów publicznych oraz inne dane służące realizacji zadań publicznych. Jak podano w uzasadnieniu do ustawy: „W repozytorium interoperacyjności będą udostępniane informacje dotyczące wykorzystywanych przez podmioty realizujące zadania publiczne API publicznych, tj. dostępnych dla wszystkich, oraz API partnerskich, tj. udostępnianych podmiotom, które mogą wykazać istnienie interesu prawnego lub faktycznego w dostępie do API. W repozytorium interoperacyjności nie będą publikowane informacje o API prywatnych, tj. wykorzystywanych wewnętrznie w ramach jednego podmiotu realizującego zadania publiczne. W przypadku braku udostępnienia wymaganych, wskazanych w przepisie, informacji podmiot realizujący zadania publiczne będzie obowiązany wskazać podstawę prawną, z której wynika obowiązek zachowania niejawności takich informacji.”
42.	**§ 12**	**Minister – Koordynator Służb Specjalnych**	W związku z faktem, że konieczność wydania przedmiotowego rozporządzenia wynika ze zmian wprowadzonych ustawą z dnia 25 lipca 2025 r. o zmianie ustawy o informatyzacji działalności podmiotów realizujących zadania publiczne oraz niektórych innych ustaw (Dz. U. poz. 1158) zasadne wydaje się utrzymanie niektórych regulacji zawartych w obecnie obowiązującym rozporządzeniu Rady Ministrów z dnia 21 maja 2024 r. w sprawie Krajowych Ram Interoperacyjności. minimalnych wymagań dla rejestrów publicznych i wymiany informacji w postaci elektronicznej oraz minimalnych wymagań dla systemów teleinformatycznych (Dz. U. poz. 773), a które zostały pominięte w przedmiotowym projekcie. W związku z powyższym proponuję	**Uwaga wyjaśniona** Wyjaśnienie znajduje się w odpowiedzi na uwagę nr 36.

			wprowadzenie do projektu rozporządzenia regulacji analogicznych do tych zawartych w § 12 obowiązującego rozporządzenia, które stanowią, że określając funkcjonalność rejestrów publicznych oraz systemów teleinformatycznych, uwzględnia się potrzebę zapewnienia podmiotom uprawnionym realizacji zadań wynikających z odrębnych przepisów. Przedmiotowa regulacja w kontekście zadań realizowanych przez służby specjalne ma kluczowe znaczenie i stanowi prawną możliwość do wprowadzania w systemach teleinformatycznych niestandardowych funkcjonalności wychodzących naprzeciw ich potrzebom.	
43.	**§ 12 ust. 1**	**MRiRW**	Proponuje się doprecyzowanie, że API systemu może być zapewnione również za pośrednictwem wspólnej warstwy integracyjnej lub wyspecjalizowanego komponentu udostępniającego API. W dużych środowiskach teleinformatycznych funkcje integracyjne są często centralizowane. System źródłowy nie musi w takim przypadku samodzielnie wystawiać API na zewnątrz - dostęp może być realizowany przez warstwę integracyjną lub bramę API. Doprecyzowanie tej możliwości pozwoli uniknąć interpretacji prowadzącej do konieczności wyposażania każdego systemu w odrębny mechanizm publikacji API.	**Uwaga wyjaśniona** Zgodnie z ustawą z dnia 11 sierpnia 2021 r. o otwartych danych i ponownym wykorzystywaniu informacji sektora publicznego (Dz.U. z 2023 r. poz. 1524) interfejs programistyczny aplikacji (API) oznacza „zbiór technicznych funkcji umożliwiających połączenie i wzajemną wymianę danych lub metadanych między programami komputerowymi lub systemami teleinformatycznymi”. Z kolei art. 13 ust. 5 ustawy z dnia 17 lutego 2005 r. o informatyzacji działalności podmiotów realizujących zadania publiczne nakłada obowiązek przygotowania informacji o API systemu teleinformatycznego używanego do realizacji zadań publicznych. Natomiast § 12 ust. 1 projektowanego rozporządzenia stanowi, że „Podmiot realizujący zadania publiczne wyposaża system teleinformatyczny używany do realizacji zadań publicznych w interfejsy programistyczne aplikacji, zgodne ze specyfikacją, określoną w załączniku nr 4 do rozporządzenia.” W związku z powyższym API systemu teleinformatycznego może być zapewnione za pośrednictwem wspólnej warstwy integracyjnej lub wyspecjalizowanego komponentu udostępniającego API, o ile będą one spełniać

				powyższe wymagania, w tym w zakresie zgodności ze specyfikacją określoną w załączniku nr 4 do rozporządzenia. Uzasadnienie projektu rozporządzenia zostanie uzupełnione o ww. wyjaśnienie.
44.	**§ 12 ust. 1**	**MI**	Należy jednoznacznie dopuścić możliwość realizacji wymagań rozporządzenia z wykorzystaniem istniejących interfejsów API, o ile zapewniają one interoperacyjność, bezpieczeństwo i udokumentowany dostęp do danych. Podmioty publiczne, w tym IMGW-PIB, posiadają już funkcjonujące i wykorzystywane przez odbiorców API REST/JSON. Projekt nie powinien wymuszać budowy nowych interfejsów wyłącznie z powodów formalnych, jeśli istniejące rozwiązania spełniają cele interoperacyjności (w tym określone w niniejszym rozporządzeniu).	**Uwaga wyjaśniona** Zgodnie z art. 13 ustawy z dnia 17 lutego 2005 r. o informatyzacji działalności podmiotów realizujących zadania publiczne, który wchodzi w życie z dniem 23.02.2027 r.: „1. Podmiot realizujący zadania publiczne używa do ich realizacji systemów teleinformatycznych: 1) spełniających minimalne wymagania dla systemów teleinformatycznych używanych do realizacji zadań publicznych i wymiany danych z podmiotami publicznymi: (...) b) określających model architektury oraz specyfikacje interfejsu programistycznego aplikacji, zwanego dalej „API”, tych systemów,(...)". Oznacza to, że publiczne systemy teleinformatyczne muszą być wyposażone w API zgodne ze specyfikacją interfejsu programistycznego aplikacji określoną w rozporządzeniu. Celem projektowanych przepisów jest zapewnienie jednolitego sposobu projektowania, dokumentowania i udostępniania interfejsów programistycznych aplikacji publicznych systemów teleinformatycznych. Nie jest natomiast zasadne wprowadzenie ogólnego odstępstwa pozwalającego na stosowanie dowolnych istniejących API wyłącznie na podstawie subiektywnej oceny, że zapewniają one interoperacyjność,

				bezpieczeństwo i udokumentowany dostęp do danych. Takie rozwiązanie prowadziłoby do utrzymania zróżnicowanych sposobów projektowania i dokumentowania interfejsów w administracji publicznej, ograniczając osiągnięcie celu regulacji ustawowej. Celem projektowanych przepisów jest bowiem nie tylko zapewnienie dostępu do danych, ale również ujednolicenie sposobu udostępniania tych danych przez publiczne systemy teleinformatyczne.
45.	**§ 12 ust. 1, zał. nr 5**	**MFiG (MRiT)**	Prosimy o doprecyzowanie, że wymagania dotyczą interfejsów udostępnianych podmiotom zewnętrznym, a nie interfejsów wewnętrznych między komponentami systemu. W architekturze mikroserwisowej objęcie ich wymogami subdomeny „api", HATEOAS czy OIDC byłoby nieproporcjonalne.	**Uwaga wyjaśniona** Wymagania dotyczą API publicznych oraz API partnerskich. Szersze wyjaśnienie znajduje się w odpowiedzi na uwagę nr 41.
46.	**§ 12 ust. 1 wraz z Załącznikiem nr 5**	**MI**	Generalna Dyrekcja Dróg Krajowych i Autostrad (GDDKiA) od 2017 r. utrzymuje rozwiązanie informatyczne w postaci Krajowego Punktu Dostępowego (KPD) do informacji o warunkach ruchu. KPD funkcjonuje w związku z realizacją obowiązków wynikających z Rozporządzenia Delegowanego Komisji (UE) nr 886/2013 z dnia 15 maja 2013 r., uzupełniającego dyrektywę Parlamentu Europejskiego i Rady 2010/40/UE w odniesieniu do danych i procedur dotyczących dostarczania bezpłatnie użytkownikom, w miarę możliwości, minimalnych powszechnych informacji o ruchu związanych z bezpieczeństwem drogowym. KPD służy zapewnieniu interoperacyjnej wymiany danych dotyczących warunków ruchu i bezpieczeństwa ruchu drogowego w ramach krajowego oraz europejskiego ekosystemu inteligentnych systemów transportowych. Do wymiany danych w swoim API KPD wykorzystuje europejski standard wymiany danych DATEX II, właściwy dla danych szybkozmiennych w obszarze ITS. Projekt rozporządzenia w § 12 ust. 1 przewiduje, że system teleinformatyczny używany do realizacji zadań publicznych jest wyposażony w interfejsy programistyczne aplikacji, zgodne ze specyfikacją określoną w załączniku nr 5 do rozporządzenia. Załącznik nr 5 do rozporządzenia wskazuje natomiast, że API w standardzie REST wykorzystuje format reprezentacji danych JSON5, jest zgodne ze standardem JSON Schema, przyjmuje JSON API jako standard komunikatów oraz	**Uwaga wyjaśniona** Projektowane rozporządzenie ma charakter horyzontalny, określa minimalne wymagania interoperacyjności dla systemów teleinformatycznych używanych do realizacji zadań publicznych i nie ustanawia rozwiązań dedykowanych poszczególnym sektorom. Przepisy projektu rozporządzenia nie wyłączają obowiązków płynących z przepisów odrębnych, w tym nie wykluczają stosowania standardu DATEX II dla danych szybkozmiennych w obszarze ITS Standard ten może być stosowany równolegle z wymaganiami określonymi w rozporządzeniu, w zakresie zgodnym z przepisami odrębnymi. W związku z tym nie ma uzasadnienia do zmiany wskazanego przepisu projektu rozporządzenia.

			wykorzystuje JSON-LD. Załącznik nr 5 przewiduje również obowiązek zapewnienia dostępu do zasobów w formacie JSON, przy czym XML może być udostępniany jedynie opcjonalnie w uzasadnionych przypadkach. W praktyce powyższe wymagania mogą zostać odczytane jako obowiązek stosowania standardu JSON do wymiany danych za pomocą API również w odniesieniu do danych szybkozmiennych ITS. Taka interpretacja mogłaby prowadzić do niespójności z europejskim standardem DATEX II, który jest stosowany przez KPD w celu zapewnienia interoperacyjności wymiany danych o ruchu drogowym. Mając na uwadze specyfikę danych szybkozmiennych związanych z inteligentnymi systemami transportowymi oraz konieczność zachowania zgodności z europejskim standardem wymiany danych DATEX II, zasadnym jest dodanie do projektu rozporządzenia przepisu przesądzającego, że w tym obszarze dane są przekazywane zgodnie z DATEX II. W związku z powyższym proponuję dodanie w § 12 po ust. 3 nowego ust. 4 w brzmieniu: „4. W przypadku danych szybkozmiennych związanych z inteligentnymi systemami transportowymi, w szczególności danych dotyczących warunków ruchu, zdarzeń drogowych, utrudnień, bezpieczeństwa ruchu drogowego oraz informacji dla użytkowników dróg, stosuje się europejski standard wymiany danych DATEX II. W tym zakresie wymagań określonych w załączniku nr 5 dotyczących formatu reprezentacji danych nie stosuje się, jeżeli prowadziłyby do obowiązku zastąpienia standardu DATEX II innym standardem wymiany danych.”. Dodatkowo należy podkreślić, że KPD zostanie wprowadzony do przepisów ustawy z dnia 21 marca 1985 r. o drogach publicznych na mocy projektu ustawy o zmianie ustawy o drogach publicznych oraz niektórych innych ustaw (UC89), który aktualnie jest na etapie rozpatrzenia przez Stały Komitet Rady Ministrów.	
47.	**§ 12 ust. 1 wraz z Załącznikiem nr 5**	**MKiŚ**	Zasadne jest doprecyzowanie relacji między obowiązkiem wyposażenia systemów w API zgodnie z załącznikiem nr 5 a interoperacyjnymi standardami branżowymi stosowanymi na podstawie przepisów odrębnych, w szczególności w obszarze informacji przestrzennej. Nie jest jasne czy system udostępniający dane zgodnie ze standardami właściwymi dla danej dziedziny musi równolegle udostępniać API zgodnie z załącznikiem nr 5.	**Uwaga wyjaśniona** Przepisy projektu rozporządzenia na wyłączają obowiązków płynących z przepisów odrębnych. Jeżeli takie przepisy wyłączają stosowanie przepisów rozporządzenia w określonym zakresie, to nie ma obowiązku ich stosowania.

48.	**§ 12 ust. 1 wraz z Załącznikiem nr 5**	**MI**	Należy doprecyzować, że zgodność z wymaganiami dla API oznacza osiągnięcie wymaganej interoperacyjności i funkcjonalności, a nie obowiązek implementacji każdego elementu specyfikacji zawartej w załączniku nr 5 do projektu rozporządzenia. Załącznik nr 5 do projektu rozporządzenia zawiera bardzo szczegółowe wymagania dotyczące m.in. JSON API, JSON-LD, HATEOAS, sposobu wersjonowania, struktury URI i dokumentacji API. Wiele istniejących interfejsów API wykorzystywanych przez administrację publiczną zapewnia interoperacyjność, choć nie implementuje wszystkich wskazanych mechanizmów.	**Uwaga wyjaśniona** Załączniki do rozporządzenia stanowią jego integralną całość i muszą być rozpatrywane całościowo w zakresie wskazanych w rozporządzeniu obowiązków.
49.	**§ 12 ust. 1 wraz z Załącznikiem nr 5**	**MI**	Należy dopuścić utrzymanie istniejących, udokumentowanych interfejsów API, które są powszechnie wykorzystywane, zapewniają interoperacyjność oraz bezpieczną wymianę danych, nawet jeśli nie implementują wszystkich elementów standardów JSON API, JSON-LD lub innych szczegółowych wymagań określonych w załączniku nr 5 do projektu rozporządzenia. Obowiązek dostosowania powinien dotyczyć wyłącznie nowych interfejsów lub zmian istotnie modyfikujących funkcjonalność istniejących API. Taka możliwość ogranicza ryzyko kosztownych i nieuzasadnionych przebudów działających już usług.	**Uwaga wyjaśniona** Wyjaśnienie znajduje się w odpowiedzi na uwagę nr 48.
50.	**§ 12 ust. 1 albo Załącznik nr 5**	**MI**	Proponuję dodanie przepisu stanowiącego, że za spełniające wymagania uznaje się również rozwiązania równoważne funkcjonalnie i interoperacyjnie względem standardów określonych w załączniku nr 5 projektu rozporządzenia. Rozwiązanie takie byłoby zgodne z zasadą neutralności technologicznej wskazaną w ustawie i projekcie rozporządzenia. Ponadto pozwoliłoby zachować istniejące inwestycje oraz ograniczyć koszty dostosowania systemów.	**Uwaga wyjaśniona** Wyjaśnienie znajduje się w odpowiedzi na uwagę nr 48.
51.	**§ 12 ust. 1 albo Załącznik nr 5**	**MRiRW**	**<u>Projektowane brzmienie § 12 ust. 1:</u>** „1. System teleinformatyczny używany do realizacji zadań publicznych jest wyposażony w interfejsy programistyczne aplikacji, zgodne ze specyfikacją, określoną w załączniku nr 5 do rozporządzenia.” **<u>Proponowane brzmienie § 12 ust. 1:</u>** „1. System teleinformatyczny używany do realizacji zadań publicznych jest wyposażony w interfejsy programistyczne aplikacji, zgodne ze specyfikacją, określoną w załączniku nr 5 do rozporządzenia. W przypadku danych przestrzennych interfejsy	**Uwaga wyjaśniona** Projektowane rozporządzenie ma charakter horyzontalny, określa minimalne wymagania interoperacyjności dla systemów teleinformatycznych używanych do realizacji zadań publicznych i nie ustanawia rozwiązań dedykowanych poszczególnym sektorom. Przepisy projektu rozporządzenia nie wyłączają obowiązków płynących z przepisów odrębnych, w tym nie wykluczają stosowania

			programistyczne aplikacji mogą być realizowane również z wykorzystaniem standardów Open Geospatial Consortium (OGC), w szczególności WFS, WMS, WMTS oraz OGC API Features.”. Projekt koncentruje się na REST API i SOAP, pomijając wyspecjalizowane standardy usług geoprzestrzennych stosowane powszechnie w infrastrukturach informacji przestrzennej. WFS stanowi podstawowy standard udostępniania danych wektorowych w postaci usług sieciowych i jest obecnie wykorzystywany przez Geoportal ARiMR. Uwzględnienie standardów OGC zapewni spójność z ustawą o infrastrukturze informacji przestrzennej, INSPIRE oraz funkcjonującymi systemami GIS administracji publicznej.	wyspecjalizowanych standardów usług geoprzestrzennych. Standardy takie, określone w przepisach szczególnych, a w szczególności w przepisach ustawowych, mogą wyłączać stosowanie przepisów projektowanego rozporządzenia. W związku z tym nie ma uzasadnienia do zmiany wskazanego przepisu projektu rozporządzenia.
52.	**§ 12 ust. 1**	**MSWiA**	2) odnośnie do projektowanego § 12 ust. 1 proponuję rozważyć wprowadzenie wyjątku od obowiązku określonego w § 12 ust. 1 w przypadkach uzasadnionych architekturą, przeznaczeniem i sposobem wykorzystania danego systemu teleinformatycznego – wskazać należy, że w przypadku niektórych systemów teleinformatycznych o charakterze wewnętrznym lub pomocniczym, które nie uczestniczą w wymianie danych z innymi systemami, obowiązek wyposażenia ich w interfejs API zgodny ze specyfikacją określoną w załączniku nr 5 może być nieproporcjonalny do celu regulacji;	**Uwaga wyjaśniona** Wymagania dotyczą API publicznych oraz API partnerskich. Szersze wyjaśnienie znajduje się w odpowiedzi na uwagę nr 41.
53.	**§ 12. (zmiana poprzez dodanie kolejnej jednostki redakcyjnej)**	**MRiRW**	**W § 12 proponuję po ust. 1 dodanie ust. 1a w brzmieniu:** „1a. W przypadku istniejących systemów teleinformatycznych obowiązek zapewnienia API stosuje się przy ich istotnej modernizacji lub wymianie, z uwzględnieniem możliwości technicznych, kosztów oraz konieczności zachowania ciągłości realizacji zadań publicznych. W przypadku braku technicznej lub ekonomicznej możliwości zapewnienia API podmiot realizujący zadanie publiczne dokumentuje przyczyny odstąpienia od tego wymagania.”. W wielu przypadkach zapewnienie API będzie wymagało budowy dodatkowej warstwy integracyjnej albo przebudowy systemu. Podmiot publiczny powinien mieć możliwość wykazania w dokumentacji wewnętrznej, że w konkretnym przypadku wykonanie obowiązku w określonym terminie jest niemożliwe lub nieproporcjonalne np. dotyczy to systemów, które w najbliższych latach będą wygaszane.	**Uwaga wyjaśniona** Okresy przejściowe dotyczące obowiązków związanych z realizacją zadań, określonych m.in. w art. 13 ust. 5 oraz art. 14 ust. 1a ustawy z dnia 17 lutego 2005 r. o informatyzacji działalności podmiotów realizujących zadania publiczne, zostały przewidziane w ustawie z dnia 25 lipca 2025 r. o zmianie ustawy o informatyzacji działalności podmiotów realizujących zadania publiczne oraz niektórych innych ustaw (Dz.U. poz. 1158). Zgodnie z art. 14 ust. 1 ustawy z dnia 25 lipca 2025 r. o zmianie ustawy o informatyzacji działalności podmiotów realizujących zadania publiczne oraz niektórych innych ustaw, organy administracji rządowej oraz jednostki budżetowe

				obsługujące te organy są obowiązane zrealizować wskazane wyżej zadania w terminie nie dłuższym niż 50 miesięcy od dnia wejścia w życie ustawy, tj. do 7 listopada 2029 r. Termin ten nie ma jednak zastosowania w przypadkach określonych w art. 14 ust. 4 ww. ustawy. Przepis ten stanowi, że regulacji przejściowych przewidzianych w art. 14 ust. 1-3 nie stosuje się do podmiotów realizujących zadania publiczne z wykorzystaniem systemu teleinformatycznego: - używanego do realizacji zadań publicznych w dniu wejścia w życie ustawy, jeżeli po upływie 18 miesięcy od dnia jej wejścia w życie (tj. po 7 marca 2027 r.) system ten został poddany zmianom w zakresie funkcjonalności wykorzystywanych do realizacji zadań publicznych, z wyłączeniem konserwacji oprogramowania, aktualizacji bezpieczeństwa oraz aktualizacji technicznych; - wdrożonego do realizacji zadań publicznych w okresie pierwszych 18 miesięcy od dnia wejścia w życie ustawy, jeżeli po upływie tego okresu system został poddany zmianom w zakresie funkcjonalności wykorzystywanych do realizacji zadań publicznych, z wyłączeniem konserwacji oprogramowania, aktualizacji bezpieczeństwa oraz aktualizacji technicznych; - utworzonego po upływie 18 miesięcy od dnia wejścia w życie ustawy. W konsekwencji nie wszystkie podmioty objęte zakresem art. 14 ust. 1 będą mogły korzystać z 50-miesięcznego okresu dostosowawczego. Utrata prawa do stosowania tego okresu następuje bowiem również w przypadku dokonania, po upływie 18 miesięcy od wejścia w życie ustawy, zmian funkcjonalnych w systemie teleinformatycznym wykorzystywanym do realizacji zadań publicznych.

54.	**§ 12 ust. 2**	**MRiRW**	**<u>Projektowane brzmienie § 12 ust. 2:</u>** „2. Podmiot realizujący zadania publiczne zapewnia dostępność, stabilność, łatwość sposobu korzystania, utrzymanie przez cały cykl użytkowania oraz bezpieczeństwo stosowanych interfejsów programistycznych systemu teleinformatycznego, o których mowa w ust. 1.” **<u>Proponowane brzmienie § 12 ust. 2:</u>** „2. Podmiot realizujący zadania publiczne zapewnia dostępność, stabilność, **bezpieczeństwo oraz mechanizmy ochrony danych osobowych realizujące zasadę privacy by design i privacy by defoult, w szczególności poprzez ograniczenie zakresu przetwarzanych danych, okresu ich przechowywania oraz ich dostępności do zakresu niezbędnego do realizacji zadania publicznego, kontrolę dostępu oraz rejestrację operacji przetwarzania**, a także łatwość sposobu korzystania, utrzymanie przez cały cykl użytkowania oraz bezpieczeństwo stosowanych interfejsów programistycznych systemu teleinformatycznego, o których mowa w ust. 1.”. Podmiot realizujący zadania publiczne jest administratorem danych osobowych w związku z czym odpowiada za ich właściwe, legalne i bezpieczne przetwarzanie. Proponowana zmiana nie modyfikuje pozostałych wymagań dotyczących dostępności, stabilności, łatwości korzystania oraz utrzymania interfejsów przez cały cykl ich użytkowania. Ma ona na celu ich uzupełnienie o jednoznaczne odniesienie do ochrony danych osobowych i mechanizmów zapewniających realizację zasad privacy by design i privacy by default, z uwzględnieniem zakresu niezbędnego do realizacji konkretnego zadania publicznego.	**Uwaga wyjaśniona** Wyjaśnienie podano w odpowiedzi na uwagę nr 7.
55.	**§ 14 ust. 1**	**MKiŚ**	Zasadne jest rozróżnienie formatów przeznaczonych do prezentacji dokumentów od formatów przeznaczonych do wymiany, automatycznego przetwarzania i ponownego wykorzystania danych. W przypadku danych ustrukturyzowanych lub tabelarycznych powinno być wymagane zapewnienie co najmniej jednego formatu maszynowo czytelnego umożliwiającego dalsze przetwarzanie. Samo udostępnienie danych np. w PDF nie zapewnia interoperacyjności.	**Uwaga wyjaśniona** Dla danych ustrukturyzowanych projekt rozporządzenia przewiduje formaty xml, gml, JSON, GeoJSON. Dla danych tabelarycznych projekt przewiduje m.in. formaty ods, xlsx, csv. Zgodnie z projektem pliki w formacie pdf powinny być stosowany do dokumentów tekstowo-graficznych.
56.	**§ 14 ust. 2**	**MKiŚ**	Obowiązek określony w § 14 ust. 2 projektu jest sprzeczny	**Uwaga uwzględniona**

			z ogólną zasadą wspierania neutralności technologicznej projektu wskazaną w § 3 ust. 2 projektu. W załączniku nr 3 są wskazane zamknięte, komercyjne formaty plików, co do których wprowadzono wymóg, by podmiot publiczny umożliwiał przyjmowanie w nich pism, w szczególności dotyczy to formatów wymiany danych CAD, które w znacznej mierze do poprawnego odczytu wymagają dedykowanego, zamkniętego oprogramowania. Usunięcie w § 14 ust. 2 odniesienia do załącznika nr 3 – pozostawienie wyłącznie odniesienia do załącznika nr 2. Proponowane brzmienie: „2. Podmiot realizujący zadania publiczne umożliwia przyjmowanie pism utrwalonych w postaci elektronicznej, służących do załatwiania spraw należących do zakresu jego działania, w formatach plików określonych w załączniku nr 2 do rozporządzenia.”	
57.	**§ 14 ust. 4**	**RCL**	w § 14 ust. 4 projektu rozporządzenia, mając na uwadze przepis art. 5 ust. 4 ustawy z dnia 12 września 2002 r. o normalizacji (Dz. U. z 2015 r. poz. 1483), zgodnie z którym Polskie Normy mogą być powoływane w przepisach prawnych po ich opublikowaniu w języku polskim – mając na uwadze, że wskazana w przedmiotowym przepisie norma ETSI EN 301 549 V3.2.1:2021 została opublikowana w języku polskim, proponuje się wprowadzenie odesłania do jej do wersji polskiej. Jednocześnie przywołane w przedmiotowym projekcie normy ISO wymagają ponownej analizy i weryfikacji pod kątem ich poprawnego wprowadzenia do aktu powszechnie obowiązującego (jako budzące wątpliwości można przykładowo: wskazaną w § 3 ust. 6 projektu normę ISO/IEC 19510, która nie została wprowadzona do polskiego systemu norm, a także wymienioną w § 11 ust. 3 projektu normę ISO/IEC 20000-1 – której polska wersja językowa została wycofana);	**Uwaga wyjaśniona** W informatyce, a szczególnie w obszarze publicznych systemów teleinformatycznych i rejestrów publicznych, odwoływanie się wyłącznie do Polskich Norm (PN) publikowanych przez Polski Komitet Normalizacyjny (PKN) nie jest wystarczające. Wynika to zarówno z charakteru współczesnych technologii informatycznych, jak i z potrzeb interoperacyjności, które z natury wykraczają poza granice jednego państwa. **1. Informatyka jest dziedziną globalną** Większość technologii informatycznych stosowanych w administracji publicznej powstaje i jest rozwijana w środowisku międzynarodowym. Dotyczy to m.in.: • formatów danych (XML, JSON, PDF), • protokołów komunikacyjnych (HTTP, TLS), • metod zarządzania usługami IT (ISO/IEC 20000), • bezpieczeństwa informacji (ISO/IEC 27001), • zarządzania jakością danych i systemów. Gdyby administracja publiczna opierała się wyłącznie na normach krajowych, mogłoby dojść

				do izolacji technologicznej oraz utrudnienia współpracy z podmiotami zagranicznymi. Polska administracja publiczna jest zobowiązania do współpracy międzynarodowej między podmiotami publicznymi m.in. na podstawie aktu ws. Interoperacyjnej Europy. **2. Nie wszystkie normy ISO są opublikowane jako Polskie Normy.** W obszarze teleinformatyki liczba norm rozwija się bardzo szybko. Nie każda norma zostaje wdrożona jako PN, zostaje przetłumaczona, czy jest dostępna w najnowszej wersji krajowej. Odwołanie do normy ISO umożliwia stosowanie aktualnych i uznanych międzynarodowo rozwiązań nawet wtedy, gdy odpowiednia PN jeszcze nie istnieje. **3. Wymagania interoperacyjności wymagają wspólnego języka technicznego.** Interoperacyjność oznacza zdolność podmiotów do współdziałania przez wymianę danych za pomocą środków komunikacji elektronicznej. Warunkiem interoperacyjności jest stosowanie wspólnych standardów: • modeli danych, • metadanych, • identyfikatorów, • metod zarządzania jakością, • procesów eksploatacyjnych. Normy ISO pełnią tutaj rolę uniwersalnego punktu odniesienia, pozwalającego różnym państwom, organizacjom i dostawcom rozumieć wymagania w taki sam sposób. **4. Normy ISO są często jedynym źródłem uzgodnionej terminologii.**

				W wielu obszarach normy ISO nie tylko określają wymagania techniczne, ale także definiują pojęcia. W administracji publicznej ma to szczególne znaczenie dla jednoznaczności interpretacyjnej oraz spójności regulacji. **5. Krajowe Ramy Interoperacyjności wymagają śledzenia rozwoju standardów** KRI wskazują, że interoperacyjność osiąga się również przez stosowanie norm, specyfikacji i innych dokumentów technicznych uznanych na poziomie krajowym, europejskim i międzynarodowym. Ponieważ technologie informatyczne rozwijają się szybciej, niż proces legislacyjny i normalizacyjny na poziomie krajowym, odwoływanie się do norm ISO pozwala zachować aktualność wymagań technicznych. **Pozostałe wyjaśnienia** Norma ISO/IEC 19510 nie posiada oficjalnej polskiej wersji językowej w bazie Polskiego Komitetu Normalizacyjnego. Jednak w oparciu o treść delegacji ustawowej z art. 18, tj. "Rada Ministrów określi, w drodze rozporządzenia, szczegółowe sposoby realizacji obowiązków (...) uwzględniając zasady neutralności technologicznej i otwartości używanych standardów oraz specyfikacji oraz zgodności z opublikowanymi normami zatwierdzonymi przez międzynarodową, europejską lub krajową jednostkę normalizacyjną." (podkreślenie własne), podano odwołanie do opublikowanej normy zatwierdzonej przez międzynarodową jednostkę normalizacyjną. Norma ISO/IEC 20000-1 została zaktualizowana przez międzynarodową jednostkę normalizacyjną ISO w 2018 roku. Starsza, polska wersja tej

				normy PN-ISO/IEC 20000-1:2014-01 została wycofana przez Polski Komitet Normalizacyjny (PKN). W tekście rozporządzenia nie można przywoływać wycofanej normy, a zatem pozostawiono odwołanie do opublikowanej normy zatwierdzonej przez międzynarodową jednostkę normalizacyjną. Sytuacja wygląda analogicznie w przypadku normy ISO/IEC 20000-2 (wersja polska PN-ISO/IEC 20000-2:2007 posiada status "wycofana"). Analogicznie, przywołane w tekście normy międzynarodowe ISO/IEC lub ISO o numerach (w kolejności podanej wg występowania w projekcie rozporządzenia): 10646, 32000, 26300, 29500, 23736, 10918, 12639, 15948, 11172-3, 13818, 14496, 21320, 19757-2 nie mają aktualnych (tj. niewycofanych) polskich odpowiedników. Normę ISO 16739-1 w projekcie rozporządzenia zastąpiono normą PN-EN ISO 16739-1, a normę ISO/IEC 19136 - normą PN-EN ISO 19136-1.
58.	**§ 15 (zmiana poprzez dodanie kolejnej jednostki redakcyjnej)**	**MRiRW**	**Proponuje się w § 15 po ust. 3 dodanie ust. 4 w brzmieniu:** „4. W przypadku wymiany lub udostępniania danych opisujących obiekty przestrzenne, o których mowa w § 5 ust. 1 pkt 3, podmiot realizujący zadania publiczne zapewnia jednoznaczne określenie układu odniesienia przestrzennego poprzez wskazanie identyfikatora układu zgodnego z rejestrem EPSG lub innym równoważnym rejestrem układów odniesienia przestrzennego.” Projekt określa wymagania dotyczące wymiany danych oraz identyfikacji wybranych obiektów przestrzennych, jednak nie przewiduje obowiązku jednoznacznego identyfikowania układu odniesienia przestrzennego wykorzystywanego przy udostępnianiu lub wymianie danych. Informacja o układzie odniesienia stanowi podstawowy element interoperacyjności danych przestrzennych i jest niezbędna do ich prawidłowego integrowania, analizy oraz wykorzystania przez odbiorców. Wprowadzenie takiego wymagania zapewni spójność z zasadami infrastruktury informacji przestrzennej oraz powszechnie stosowanymi standardami geoinformacyjnymi.	**Uwaga wyjaśniona** Projektowane rozporządzenie ma charakter horyzontalny, określa minimalne wymagania interoperacyjności dla systemów teleinformatycznych używanych do realizacji zadań publicznych i nie ustanawia rozwiązań dedykowanych poszczególnym sektorom. Przepisy projektu rozporządzenia nie wyłączają obowiązków płynących z przepisów odrębnych, w tym regulujących wymianę lub udostępnianie danych opisujących obiekty przestrzenne. Wymagania takie określone w przepisach szczególnych, a w szczególności w przepisach ustawowych, będą mogły wyłączać stosowanie przepisów projektowanego rozporządzenia. W związku z tym nie ma uzasadnienia do zmiany wskazanego przepisu projektu rozporządzenia.

59.	**§ 16 ust. 2 pkt 4 w**	**MI**	Wnoszę o dodanie § 16 ust. 2 pkt 4 w brzmieniu: „4) zdarzeń mających znaczenie dla wykrywania incydentów cyberbezpieczeństwa, w szczególności nieudanych prób uwierzytelnienia, prób eskalacji uprawnień, zmian uprawnień użytkowników oraz naruszeń mechanizmów bezpieczeństwa.” Projekt rozporządzenia określa minimalny zakres zdarzeń podlegających rejestrowaniu, obejmując przede wszystkim działania administratorów, zmiany konfiguracji oraz danych, przetwarzanych w systemie teleinformatycznym. Zakres ten nie jest jednak wystarczający z punktu widzenia współczesnych wymagań cyberbezpieczeństwa. Ustawa z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa definiuje obsługę incydentu jako proces obejmujący wykrywanie, rejestrowanie, analizowanie, klasyfikowanie, priorytetyzację oraz podejmowanie działań naprawczych. Realizacja tych obowiązków wymaga rejestrowania nie tylko działań administratorów, ale również zdarzeń mogących świadczyć o próbach naruszenia bezpieczeństwa, takich jak nieudane próby logowania, eskalacja uprawnień, zmiany uprawnień użytkowników czy naruszenia mechanizmów bezpieczeństwa.	**Uwaga uwzględniona** Dodano punkt: „4) naruszenia lub próby naruszenia bezpieczeństwa systemu teleinformatycznego, w szczególności nieudanych prób uwierzytelnienia, prób uzyskania nieuprawnionego dostępu oraz prób nieuprawnionych zmian uprawnień.”
60.	**§ 16 ust. 6**	**MI**	Wnoszę o dodanie § 16 ust. 6 w brzmieniu: „6. System teleinformatyczny gromadzenia dzienników systemowych powinien zapewniać możliwość centralnej analizy zdarzeń bezpieczeństwa oraz wykrywania incydentów cyberbezpieczeństwa odpowiednio do poziomu ryzyka związanego z eksploatacją systemu teleinformatycznego.”. Projekt rozporządzenia dopuszcza możliwość centralnego gromadzenia dzienników systemowych, jednak nie wskazuje celu ich centralizacji ani wymogu prowadzenia analizy zdarzeń bezpieczeństwa. W praktyce samo przechowywanie logów nie zapewnia realizacji obowiązków wynikających m.in. z ustawy z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa, której celem jest zapewnienie odpowiedniego poziomu bezpieczeństwa systemów informacyjnych oraz skuteczna obsługa incydentów. Dyrektywa NIS2 wymaga wdrożenia środków umożliwiających wykrywanie incydentów, natomiast norma ISO/IEC 27001:2022 wskazuje na konieczność monitorowania zdarzeń bezpieczeństwa oraz analizowania zapisów dzienników. Proponowana zmiana nie narzuca stosowania konkretnej	**Uwaga wyjaśniona** Zagadnienia zapewnienia odpowiedniego poziomu bezpieczeństwa „systemów informacyjnych” oraz skutecznej obsługi incydentów znajdują się, jak wskazano w uwadze, w kompetencjach ustawy o krajowym systemie cyberbezpieczeństwa. Zapisy dzienników systemowych, niezależnie od miejsca ich gromadzenia, powinny być wykorzystywane w realizacji obowiązków przywołanej ustawy.

			technologii (np. stosowania w tym celu sytemu klasy SIEM), zachowując neutralność technologiczną rozporządzenia, lecz określa wymagany efekt organizacyjny.	
61.	**§ 16 (zmiana poprzez dodanie kolejnej jednostki redakcyjnej)**	**MRiRW**	**Proponuje się w § 16 po ust. 5 dodać ust. 6 w brzmieniu:** „6. Podmiot realizujący zadania publiczne zapewnia integralność, dostępność i ochronę zapisów dzienników systemowych przed nieuprawnioną modyfikacją, usunięciem lub utratą oraz synchronizację czasu wykorzystywanego do rejestrowania zdarzeń z zaufanym źródłem czasu.”. Proponowany przepis zapewnia realizację wymagania rozliczalności poprzez ochronę dzienników systemowych oraz zapewnienie jednoznacznego czasu rejestrowanych zdarzeń. Jest zgodny z wymaganiami norm ISO/IEC 27001 i ISO/IEC 27002 oraz wspiera obsługę incydentów i czynności kontrolne.	**Uwaga uwzględniona**
62.	**§ 17**	**MRiRW**	**Projektowane brzmienie § 17:** „W systemie teleinformatycznym używanym do realizacji zadań publicznych stosuje się mechanizmy umożliwiające zbieranie danych o korzystaniu przez użytkowników z elektronicznej usługi publicznej oraz pozwalające użytkownikom na przekazywanie informacji zwrotnych na jej temat, które pozwalają na doskonalenie i dalszy rozwój takiej usługi.” **Proponowane brzmienie § 17:** „W systemie teleinformatycznym, za pośrednictwem którego elektroniczna usługa publiczna jest bezpośrednio udostępniana usługobiorcy, stosuje się mechanizmy umożliwiające zbieranie niezbędnych danych o korzystaniu przez użytkowników z elektronicznej usługi publicznej oraz pozwalające użytkownikom na przekazywanie informacji zwrotnych na jej temat, które pozwalają na doskonalenie i dalszy rozwój takiej usługi, z uwzględnieniem przepisów o ochronie danych osobowych.”. W realizacji usługi publicznej może uczestniczyć wiele systemów działających na zapleczu: rejestry, systemy integracyjne, systemy analityczne czy rozwiązania wykonujące automatyczne przetwarzanie. Użytkownik końcowy nie korzysta z nich bezpośrednio, dlatego zapewnianie w każdym z takich systemów mechanizmów zbierania opinii nie ma praktycznego uzasadnienia. Dlatego też proponuje się powiązanie obowiązku zbierania danych o korzystaniu z elektronicznej usługi publicznej oraz	**Uwaga uwzględniona** Wprowadzono nową treść przepisu „Podmiot realizujący zadania publiczne stosuje w systemie teleinformatycznym, za pośrednictwem którego świadczona jest elektroniczna usługa publiczna, mechanizmy umożliwiające zbieranie zagregowanych informacji o wykorzystaniu tej usługi oraz pozwalające użytkownikom na przekazywanie informacji zwrotnych na jej temat, w celu doskonalenia i dalszego rozwoju takiej usługi”.

			informacji zwrotnej z systemami, które rzeczywiście stanowią kanał świadczenia takiej usługi. Proponowane uzupełnienie „niezbędnych danych” służy ograniczeniu zakresu zbieranych informacji do danych adekwatnych do celu ich przetwarzania. Jednocześnie dodanie odesłania do przepisów o ochronie danych osobowych zapewnia, że mechanizmy służące monitorowaniu korzystania z usług publicznych oraz pozyskiwaniu informacji zwrotnych będą projektowane i stosowane z uwzględnieniem obowiązujących zasad ochrony danych osobowych. Proponowane brzmienie nie ogranicza możliwości gromadzenia informacji zwrotnych od użytkowników ani prowadzenia analiz dotyczących korzystania z usług, lecz jednoznacznie wskazuje, że działania te powinny odbywać się z poszanowaniem przepisów o ochronie danych osobowych.	
63.	**§ 18 i § 19**	**MRiRW**	(§18) Rejestry publiczne funkcjonujące w dniu wejścia w życie rozporządzenia należy dostosować do wymagań, o których mowa w rozdziale 3, w dniu ich pierwszej istotnej zmiany przypadającej po wejściu w życie rozporządzenia, jednak nie później niż w terminie 36 miesięcy od dnia wejścia w życie niniejszego rozporządzenia. (§ 19) Systemy teleinformatyczne używane do realizacji zadań publicznych funkcjonujące w dniu wejścia w życie rozporządzenia należy dostosować do wymagań, o których mowa w rozdziale 4, w dniu ich pierwszej istotnej zmiany przypadającej po wejściu w życie rozporządzenia, jednak nie później, niż w terminie 36 miesięcy od dnia wejścia w życie niniejszego rozporządzenia. Dostosowanie wielu systemów informatycznych oraz rejestrów publicznych do projektowanych wymagań wymaga przeprowadzenia szczegółowej analizy istniejących rozwiązań, przygotowania odpowiednich projektów, zabezpieczenia finansowania, przeprowadzenia postępowań zakupowych, a następnie wykonania prac wdrożeniowych, migracji danych oraz przeprowadzenia niezbędnych testów. W przypadku dużych i złożonych systemów informatycznych oraz rejestrów publicznych, a także w sytuacji konieczności równoległego dostosowania wielu systemów i rejestrów, planowany dwuletni okres przejściowy może okazać się niewystarczający. Brak odpowiednio długiego i realistycznego	**Uwaga nieaktualna** Przepisy przejściowe zostały usunięte z projektu. Okresy przejściowe dotyczące obowiązków związanych z realizacją zadań, określonych m.in. w art. 13 ust. 5 oraz art. 14 ust. 1a ustawy z dnia 17 lutego 2005 r. o informatyzacji działalności podmiotów realizujących zadania publiczne, zostały przewidziane w ustawie z dnia 25 lipca 2025 r. o zmianie o informatyzacji działalności podmiotów realizujących zadania publiczne oraz niektórych innych ustaw (Dz.U. poz. 1158). Zgodnie z art. 14 ust. 1 ustawy z dnia 25 lipca 2025 r. o zmianie ustawy o informatyzacji działalności podmiotów realizujących zadania publiczne oraz niektórych innych ustaw, organy administracji rządowej oraz jednostki budżetowe obsługujące te organy są obowiązane zrealizować wskazane wyżej zadania w terminie nie dłuższym niż 50 miesięcy od dnia wejścia w życie ustawy, tj. do 7 listopada 2029 r. Termin ten nie ma jednak zastosowania w przypadkach określonych w art. 14 ust. 4 ww. ustawy. Przepis ten stanowi, że regulacji

			okresu dostosowawczego może prowadzić do powstania ryzyka formalnej niezgodności, pomimo podejmowania przez podmioty racjonalnych i udokumentowanych działań zmierzających do spełnienia wymagań. Zasadne jest zatem wydłużenie okresu przejściowego do 36 miesięcy. Ponadto proponuje się doprecyzowanie relacji terminów dostosowania systemów teleinformatycznych i rejestrów publicznych określonych w § 18-20 projektu rozporządzenia do okresów przejściowych wynikających z art. 14 ustawy z dnia 25 lipca 2025 r. o zmianie ustawy o informatyzacji działalności podmiotów realizujących zadania publiczne oraz niektórych innych ustaw. Art. 14 ustawy przewiduje zróżnicowane okresy przejściowe dla realizacji części obowiązków wynikających ze znowelizowanej ustawy o informatyzacji, natomiast § 18 i § 19 projektu rozporządzenia przewidują dostosowanie istniejących rejestrów i systemów przy pierwszej istotnej zmianie, nie później jednak niż w terminie dwóch lat od wejścia w życie rozporządzenia. W praktyce zakres tych obowiązków jest ze sobą powiązany. Wskazane byłoby jednoznaczne określenie wzajemnej relacji terminów, tak aby nie powstawały wątpliwości co do daty, od której poszczególne wymagania powinny być spełnione.	przejściowych przewidzianych w art. 14 ust. 1-3 nie stosuje się do podmiotów realizujących zadania publiczne z wykorzystaniem systemu teleinformatycznego: - używanego do realizacji zadań publicznych w dniu wejścia w życie ustawy, jeżeli po upływie 18 miesięcy od dnia jej wejścia w życie (tj. po 7 marca 2027 r.) system ten został poddany zmianom w zakresie funkcjonalności wykorzystywanych do realizacji zadań publicznych, z wyłączeniem konserwacji oprogramowania, aktualizacji bezpieczeństwa oraz aktualizacji technicznych; - wdrożonego do realizacji zadań publicznych w okresie pierwszych 18 miesięcy od dnia wejścia w życie ustawy, jeżeli po upływie tego okresu system został poddany zmianom w zakresie funkcjonalności wykorzystywanych do realizacji zadań publicznych, z wyłączeniem konserwacji oprogramowania, aktualizacji bezpieczeństwa oraz aktualizacji technicznych; - utworzonego po upływie 18 miesięcy od dnia wejścia w życie ustawy. W konsekwencji nie wszystkie podmioty objęte zakresem art. 14 ust. 1 będą mogły korzystać z 50-miesięcznego okresu dostosowawczego. Utrata prawa do stosowania tego okresu następuje bowiem również w przypadku dokonania, po upływie 18 miesięcy od wejścia w życie ustawy, zmian funkcjonalnych w systemie teleinformatycznym wykorzystywanym do realizacji zadań publicznych. Ponadto ustawodawca przepisami ustawy z dnia 25 lipca 2025 r. o zmianie ustawy o informatyzacji działalności podmiotów realizujących zadania publiczne oraz niektórych innych ustaw odroczył termin wejścia w życie zmian spowodowanych nowelizacją upoważnienia ustawowego

				o 18 miesięcy – wyznaczając tym samym (w art. 15 tej ustawy) końcowy termin, do upływu którego będą mogły mieć zastosowanie dotychczasowe przepisy wykonawcze. Termin ten pokrywa się z dniem wejścia w życie projektowanego rozporządzenia. Tak skonstruowana regulacja ustawowa (przy braku innych regulacji intertemporalnych) ma charakter zupełny i wyczerpujący w odniesieniu do stosowania przepisów dotychczasowych. Z takiej konstrukcji przepisów wynika brak możliwości zastosowania, od dnia 23 lutego 2027 r., przepisów określających Krajowe Ramy Interoperacyjności oraz minimalne wymagania dla rejestrów publicznych i systemów teleinformatycznych – innych niż wynikające z projektowanego rozporządzenia. Jej konsekwencją powinno być jednolite wprowadzenie nowych regulacji.
64.	**§ 18 i § 19**	**MRiRW**	Proponuje się doprecyzowanie pojęcia „istotnej zmiany” użytego w przepisach przejściowych. W szczególności warto wskazać, że chodzi o zmianę wpływającą na funkcjonalność wykorzystywaną do realizacji zadań publicznych, interoperacyjność, sposób udostępniania danych lub funkcji albo strukturę rejestru. Od momentu pierwszej „istotnej zmiany” uzależniono obowiązek dostosowania całego systemu lub rejestru do nowych wymagań. Brak definicji może prowadzić do różnych interpretacji, szczególnie w przypadku systemów rozwijanych w sposób ciągły.	**Uwaga nieaktualna** Uwaga nieaktualna, gdyż przepisy przejściowe zostały usunięty z projektu rozporządzenia.
65.	**§ 18 i § 19**	**MSZ**	W § 18 i § 19 projektowanego rozporządzenia wskazano, że rejestry publiczne oraz systemy teleinformatyczne używane do realizacji zadań publicznych funkcjonujące w dniu wejścia w życie rozporządzenia należy dostosować do wymagań, o których mowa odpowiednio w rozdziale 3 i 4, w dniu ich pierwszej istotnej zmiany przypadającej po wejściu w życie rozporządzenia, jednak nie później niż w terminie 2 lat od dnia wejścia w życie niniejszego rozporządzenia. Przewiduje się, że projektowane przepisy wejdą w życie w dniu 23 lutego 2027 r., co oznacza, że dostosowanie rejestrów/systemów ma nastąpić nie później niż do 23 lutego 2029 roku. W przypadku Ministerstwa Spraw	**Uwaga nieaktualna** Przepisy przejściowe zostały usunięte z projektu. Okresy przejściowe dotyczące obowiązków związanych z realizacją zadań, określonych m.in. w art. 13 ust. 5 oraz art. 14 ust. 1a ustawy z dnia 17 lutego 2005 r. o informatyzacji działalności podmiotów realizujących zadania publiczne, zostały przewidziane w ustawie z dnia 25 lipca 2025 r. o zmianie ustawy o informatyzacji działalności podmiotów realizujących zadania

			Zagranicznych dostosowanie to może dotyczyć dwóch rejestrów publicznych: - Centralnego rejestru przyznanych oraz unieważnionych Kart Polaka oraz Kart Polaka, które utraciły ważność z mocy prawa, - Centralnego rejestru wizowego oraz przynajmniej poniższych systemów z obszaru konsularnego: - Wizy-Konsul, - e-Konsulat. Powyższe systemy z obszaru konsularnego są przewidziane do wycofania wraz z pełnym uruchomieniem planowanej Elektronicznej Platformy Usług Konsularnych, co – zgodnie z założeniami – powinno nastąpić do końca 2029 r. Obecnie resort nie jest w stanie określić skali niezbędnych dostosowań dla ww. systemów, ale istnieje możliwość, że w przypadku wejścia w życie rozporządzenia w obecnym brzmieniu MSZ zostanie zobowiązany do znaczącej modyfikacji systemów przewidzianych do wycofania w perspektywie kilkunastu miesięcy od maksymalnej daty obowiązkowego dostosowania systemów z KRI oraz zastąpienia ich nowym systemem, w pełni zgodnym z KRI. Należy zauważyć, że wydatkowanie środków budżetowych na dostosowanie do wymagań KRI systemów i rejestrów, które planowane są do wycofywania w bliskim horyzoncie czasowym, wydaje się niegospodarne. W tym kontekście wydaje się zasadne dodanie możliwości zwolnienia w takim przypadku wymienionych powyżej systemów (rejestrów), np. na wniosek składany do ministra ds. cyfryzacji lub do Komitetu ds. Cyfryzacji, z konieczności dostosowania określonej w § 18 i § 19 rozporządzenia.	publiczne oraz niektórych innych ustaw (Dz.U. poz. 1158) Zgodnie z art. 14 ust. 1 ustawy z dnia 25 lipca 2025 r. o zmianie ustawy o informatyzacji działalności podmiotów realizujących zadania publiczne oraz niektórych innych ustaw, organy administracji rządowej oraz jednostki budżetowe obsługujące te organy są obowiązane zrealizować wskazane wyżej zadania w terminie nie dłuższym niż 50 miesięcy od dnia wejścia w życie ustawy, tj. do 7 listopada 2029 r. Termin ten nie ma jednak zastosowania w przypadkach określonych w art. 14 ust. 4 ww. ustawy. Przepis ten stanowi, że regulacji przejściowych przewidzianych w art. 14 ust. 1-3 nie stosuje się do podmiotów realizujących zadania publiczne z wykorzystaniem systemu teleinformatycznego: - używanego do realizacji zadań publicznych w dniu wejścia w życie ustawy, jeżeli po upływie 18 miesięcy od dnia jej wejścia w życie (tj. po 7 marca 2027 r.) system ten został poddany zmianom w zakresie funkcjonalności wykorzystywanych do realizacji zadań publicznych, z wyłączeniem konserwacji oprogramowania, aktualizacji bezpieczeństwa oraz aktualizacji technicznych; - wdrożonego do realizacji zadań publicznych w okresie pierwszych 18 miesięcy od dnia wejścia w życie ustawy, jeżeli po upływie tego okresu system został poddany zmianom w zakresie funkcjonalności wykorzystywanych do realizacji zadań publicznych, z wyłączeniem konserwacji oprogramowania, aktualizacji bezpieczeństwa oraz aktualizacji technicznych; - utworzonego po upływie 18 miesięcy od dnia wejścia w życie ustawy. W konsekwencji nie wszystkie podmioty objęte zakresem art. 14 ust. 1 będą mogły korzystać z

				50-miesięcznego okresu dostosowawczego. Utrata prawa do stosowania tego okresu następuje bowiem również w przypadku dokonania, po upływie 18 miesięcy od wejścia w życie ustawy, zmian funkcjonalnych w systemie teleinformatycznym wykorzystywanym do realizacji zadań publicznych.
66.	**§ 18 i § 19**	**MSWiA**	1) proponuję rozważenie możliwość odstępstwa w odniesieniu do interfejsów systemów przeznaczonych do wycofania w określonym terminie, jeżeli ich dostosowanie byłoby nieproporcjonalne do ponoszonych kosztów i przewidywanego okresu dalszej eksploatacji, przy zachowaniu wymaganego poziomu bezpieczeństwa;	**Uwaga wyjaśniona** Obowiązki, których szczegółowe sposoby realizacji określone zostały w projekcie rozporządzenia, wynikają z przepisów ustawowych. Akt wykonawczy nie może modyfikować obowiązków nałożonych przez przepisy ustawowe. Natomiast okresy przejściowe dotyczące obowiązków związanych z realizacją zadań, określonych m.in. w art. 13 ust. 5 oraz art. 14 ust. 1a ustawy o informatyzacji, zostały przewidziane w ustawie z dnia 25 lipca 2025 r. o zmianie ustawy o informatyzacji działalności podmiotów realizujących zadania publiczne oraz niektórych innych ustaw Dz.U. poz. 1158). Zgodnie z art. 14 ust. 1 ustawy z dnia 25 lipca 2025 r. o zmianie ustawy o informatyzacji działalności podmiotów realizujących zadania publiczne oraz niektórych innych ustaw, organy administracji rządowej oraz jednostki budżetowe obsługujące te organy są obowiązane zrealizować wskazane wyżej zadania w terminie nie dłuższym niż 50 miesięcy od dnia wejścia w życie ustawy, tj. do 7 listopada 2029 r. Termin ten nie ma jednak zastosowania w przypadkach określonych w art. 14 ust. 4 ww. ustawy. Przepis ten stanowi, że regulacji przejściowych przewidzianych w art. 14 ust. 1-3 nie stosuje się do podmiotów realizujących zadania publiczne z wykorzystaniem systemu teleinformatycznego:

				- używanego do realizacji zadań publicznych w dniu wejścia w życie ustawy, jeżeli po upływie 18 miesięcy od dnia jej wejścia w życie (tj. po 7 marca 2027 r.) system ten został poddany zmianom w zakresie funkcjonalności wykorzystywanych do realizacji zadań publicznych, z wyłączeniem konserwacji oprogramowania, aktualizacji bezpieczeństwa oraz aktualizacji technicznych; - wdrożonego do realizacji zadań publicznych w okresie pierwszych 18 miesięcy od dnia wejścia w życie ustawy, jeżeli po upływie tego okresu system został poddany zmianom w zakresie funkcjonalności wykorzystywanych do realizacji zadań publicznych, z wyłączeniem konserwacji oprogramowania, aktualizacji bezpieczeństwa oraz aktualizacji technicznych; - utworzonego po upływie 18 miesięcy od dnia wejścia w życie ustawy. W konsekwencji nie wszystkie podmioty objęte zakresem art. 14 ust. 1 będą mogły korzystać z 50-miesięcznego okresu dostosowawczego. Utrata prawa do stosowania tego okresu następuje bowiem również w przypadku dokonania, po upływie 18 miesięcy od wejścia w życie ustawy, zmian funkcjonalnych w systemie teleinformatycznym wykorzystywanym do realizacji zadań publicznych.
67.	**§ 18–20**	**RCL**	wątpliwości budzi przewidywany w projekcie zakres zastosowania jego regulacji wynikający z przepisów przejściowych i końcowych (rozdział 5 projektu, przepisy § 18–20). Przede wszystkim należy zauważyć, że ustawodawca przepisami ustawy z dnia 25 lipca 2025 r. o zmianie ustawy o informatyzacji działalności podmiotów realizujących zadania publiczne oraz niektórych innych ustaw (Dz. U. poz. 1158) odroczył termin wejścia w życie zmian spowodowanych nowelizacją upoważnienia ustawowego o 18 miesięcy – wyznaczając tym samym (w art. 15 tej ustawy) końcowy termin, do upływu którego będą mogły mieć zastosowanie dotychczasowe przepisy wykonawcze. Termin ten	**Uwaga uwzględniona** Przepisy zostały usunięte z projektu.

			pokrywa się z dniem wejścia w życie projektowanego rozporządzenia. W ocenie Rządowego Centrum Legislacji tak skonstruowana regulacja ustawowa (przy braku innych regulacji intertemporalnych) ma charakter zupełny i wyczerpujący w odniesieniu do stosowania przepisów dotychczasowych. Z takiej konstrukcji przepisów wynika brak możliwości zastosowania, od dnia 23 lutego 2027 r., przepisów określających Krajowe Ramy Interoperacyjności oraz minimalne wymagania dla rejestrów publicznych i systemów teleinformatycznych – innych niż 3 wynikające z projektowanego rozporządzenia. Jej konsekwencją powinno być jednolite wprowadzenie nowych regulacji. W świetle powyższego, mając również na względzie brak określenia w projekcie np. innych rozwiązań mających zastosowanie w początkowym okresie obowiązywania projektowanego rozporządzenia, wątpliwości budzi przewidywane w § 18 i § 19 projektu odsunięcie obowiązku dostosowania funkcjonujących w dniu wejścia w życie projektowanego rozporządzenia rejestrów publicznych i systemów teleinformatycznych do proponowanych regulacji o 2 lata, a także przewidywane w § 20 odroczenie wejścia w życie części z projektowanych regulacji odpowiednio o 6 i 12 miesięcy – w stosunku do pozostałych rejestrów i systemów teleinformatycznych. Przykładowo w ww. okresach nie będzie obowiązku ustanowienia planu ciągłości świadczenia elektronicznych usług publicznych oraz planu przywracania po awarii tych usług (§ 11 ust. 4 projektu) czy udostępniania danych w systemie teleinformatycznym w formatach i standardach wynikających z załącznika nr 2 do rozporządzenia (§ 14 ust. 1 projektu). Wprowadzane projektem odstępstwa od jednolitego pod względem czasowym zastosowania projektowanych przepisów wymagają obszernego i szczegółowego wyjaśnienia z uwzględnieniem ich wpływu na realizację przez podmioty publiczne zadań publicznych z wykorzystaniem rejestrów publicznych i systemów teleinformatycznych zgodnie z regulacją ustawową (przede wszystkim art. 13 ust. 1 i 2 oraz art. 14 ust. 1 ustawy);	
68.	**§ 18–19**	**RCL**	Niezależnie od powyższego zwrócić należy uwagę na nieprecyzyjność użytego w § 18 i § 19 projektu pojęcia „pierwszej istotnej zmiany” systemu teleinformatycznego bądź rejestru	**Uwaga nieaktualna** Uwaga nieaktualna, gdyż przepisy zostały usunięte z projektu.

			publicznego, wprowadzającego zbyt szerokie pole interpretacji obowiązku stosowania przepisów rozporządzenia.	
69.	**§ 19**	**MSWiA**	3) w ocenie resortu spraw wewnętrznych i administracji zasadne jest uwzględnienie specyfiki systemów o szczególnym znaczeniu dla bezpieczeństwa i porządku publicznego, w tym ich złożoności, wymogów bezpieczeństwa, konieczności zachowania ciągłości działania oraz czasu potrzebnego na przeprowadzenie postępowań zakupowych, wdrożenie i testy. W związku z tym zasadnym wydaje się rozważenie wprowadzenia mechanizmu umożliwiającego indywidualne wydłużenie okresu dostosowawczego dla tych systemów, przy jednoczesnym pozostawieniu dwuletniego terminu jako zasady;	**Uwaga wyjaśniona** Obowiązki, których szczegółowe sposoby realizacji określone zostały w projekcie rozporządzenia wynikają z przepisów ustawowych. Akt wykonawczy nie może modyfikować obowiązków nałożonych przez przepisy ustawowe. Natomiast okresy przejściowe dotyczące obowiązków związanych z realizacją zadań, określonych m.in. w art. 13 ust. 5 oraz art. 14 ust. 1a ustawy o informatyzacji, zostały przewidziane w ustawie z dnia 25 lipca 2025 r. o zmianie ustawy o informatyzacji działalności podmiotów realizujących zadania publiczne oraz niektórych innych ustaw (Dz. U. poz. 1158). Zgodnie z art. 14 ust. 1 ustawy z dnia 25 lipca 2025 r. o zmianie ustawy o informatyzacji działalności podmiotów realizujących zadania publiczne oraz niektórych innych ustaw, organy administracji rządowej oraz jednostki budżetowe obsługujące te organy są obowiązane zrealizować wskazane wyżej zadania w terminie nie dłuższym niż 50 miesięcy od dnia wejścia w życie ustawy, tj. do 7 listopada 2029 r. Termin ten nie ma jednak zastosowania w przypadkach określonych w art. 14 ust. 4 ww. ustawy. Przepis ten stanowi, że regulacji przejściowych przewidzianych w art. 14 ust. 1-3 nie stosuje się do podmiotów realizujących zadania publiczne z wykorzystaniem systemu teleinformatycznego: - używanego do realizacji zadań publicznych w dniu wejścia w życie ustawy, jeżeli po upływie 18 miesięcy od dnia jej wejścia w życie (tj. po 7 marca 2027 r.) system ten został poddany zmianom w zakresie funkcjonalności wykorzystywanych do realizacji zadań

				publicznych, z wyłączeniem konserwacji oprogramowania, aktualizacji bezpieczeństwa oraz aktualizacji technicznych; - wdrożonego do realizacji zadań publicznych w okresie pierwszych 18 miesięcy od dnia wejścia w życie ustawy, jeżeli po upływie tego okresu system został poddany zmianom w zakresie funkcjonalności wykorzystywanych do realizacji zadań publicznych, z wyłączeniem konserwacji oprogramowania, aktualizacji bezpieczeństwa oraz aktualizacji technicznych; - utworzonego po upływie 18 miesięcy od dnia wejścia w życie ustawy. W konsekwencji nie wszystkie podmioty objęte zakresem art. 14 ust. 1 będą mogły korzystać z 50-miesięcznego okresu dostosowawczego. Utrata prawa do stosowania tego okresu następuje bowiem również w przypadku dokonania, po upływie 18 miesięcy od wejścia w życie ustawy, zmian funkcjonalnych w systemie teleinformatycznym wykorzystywanym do realizacji zadań publicznych.
70.	**§ 19**	**MI**	Projekt przewiduje obowiązek dostosowania istniejących systemów teleinformatycznych do wymagań rozporządzenia najpóźniej w terminie 2 lat od wejścia w życie rozporządzenia. W przypadku podmiotów posiadających dużą liczbę systemów oraz wieloletnich integracji z odbiorcami zewnętrznymi, w szczególności systemów udostępniających dane specjalistyczne (np. meteorologiczne i hydrologiczne), termin ten może okazać się niewystarczający dla przeprowadzenia pełnego procesu analizy, projektowania, wdrożenia, testów i migracji użytkowników. Proponuję zatem: - wydłużenie okresu dostosowawczego dla istniejących interfejsów API, - albo wprowadzenie zasady, że istniejące API mogą być utrzymywane do czasu ich istotnej modernizacji, - albo uznanie istniejących API za zgodne, jeśli zapewniają interoperacyjność i są udokumentowane.	**Uwaga wyjaśniona** Przepisy przejściowe zostały usunięte z projektu. Okresy przejściowe dotyczące obowiązków związanych z realizacją zadań, określonych m.in. w art. 13 ust. 5 oraz art. 14 ust. 1a ustawy o informatyzacji, zostały przewidziane w ustawie z dnia 25 lipca 2025 r. o zmianie ustawy o zmianie ustawy o informatyzacji działalności podmiotów realizujących zadania publiczne oraz niektórych innych ustaw (Dz. U. poz. 1158). Zgodnie z art. 14 ust. 1 ustawy z dnia 25 lipca 2025 r. o zmianie ustawy o informatyzacji działalności podmiotów realizujących zadania publiczne oraz niektórych innych ustaw, organy administracji rządowej oraz jednostki budżetowe obsługujące te organy są obowiązane zrealizować wskazane wyżej zadania w terminie

				nie dłuższym niż 50 miesięcy od dnia wejścia w życie ustawy, tj. do 7 listopada 2029 r. Termin ten nie ma jednak zastosowania w przypadkach określonych w art. 14 ust. 4 ww. ustawy. Przepis ten stanowi, że regulacji przejściowych przewidzianych w art. 14 ust. 1-3 nie stosuje się do podmiotów realizujących zadania publiczne z wykorzystaniem systemu teleinformatycznego: - używanego do realizacji zadań publicznych w dniu wejścia w życie ustawy, jeżeli po upływie 18 miesięcy od dnia jej wejścia w życie (tj. po 7 marca 2027 r.) system ten został poddany zmianom w zakresie funkcjonalności wykorzystywanych do realizacji zadań publicznych, z wyłączeniem konserwacji oprogramowania, aktualizacji bezpieczeństwa oraz aktualizacji technicznych; - wdrożonego do realizacji zadań publicznych w okresie pierwszych 18 miesięcy od dnia wejścia w życie ustawy, jeżeli po upływie tego okresu system został poddany zmianom w zakresie funkcjonalności wykorzystywanych do realizacji zadań publicznych, z wyłączeniem konserwacji oprogramowania, aktualizacji bezpieczeństwa oraz aktualizacji technicznych; - utworzonego po upływie 18 miesięcy od dnia wejścia w życie ustawy. W konsekwencji nie wszystkie podmioty objęte zakresem art. 14 ust. 1 będą mogły korzystać z 50-miesięcznego okresu dostosowawczego. Utrata prawa do stosowania tego okresu następuje bowiem również w przypadku dokonania, po upływie 18 miesięcy od wejścia w życie ustawy, zmian funkcjonalnych w systemie teleinformatycznym wykorzystywanym do realizacji zadań publicznych.
71.	**Załaczniki**	**RCL**	zgodnie z § 15a ust. 2 Zasad techniki prawodawczej załączniki wprowadza się w przepisach części artykułowej aktu. W przepisie,	**Uwaga uwzględniona**

			który wprowadza załącznik, określa się zakres treści załącznika. W przypadku przedmiotowego projektu rozporządzenia zauważenia wymaga, że załączniki rozporządzenia w części tekstowej zostały wprowadzone niejednolicie przez odesłanie do zakresu przedmiotowego załącznika (np. załącznik nr 2) – proponuje się więc ujednolicenie sposobu wprowadzania załączników, zgodnie z Zasadami techniki prawodawczej; proponuje się także zmianę numeracji załączników i ich przywoływanie w tekście projektowanego rozporządzenia w kolejności numerycznej, rozpoczynając od nr 1;	Do projektu zostały wprowadzone odpowiednie zmiany. Ujednolicono sposób wprowadzania załączników do projektu oraz zmieniono numerację załączników zgodnie z kolejnością ich występowania w projekcie, rozpoczynając od 1.
72.	**Załączniki**	**MI**	Ponadto, zwracam uwagę na omyłki pisarskie znajdujące się na stronach: 29, 31 i 35: [1] - str. 29 – w załączniku 3 w tabeli Formaty plików obsługiwane przez podmiot realizujący zadanie publiczne w trybie odczytu w liczbie porządkowej brakuje numerów 2 i , [2] - str. 31 – w pierwszym zdaniu zamiast „do realizacji zadań publicznych jest zgodne z standardem architektury usług REST” powinno być „do realizacji zadań publicznych jest zgodne ze standardem architektury usług REST”, [3] - str. 35 – w pkt 8 wymagania dotyczące wersjonowania API, w lit. g znajduje się spacja przed przecinkiem.	**Uwaga uwzględniona** 1. Załącznik został usunięty. 2. Uwaga uwzględniona. 3. Uwaga uwzględniona.
73.	**Załącznik nr 1**	**MKiŚ**	Konstrukcja przepisu § 5 („Strukturę ... określa załącznik nr 1”) sugeruje, że zawarta w załączniku nr 1 struktura identyfikatorów stanowi ich wyczerpujący katalog. Wydaje się to jednak stać w sprzeczności z tytułem rozdziału 3 (Minimalne wymagania dla rejestrów publicznych), w którym znajduje się ten przepis. Rozbieżność ta nie pozwala jednoznacznie ustalić, czy załącznik nr 1 określa minimalny czy zamknięty zestaw identyfikatorów. Również uzasadnienie nie zawiera wyjaśnień w tym zakresie. Ponadto katalog zawarty w załączniku nr 1 nie uwzględnia wielu identyfikatorów powszechnie stosowanych w rejestrach publicznych, w szczególności: 1. w odniesieniu do osób fizycznych – identyfikatorów cudzoziemców; 2. w odniesieniu do podmiotów – NIP, KRS oraz identyfikatorów europejskich, w tym EUID; 3. w odniesieniu do obiektów przestrzennych – identyfikatorów Państwowego Rejestru Granic oraz TERYT, wykorzystywanych	**Uwaga wyjaśniona** W powszechnie obowiązujących przepisach prawa nie zostały ustanowione referencyjne rejestry publiczne. Ministerstwo Cyfryzacji prowadzi prace przygotowawcze do przygotowania przepisów ustanawiających zasady i procedurę nadawania referencyjności atrybutom obiektów danych przechowywanych w rejestrach publicznych. W ramach projektowanego rozporządzenia załącznik będzie zawierał strukturę unikatowych identyfikatorów obiektów: osoba fizyczna, podmiot oraz obiekt przestrzenny, w zakresie dotyczącym punktu adresowego, działki ewidencyjnej oraz budynku.

			do identyfikacji jednostek podziału terytorialnego w rejestrach publicznych. Załącznik nr 1 nie odzwierciedla tym samym rzeczywistej różnorodności rejestrów publicznych. W nowoczesnej architekturze interoperacyjności stosuje się podejście, zgodnie z którym podstawę stanowią rejestry referencyjne państwa oraz wykorzystywane w nich identyfikatory, a nie sztywna klasyfikacja typów obiektów.	
74.	**Załącznik nr 1 w lp.1**	**MFiG (MF)**	w polu wyrażenie regularne powinna znajdować się składnia \d{11} zamiast \d{ll}	**Uwaga uwzględniona**
75.	**Załącznik nr 1, poz. 3**	**MFiG (MRiT)**	Jako rejestr zawierający dane referencyjne dla punktu adresowego wskazano Ewidencję Miejscowości, Ulic i Adresów. Rejestry prowadzone przez GUNB pozyskują i przechowują identyfikatory punktów adresowych pochodzące z Państwowego Rejestru Granic (przestrzeń nazw, identyfikator lokalny i wersja punktu PRG). Wskazane byłoby dopuszczenie identyfikatorów PRG albo wyraźne wskazanie relacji między identyfikatorem EMUiA a identyfikatorem PRG.	**Uwaga wyjaśniona** Wyjaśnienie podano w odpowiedzi na uwagę nr 73.
76.	**Załącznik nr 1, Lp. 3**	**MFiG (MRiT)**	Wnioskujemy, aby w ramach KRI określić ogólne wymogi co do identyfikatorów dla obiektów przestrzennych, a nie tylko dla dwóch szczególnych przypadków jakimi są punkty adresowe oraz działki ewidencyjne. Proponujemy dodać ogólny wiersz mówiący o konstrukcji identyfikatora dla obiektów przestrzennych niezależnie w jakim rejestrze publicznym są one przechowywane. Analizy i konsultacji wymagałoby w naszej ocenie określenie długości pola (kolumna nr 3). Propozycja dla poszczególnych kolumn: 1. Obiekt przestrzenny 2. Identyfikator obiektu przestrzennego 3. Przestrzeń nazw (uzupełnić o znaki _,.,–,-) Identyfikator lokalny (uzupełnić o znak: -) Identyfikator wersji 4. Rejestr publiczny właściwy dla rodzaju obiektu przestrzennego.	**Uwaga częściowo uwzględniona** Wskutek uwzględnienia uwagi nr 16 załącznik do rozporządzenia został uzupełniony o strukturę identyfikatora obiektu przestrzennego w zakresie dotyczącym budynku.

			Ustawa z dnia 4 marca 2010 r. o infrastrukturze informacji przestrzennej (Dz. U. z 2025 r. poz. 242) oraz ustawa właściwa dla rodzaju obiektu przestrzennego.	
77.	**Załącznik nr 2**	**MFiG (MRiT)**	Do weryfikacji, czy ten załącznik nie powinien zostać rozszerzony o format JSON, a przyszłościowo także GeoJSON.	**Uwaga uwzględniona**
78.	**Załącznik nr 2**	**MKiŚ**	Zestawienie zawarte w załączniku nr 2 łączy różne kategorie, tj.: 1. katalog formatów danych; 2. katalog standardów wymiany danych; 3. katalog standardów dokumentów; 4. katalog standardów publikacji otwartych danych; 5. katalog standardów podpisu elektronicznego; 6. katalog słowników interoperacyjności. Przykładowo: DOCX opisuje sposób zapisu dokumentu biurowego, RDF opisuje semantykę danych, natomiast CPSV-AP opisuje model usług publicznych. W konsekwencji załącznik jest bardzo szczegółowy technicznie, niekompletny, niespójny oraz trudny do interpretacji i utrzymania. Brakuje w nim między innymi DCAT-AP, stanowiącego podstawowy europejski profil katalogowy dla otwartych danych i danych o wysokiej wartości. Nie określono również wymagań dotyczących wersjonowania.	**Uwaga częściowo uwzględniona** **Wyjaśnienie** Rozdział 4 projektu rozporządzenia określa minimalne wymagania dla systemów teleinformatycznych używanych do realizacji zadań publicznych i wymiany danych z podmiotami publicznymi. W oparciu o przepisy § 14 projektu rozporządzenia podmiot realizujący zadania publiczne udostępnia dane przetwarzane w systemie teleinformatycznym używanym do realizacji zadań publicznych w co najmniej jednym z formatów plików lub standardów określonych w załączniku nr 1 do rozporządzenia, a także umożliwia przyjmowanie pism utrwalonych w postaci elektronicznej, służących do załatwiania spraw należących do zakresu jego działania, w formatach plików określonych w załączniku nr 1 do rozporządzenia. W odniesieniu do wersjonowania minimalne wymagania oznaczają, że podmiot jest zobowiązany do używania wskazanej lub nowszej wersji formatu i standardu, określonej w załączniku nr 1 do projektu rozporządzenia. Do załącznika dodano DCAT-AP jako specyfikację służącą do opisywania zestawów danych sektora publicznego w formacie nadającym się do odczytu maszynowego.
79.	**Załącznik nr 2**	**MKiŚ**	Konieczne jest uzupełnienie listy formatów i standardów o otwarte formaty dedykowane obsłudze danych przestrzennych, w szczególności o format GeoPackage (rozszerzenie nazwy pliku: GPKG), opracowany i utrzymywany przez Open Geospatial Consortium (OGC) w 2014 r. Jest on formatem otwartym	**Uwaga wyjaśniona** Rozporządzenie określa formaty oraz standardy zapewniające dostęp do danych udostępnianych za pomocą systemów teleinformatycznych używanych do realizacji zadań publicznych.

			i ustandaryzowanym (dokumentacja została zamieszczona pod linkiem https://www.ogc.org/publications/standard/geopackage/), coraz częściej stosowanym w administracji publicznej oraz w Komisji Europejskiej. Przykładem użycia jest implementacja powyższego mechanizmu na cele sprawozdawczości w związku z realizowaniem przepisów europejskiej dyrektywy w sprawie hałasu (END): (https://wikis.ec.europa.eu/download/attachments/44140427/doc4_inspire_good_practice_GPKG_v2.pdf?version=1&modificationDate=1648759569532&api=v2). GeoPackage przechowuje dane w jednej skompresowanej bazie danych SQLite, co redukuje liczbę plików i zwiększa wydajność operacji na dużych zbiorach danych przestrzennych. GML, będący formatem opartym na XML, jest często znacznie bardziej rozbudowany i trudniejszy w przetwarzaniu, zwłaszcza przy dużych zbiorach danych przestrzennych. Utrzymywanie danych w jednej bazie danych, charakteryzujące GPKG, minimalizuje ryzyko błędów interpretacyjnych wynikających z błędnej struktury XML, typowych dla GML. W przypadku GML różne interpretacje schematów XML mogą prowadzić do błędów w odczycie danych w różnych programach. Przechowywanie danych w bazie danych SQLite, jako kolejna cecha GPKG, umożliwia szybkie zapytania, indeksowanie i filtrowanie danych bez konieczności wczytywania całego pliku do pamięci. GML jako format XML wymaga większej mocy obliczeniowej do parsowania, co jest szczególnie problematyczne w środowiskach z ograniczonymi zasobami. Należy również zwrócić uwagę, że GPKG to pojedynczy plik, co ułatwia jego przesyłanie i zarządzanie nim. GML często wymaga wielu plików (np. schematów XSD), co może komplikować wymianę danych między systemami. GPKG charakteryzuje zatem lepsza przenośność i łatwość jego użytkowania. GPKG umożliwia przechowywanie zarówno obiektów wektorowych (punkty, linie, poligony) jak i danych rastrowych (obrazy satelitarne, modele terenu), co pozwala na bardziej kompleksową wymianę informacji. Obecny katalog obejmuje m.in. GML i GeoTIFF, lecz nie uwzględnia części formatów powszechnie wykorzystywanych obecnie do wymiany i udostępniania danych wektorowych.	Zakres formatów i danych określony w załączniku nr 1 do projektu rozporządzenia dotyczy każdego podmiotu realizującego zadania publiczne. Z tego względu formaty i standardy właściwe dla danego obszaru administracyjnego powinny być co do zasady regulowane w przepisach właściwych dla takiego obszaru. Dla zwiększenia interoperacyjności wymiany przestrzennych do załącznika, zgodnie z uwagą nr 77, dodano format GeoJSON.

			Uzupełnienie załącznika nr 2 o otwarty format dedykowany obsłudze danych przestrzennych – GeoPackage. Dodanie formatu (GPKG) do listy oficjalnych formatów w projekcie byłoby uzupełnieniem dla GML, szczególnie w kontekście przechowywania i analizy dużych zbiorów danych geograficznych oraz umożliwiłoby bardziej wydajną i elastyczną wymianę danych przestrzennych między podmiotami publicznymi, poprawiając interoperacyjność i łatwość użycia w systemach GIS.	
80.	**Załącznik nr 2**	**MKiŚ**	Wnoszę także o uzupełnienie listy formatów w załączniku nr 2 o otwarty format danych przestrzennych – GeoJSON. Format ten jest utrzymywany i rozwijany przez Internet Engineering Task Force (IETF) od 2015 r., z otwartą specyfikacją dostępną na stronie: https://geojson.org/. GeoJSON to format wymiany danych geoprzestrzennych oparty na notacji obiektów JavaScript (JSON). Definiuje on kilka typów obiektów JSON oraz sposób ich łączenia w celu reprezentowania danych o obiektach geograficznych, ich właściwościach i zasięgu przestrzennym. GeoJSON wykorzystuje układ współrzędnych geograficznych – Światowy System Geodezyjny 1984 (World Geodetic System 1984, WGS 84) oraz jednostki wyrażone w stopniach dziesiętnych. Uzupełnienie załącznika nr 2 o otwarty format dedykowany obsłudze danych przestrzennych – GeoJSON.	**Uwaga uwzględniona**
81.	**Załącznik nr 2, część A lub nowy punkt dotyczący danych przestrzennych.**	**MRiRW**	Proponuje się rozszerzenie katalogu formatów i standardów dla danych przestrzennych: „Do udostępniania danych przestrzennych stosuje się co najmniej jeden z następujących formatów: GML, GeoJSON, SHP, GeoPackage.” Format ESRI Shapefile pozostaje jednym z najpowszechniej stosowanych formatów wymiany danych przestrzennych pomiędzy podmiotami publicznymi. Jest wykorzystywany przez liczne systemy GIS administracji publicznej. Brak jego uwzględnienia może ograniczyć interoperacyjność istniejących rozwiązań i generować konieczność kosztownych konwersji danych. Projekt przewiduje GML i GeoTIFF, jednak nie obejmuje tego podstawowego formatu wymiany danych wektorowych. Również GeoJSON jest obecnie coraz częściej wykorzystywanym formatem wymiany danych przestrzennych w usługach internetowych, portalach mapowych oraz rozwiązaniach opartych na architekturze REST API. Uwzględnienie wyłącznie GML nie	**Uwaga częściowo uwzględniona** Rozważono uwagę i po analizie, dla zwiększenia interoperacyjności wymiany danych przestrzennych do załącznika - zgodnie z uwagą nr 77 - dodano format GeoJSON.

			odzwierciedla aktualnego stanu techniki i może utrudniać integrację z nowoczesnymi systemami teleinformatycznymi. GeoPackage jest obecnie rekomendowanym przez OGC otwartym formatem wymiany danych przestrzennych, stanowiącym nowoczesną alternatywę dla formatu SHP. Umożliwia przechowywanie danych wektorowych, rastrowych oraz metadanych w jednym pliku. Ujęcie tego standardu będzie zgodne z zasadą otwartych standardów wskazaną w projekcie rozporządzenia.	
82.	**Zał. nr 2, cz. A**	**MFiG (MRiT)**	W załączniku nr 2, w części A (formaty do wymiany danych przez podmioty realizujące zadania publiczne), w punkcie 1 (formaty dla danych tekstowych, tekstowo-graficznych lub multimedialnych) projektu, należy przewidzieć również JSON, tak jak w punkcie 2.4 (dla publikowania otwartych danych). Ponadto JSON powinien być uwzględniony również w części B (w szczególności w kontekście określania struktury dokumentu elektronicznego). Uzasadnienie: Przekazywanie ustrukturalizowanych danych w ramach formatu .json może być wygodnym sposobem komunikowania się między podmiotami realizującymi zadania publiczne (np. zamiast przesyłać plik w formacie .pdf lub .docx, który może zawierać nienadające się (lub trudne) do odczytu maszynowego wyspy danych, można przesłać dane w formacie .json, co sprzyja reużywalności i agregacji danych i możliwe jest również przesyłanie technikami innymi niż API, o którym mowa w Załączniku nr 5 do opiniowanego projektu, m.in. w kontekście wykorzystania JavaScript Object Notation wśród standardów architektury usług REST). Przykład: przesyłanie pocztą elektroniczną lub ezd zestawu danych dotyczących Oceny Skutków Regulacji lub zestawu danych związanych z realizacją obowiązku przekazania informacji o wynikach przeglądu prawa gospodarczego na podstawie art. 70 ustawy z dnia 6 marca 2018 r. – Prawo przedsiębiorców. Należy zauważyć, że w projektowanym § 11 projektu rozporządzenia Rady Ministrów w sprawie repozytorium interoperacyjności (RD309) - w kontekście art. 12k ust. 3 pkt 1 lit. g ustawy z dnia 17 lutego 2005 r. o informatyzacji działalności podmiotów realizujących zadania publiczne, dla struktur danych i dla znaczenia danych zawartych w tych strukturach dla danych	**Uwaga uwzględniona**

			gromadzonych w rejestrze publicznym wskazywany jest JSON oraz XML. Konsekwencją przyjęcia przedstawionej do opinii wersji załącznika (bez proponowanej poprawki) jest sytuacja, w której chcąc przekazać dane w strukturze JSON (wymienić dane przez podmioty realizujące zadania publiczne) należy dodatkowo (obok) przekazać je w jednym z formatów plików wskazanych w części A1 tabeli stanowiącej Załącznik nr 2 do opiniowanego projektu rozporządzenia. Sensem propozycji jest to, by wymiana danych wyłącznie JSON między podmiotami realizującymi zadania publiczne była uznana za spełniającą minimalne wymagania dla systemów teleinformatycznych używanych do realizacji zadań publicznych i wymiany danych z podmiotami publicznymi (w szczególności w kontekście § 14 ust. 1 opiniowanego projektu).	
83.	**Załącznik nr 2 w lp. 1.2 kol.4**	**MFiG (MF)**	opis plików typu .pdf błędnie wskazuje na przynależność do rodziny Open Dokument Format (ODF)	**Uwaga uwzględniona**
84.	**Załącznik nr 2, część A, pkt 1**	**MFiG (MRiT)**	Prosimy o weryfikację czy nie należy tej części rozszerzyć o format xml – w tym formacie przekazywane są m.in. projekty aktów prawnych w procesie uzgodnień i opiniowania i jest to format powszechnie używany w odniesieniu do plików tekstowych w administracji publicznej.	**Uwaga uwzględniona** Format xml został ujęty w części „B. Do reprezentacji i wymiany danych ustrukturyzowanych w postaci nadającej się do odczytu maszynowego stosuje się następujące formaty danych:”, co pozwala na uwzględnianie go w procesie przekazywane projektów aktów prawnych w formacie do odczytu maszynowego. Dla danych tekstowych, w formacie do odczytu przez człowieka, należy stosować formaty plików wskazane w części A.
85.	**Załącznik nr 2 Część A pkt 7**	**MFiG (MF)**	luka w numeracji między 7.2 i 7.4 (brak pozycji 7.3)	**Uwaga uwzględniona**
86.	**Załącznik nr 2, część B, pkt 1.3**	**MFiG (MRiT)**	W niewłaściwym miejscu zamieszczona została informacja nt. formatu GML. Należy przenieść format GML z części B do części A jako format w którym udostępniane są dane przestrzenne – ich struktura określana jest w pliku xsd (o którym mowa w części B). Ponadto należałoby zmienić jego definicję.	**Uwaga uwzględniona**

			Należy przenieść format GML z części B do części A jako format, w którym udostępniane są dane przestrzenne. Propozycja definicji: Format GML (Geography Markup Language) - oparty na języku XML standard kodowania danych geograficznych i przestrzennych.	
87.	**Załącznik nr 3**	**MKiŚ**	W załączniku nr 3 wskazano formaty o charakterze zamkniętym lub powiązane z komercyjnymi dostawcami rozwiązań IT, dla których nie wskazano otwartych standardów lub specyfikacji, podczas gdy projekt rozporządzenia w § 3 ust. 2 odwołuje się do zasady neutralności technologicznej (która obejmuje m.in. wymóg stosowania otwartych standardów i specyfikacji). Wymóg obsługiwania przez urząd formatu (nawet w trybie do odczytu) o zamkniętym bądź komercyjnym charakterze (szczególnie poprzez imienne wskazanie konkretnej firmy w akcie prawnym, może rodzić zarzuty promowania konkretnych rozwiązań), nie jest spójny zasadami neutralności technologicznej. W szczególności imienne wskazanie w akcie prawnym konkretnej firmy może rodzić zarzut promowania określonych rozwiązań. Należy podkreślić, że sam przepis upoważniający do wydania tego aktu wykonawczego zawiera wytyczną nakazującą zachowanie zasady równego traktowania różnych rozwiązań informatycznych. Zasadne jest zastąpienie tych formatów ich otwartymi zamiennikami albo wyraźne wskazanie, że ich obsługa jest dopuszczalna jedynie w ramach już stosowanych rozwiązań lub systemów, w celu zachowania kompatybilności wstecznej. Należałoby przy tym wprowadzić obowiązek przejścia na formaty otwarte przy najbliższej istotnej zmianie systemu i uwzględnić to rozwiązanie w przepisach przejściowych tj. w § 18 i § 19. Usunięcie odniesień do zamkniętych formatów plików w projekcie i zastąpienie na ich otwarte otwartymi zamiennikami lub formatami o znanych specyfikacjach.	**Uwaga uwzględniona** Projekt KRI realizuje zasadę otwartości standardów i specyfikacji poprzez preferowanie oraz uwzględnianie otwartych standardów przy wyborze formatów plików. Jednocześnie projekt zachowuje zasadę neutralności technologicznej wynikającą z ustawy o informatyzacji i nie wprowadza generalnego wymogu stosowania wyłącznie otwartych standardów. Kryterium rozstrzygającym jest zapewnienie interoperacyjności i dostępu do danych, a otwarte standardy są wskazywane jako rozwiązanie co do zasady najbardziej sprzyjające osiągnięciu tych celów. Jednakże wprowadzenie obowiązku stosowania wyłącznie otwartych standardów mogłoby prowadzić do nieuzasadnionego ograniczenia neutralności technologicznej oraz wykraczać poza zakres delegacji ustawowej. Załącznik nr 3 został usunięty z rozporządzenia wskutek uwzględnienia uwagi nr 9.
88.	**Załącznik nr 3**	**MKiŚ**	W załączniku nr 3 wątpliwości budzi: 1. prawdopodobny błąd merytoryczny dotyczący formatu ICS; 2. brak kluczowych formatów geoprzestrzennych i środowiskowych, takich jak GeoPackage, KML, NetCDF, HDF5 oraz GRIB; 3. nieuzasadnione uprzywilejowanie historycznych formatów binarnych Microsoft DOC, XLS i PPT;	**Uwaga nieaktualna** Załącznik nr 3 został usunięty z rozporządzenia wskutek uwzględnienia uwagi nr 9.

			4. brak wskazania minimalnego okresu utrzymywania kompatybilności z formatami historycznymi; 5. brak odniesienia do rzeczywistych potrzeb rejestrów publicznych i systemów dziedzinowych, w tym systemów środowiskowych funkcjonujących m.in. w Głównym Inspektoracie Ochrony Środowiska i Generalnej Dyrekcji Ochrony Środowiska.	
89.	**Załącznik nr 3 w lp. 4**	**MFiG (MF)**	format .ics (rozszerzenie nazwy pliku) jest formatem danych kalendarzowych. Formatami stosowanymi do wymiany danych CAD rozwijanymi przez buildingSMART są .ifc lub .icdd Luka w wierszach między 1 a 4 (brak pozycji 2 i 3)	**Uwaga nieaktualna** Załącznik nr 3 został usunięty z rozporządzenia wskutek uwzględnienia uwagi nr 9.
90.	**Załącznik nr 3 w lp. 6**	**MFiG (MF)**	jest Microsoft Excell powinno być Microsoft Excel.	**Uwaga nieaktualna** Załącznik nr 3 został usunięty z rozporządzenia wskutek uwzględnienia uwagi nr 9.
91.	**Załącznik nr 4**	**MKiŚ**	Załącznik nr 4 nie opisuje samej oceny interoperacyjności krajowej, lecz określa listę elementów tej oceny, traktując ocenę jako dokument. Tymczasem zgodnie z art. 12n ustawy o informatyzacji działalności podmiotów realizujących zadania publiczne ocena interoperacyjności jest procesem. W związku z tym załącznik nr 4 lub bezpośrednio przepisy rozporządzenia powinny określić jako elementy oceny m.in. jej metodologię, kryteria, progi istotności zmian, sposób identyfikacji interesariuszy, sposób weryfikacji jakości oceny, a także kwestie odpowiedzialności za błędną ocenę.	**Uwaga częściowo uwzględniona** **Wyjaśnienie** Zgodnie z art. 12n ustawy o informatyzacji ocena interoperacyjności krajowej jest procesem. Zgodnie z przywołanym artykułem w repozytorium interoperacyjności publikuje się wynik takiej oceny. Wskutek zgłoszonej uwagi został zmieniony § 4 ust. 2 projektowanego rozporządzenia: „Podmiot realizujący zadania publiczne uwzględnia elementy wyniku oceny interoperacyjności krajowej stanowiące załącznik nr 2 do rozporządzenia.” W uzasadnieniu do projektu rozporządzenia podano informacje na temat przeprowadzania oceny: Ocena ta pozwoli podmiotowi realizującemu zadania publiczne na wprowadzanie takiego zakresu zmian, których skutki będą w najmniejszym możliwym stopniu oddziaływać negatywnie na inne podmioty publiczne. Należy podkreślić, że ocena taka realizowana ma być przed wprowadzeniem zmian, co pozwoli na organizacyjne i techniczne przygotowanie się podmiotów publicznych do zmiany procedur oraz rozwiązań

				pozwalających na kontynuowanie dostępu do systemu teleinformatycznego używanego do realizacji zadań publicznych czy do danych gromadzonych w rejestrze publicznym, co zmniejszy ryzyko zakłócenia ciągłości wykonywania zadań publicznych. Zgodnie z nowelizacją ustawy o informatyzacji wynik oceny interoperacyjności krajowej należy publikować w formacie nadającym się do odczytu maszynowego w repozytorium interoperacyjności przed wprowadzeniem zmian. Zgodnie z przepisami ustawowymi publikacja następuje w terminie pozwalającym podmiotom publicznych na realizację zadań publicznych wynikających z odrębnych przepisów. Elementy wyniku oceny interoperacyjności krajowej zostały zamieszczone w załączniku nr 2 do projektowanego rozporządzenia.
92.	**Załącznik nr 5**	**MKiŚ**	W załączniku nr 5 do projektu w pkt 3 lit. c wskazano, że do oznaczania zależności hierarchicznej między zasobami stosuje się znak „/” – ukośnik wskazany w tablicy podstawowej znaków UTF-8 na pozycji 2215 – oraz że znaku tego nie zamieszcza się na końcu URI. Regulacja ta zawiera błąd merytoryczny. W standardzie URI określonym w RFC 3986 separatorem ścieżki jest znak U+002F SOLIDUS. Większość bibliotek URI, serwerów WWW, bram API, parserów OpenAPI i przeglądarek nie traktuje znaku U+2215 jako separatora ścieżki URI. Powyższy błąd wskazuje, że regulacje techniczne na tym poziomie szczegółowości nie powinny być zamieszczane w treści rozporządzenia, będącego aktem normatywnym, a nie dokumentem technicznym. Zasadne byłoby zastąpienie szczegółowych opisów odwołaniami do utrwalonych standardów technicznych, w szczególności RFC, W3C, OASIS, ISO oraz OGC. Należy przy tym zauważyć, że w innych miejscach projektu prawidłowo odwołano się do JSON Schema, OpenAPI, OAuth 2.0, OpenID Connect oraz XML Schema, zamiast powtarzać treść tych specyfikacji w rozporządzeniu.	**Uwaga uwzględniona** W RFC 3986 separatorem ścieżki URI jest znak U+002F.

93.	**Załącznik nr 5 - część 1**	**MRiRW**	Proponuje się ograniczenie załącznika do wymagań niezbędnych do zapewnienia interoperacyjności, natomiast szczegółowe reguły projektowania API przenieść do standardu lub wytycznych, które mogą być aktualizowane niezależnie od rozporządzenia. Załącznik określa bardzo szczegółowo sposób projektowania API, w tym strukturę URI, sposób nazewnictwa zasobów, HATEOAS, JSON API, JSON-LD, wersjonowanie, metadane, sposób ograniczania ruchu czy mechanizmy uwierzytelniania. Część tych rozwiązań ma charakter reguł projektowych, które mogą zmieniać się szybciej niż przepisy prawa.	**Uwaga wyjaśniona** Specyfikacja API pozostaje załącznikiem do rozporządzenia. Jednocześnie należy podać, że art. 18a ustawy z dnia 17 lutego 2005 r. o informatyzacji działalności podmiotów realizujących zadania publiczne stanowi, że „Rada Ministrów upoważnia ministra właściwego do spraw informatyzacji do: 1) dokonywania nie rzadziej niż raz na 3 lata przeglądu standardów oraz specyfikacji, o których mowa w przepisach wydanych na podstawie art. 18, w szczególności w celu ich oceny pod kątem zapewniania interoperacyjności, w tym stwierdzenia: a) stopnia ich zgodności z aktualnymi, opublikowanymi normami, które zostały zatwierdzone przez międzynarodową, europejską lub krajową jednostkę normalizacyjną – z uwzględnieniem otwartych standardów i specyfikacji oraz zasady równego traktowania różnych rozwiązań informatycznych, b) stopnia ich zgodności z europejskimi ramami interoperacyjności, o których mowa w art. 6 ust. 1 rozporządzenia 2024/903, c) zakresu i stopnia ich stosowania przez podmioty realizujące zadania publiczne; (…)”.
94.	**Załącznik nr 5 pkt 1.1 lit. b) i c)**	**MFiG (MF)**	czy faktycznie i celowo zdefiniowano JSON5 a dalej JSON (to są różne standardy JSON5 vs JSON).	**Uwaga uwzględniona** Intencją projektodawcy jest stosowanie formatu JSON zgodnego z powszechnie przyjętym standardem JavaScript Object Notation. Usunięto odwołanie do JSON5, pozostawiono natomiast JSON. W celu zapewnienia standard JSON został określony w załączniku nr 1 poprzez odwołanie do specyfikacji RFC 8259.
95.	**Załącznik nr 5 pkt 1 ppkt 1 lit. b-e**	**MRiRW**	Proponuje się ponowne przeanalizowanie obowiązku jednoczesnego stosowania JSON, JSON Schema, JSON API oraz JSON-LD i pozostawienie możliwości doboru sposobu reprezentacji danych odpowiednio do charakteru API. Zestawienie	**Uwaga wyjaśniona** Wymienione standardy pełnią różne funkcje i nie są względem siebie komplementarne w każdym przypadku.

			kilku standardów jako obowiązkowych może powodować niepotrzebne komplikowanie prostych interfejsów oraz konieczność przebudowy istniejących API, mimo że zapewniają one jednoznaczną i dobrze udokumentowaną wymianę danych. Wymaganiem podstawowym powinno być jednoznaczne określenie struktury, semantyki i sposobu wymiany danych.	JSON jest formatem reprezentacji danych. JSON Schema służy do formalnego opisu struktury danych i reguł ich walidacji. JSON-LD jest rozszerzeniem JSON przeznaczonym do publikowania danych powiązanych (linked data) i nadawania im jednoznacznej semantyki. Natomiast JSON API jest specyfikacją organizacji interfejsu REST, obejmującą m.in. strukturę zasobów, relacji, filtrowania, sortowania i stronicowania. Wymagania te dotyczą różnych warstw interoperacyjności i nie zawsze muszą występować łącznie.
96.	**Zał. nr 5, pkt 1 ppkt 1 lit. b**	**MFiG (MRiT)**	Wskazano format „JSON5", który jest odrębnym, nieustandaryzowanym rozszerzeniem JSON, niezgodnym z RFC 8259. Jeżeli intencją jest JSON wg RFC 8259, postulujemy wskazanie tego wprost.	**Uwaga uwzględniona** Wyjaśnienia podano w odpowiedzi na uwagę nr 94.
97.	**Załącznik nr 5 – pkt 1.3 lit. c**	**MFiG (MF)**	do oznaczania zależności hierarchicznej między zasobami w URI (unikalny identyfikator zasobów) stosowany jest raczej znak / z pozycji 47 w tablicy UTF-8 (forward slash) a nie znak z pozycji 2215 (division slash).	**Uwaga uwzględniona** Wyjaśnienia podano w odpowiedzi na uwagę nr 92.
98.	**Załącznik nr 5 pkt 1 ppkt 4 lit. c-e**	**MRiRW**	Proponuje się uzależnienie obowiązku stosowania HATEOAS od charakteru udostępnianego API. Proponowane brzmienie: „API wykorzystuje technikę HATEOAS, jeżeli jest to uzasadnione charakterem udostępnianego API, sposobem jego wykorzystania oraz potrzebą dynamicznego odkrywania powiązanych zasobów i dostępnych operacji.". HATEOAS jest szczególnie użyteczny w przypadku API udostępnianych zewnętrznym odbiorcom, gdy istotne jest ograniczenie zależności klienta od z góry znanej struktury URI oraz umożliwienie nawigowania pomiędzy powiązanymi zasobami na podstawie informacji zwracanych przez API. Nie każdy interfejs objęty wymaganiami załącznika nr 5 ma jednak taki charakter. W przypadku zamkniętych integracji system-system, opartych na stabilnym i uzgodnionym kontrakcie API, obowiązkowe stosowanie HATEOAS może zwiększać złożoność rozwiązania bez proporcjonalnej korzyści dla interoperacyjności. Zasadne jest	**Uwaga uwzględniona** Zmieniono brzmienie pkt 1 ppkt 4 lit. c aktualnego załącznika nr 4 na następujące: c) API używa techniki HATEOAS (Hypermedia As The Engine Of Application State), jeżeli jest to uzasadnione charakterem udostępnianego API, sposobem jego wykorzystania oraz potrzebą dynamicznego odkrywania powiązanych zasobów i dostępnych operacji. W przypadku stosowania HATEOAS wymagane jest, aby: - linki zawarte w ciele lub nagłówkach odpowiedzi zawierały identyfikatory URI do zasobów powiązanych, - linki do zasobów powiązanych są dostępne zarówno w ciele odpowiedzi, jak i w nagłówkach odpowiedzi API, - linki zawarte w ciele lub nagłówkach odpowiedzi jednoznacznie wskazują

			zatem powiązanie tego wymagania z charakterem i sposobem wykorzystania udostępnianego API.	identyfikatory URI dla zasobów powiązanych.
99.	**Załącznik nr 5 pkt 1 ppkt 12 lit. d**	**MRiRW**	Proponuje się jednoznaczne wskazanie OpenAPI jako standardu opisu REST API oraz określenie minimalnego zakresu informacji, które powinny być zawarte w specyfikacji, tak aby mogła ona stanowić podstawę do automatycznej prezentacji dokumentacji API w narzędziach takich jak Swagger UI. Proponowane brzmienie: „Dokumentacja REST API jest udostępniana w postaci zgodnej ze standardem OpenAPI w wersji 3.0 lub nowszej. Specyfikacja OpenAPI powinna zawierać opisy zasobów, operacji, parametrów, struktur danych, kodów odpowiedzi, błędów oraz przykładowych żądań i odpowiedzi w zakresie umożliwiającym automatyczne wygenerowanie czytelnej i interaktywnej dokumentacji API, w szczególności z wykorzystaniem narzędzi zgodnych ze standardem OpenAPI.”. Sam obowiązek udostępnienia pliku OpenAPI nie gwarantuje jeszcze użytecznej dokumentacji dla klientów API. Istotne jest, aby opisy poszczególnych operacji, parametrów, modeli danych, kodów odpowiedzi i błędów były na tyle kompletne, aby specyfikacja mogła być bezpośrednio wykorzystana do prezentacji API w narzędziach takich jak Swagger UI oraz do wsparcia procesu integracji. Dobrze przygotowana specyfikacja OpenAPI pozwala w dużym stopniu utrzymywać dokumentację razem z kontraktem API i ogranicza ryzyko rozbieżności pomiędzy implementacją a osobno prowadzoną dokumentacją.	**Uwaga wyjaśniona** Aktualny załącznik nr 4 wskazuje OpenAPI jako standard opisu REST API poprzez zapis „Spełnienie tych wymagań możliwe jest poprzez stosowanie standardu OpenAPI w wersji 3.0 lub nowszej (…)”.
100.	**Załącznik nr 5 pkt 1 ppkt 6 lit. c-f**	**MRiRW**	Proponuje się wskazanie, że zakres metadanych jest dobierany odpowiednio do rodzaju zasobu i sposobu wykorzystania API. Wymieniony w projekcie zestaw obejmuje m.in. licencję, katalog, zakres czasowy danych, częstotliwość aktualizacji czy datę zakończenia publikacji. Taki zestaw jest właściwy dla części API służących udostępnianiu zbiorów danych, ale nie wszystkie te informacje mają zastosowanie do interfejsów transakcyjnych lub integracji system-system.	**Uwaga częściowo uwzględniona** Pozostawiono minimalny zestaw metadanych, ale usunięto z niego dotychczasowe obowiązkowe metadane: licencja oraz katalog.
101.	**Załącznik nr 5 pkt 1 ppkt 8 lit. g**	**MRiRW**	Proponuje się odejście od sztywnego, co najmniej dwuletniego okresu utrzymywania wycofywanej wersji API. Okres przejściowy powinien być ustalany z uwzględnieniem liczby i charakteru systemów korzystających z API oraz czasu potrzebnego na ich	**Uwaga wyjaśniona** Załącznik określa, że poza uzasadnionymi wypadkami nie należy wycofywać obsługi wersji API szybciej, niż dwa lata po powiadomieniu

			dostosowanie. Dwuletni okres może być uzasadniony dla interfejsów wykorzystywanych przez wielu odbiorców, ale w innych przypadkach będzie prowadził do niepotrzebnego utrzymywania kilku wersji API równolegle. Istotne jest zapewnienie odbiorcom realnej możliwości migracji, natomiast okres potrzebny na migrację może różnić się w zależności od interfejsu.	użytkowników. Oznacza to, że czas może być krótszy, niż określony, w przypadku podania uzasadnienia bazującego na analizie wykorzystania publicznego systemu teleinformatycznego.
102.	**Załącznik nr 5 pkt 1 ppkt 10 lit. c**	**MRiRW**	Proponuje się usunięcie zdania: „API nie może być zamknięte dla użytkowników nieuwierzytelnionych”. Proponowane brzmienie: „Zakres dostępu do API, w tym możliwość dostępu przez użytkowników nieuwierzytelnionych, określa podmiot realizujący zadania publiczne, z uwzględnieniem charakteru danych, podstawy prawnej dostępu oraz wymagań bezpieczeństwa.”. Część interfejsów administracji jest przeznaczona wyłącznie do komunikacji pomiędzy określonymi systemami i udostępnia dane, do których dostęp może mieć tylko wskazany krąg odbiorców. W takich przypadkach całkowite wyłączenie dostępu anonimowego jest rozwiązaniem właściwym. Obecny zapis może budzić wątpliwości, czy każde API powinno oferować choćby ograniczony dostęp użytkownikowi nieuwierzytelnionemu.	**Uwaga uwzględniona** Zmieniono brzmienie pkt 1 ppkt 10 lit. c aktualnego załącznika nr 4 na następujące: „c) zakres dostępu do API, w tym możliwość dostępu przez użytkowników nieuwierzytelnionych, określa podmiot realizujący zadania publiczne, z uwzględnieniem charakteru danych, podstawy prawnej dostępu oraz wymagań bezpieczeństwa.(…)”.
103.	**Załącznik nr 5 pkt 1 ppkt 10 lit. d-e**	**MRiRW**	Proponuje się rozdzielenie mechanizmów uwierzytelniania i autoryzacji oraz jednoznaczne przypisanie im właściwych standardów. Proponowane brzmienie: d) „uwierzytelnianie użytkowników API realizuje się z wykorzystaniem OpenID Connect;” e) „autoryzację dostępu do zasobów API realizuje się z wykorzystaniem OAuth 2.0, z zastosowaniem mechanizmów i profili odpowiednich do rodzaju klienta oraz sposobu integracji;”. Obecne brzmienie łączy uwierzytelnianie i autoryzację w ramach OpenID Connect, a jednocześnie wskazuje OAuth 2.0 jako rozwiązanie wymagające uzupełnienia w zakresie autoryzacji. Takie sformułowanie jest nieprecyzyjne. OpenID Connect służy przede wszystkim do uwierzytelniania i przekazywania informacji o tożsamości, natomiast OAuth 2.0 służy do autoryzacji dostępu do zasobów. Rozdzielenie obu funkcji zwiększy jednoznaczność	**Uwaga uwzględniona** Zmieniono brzmienie pkt 1 ppkt 10 lit. d-e aktualnego załącznika nr 4 na następujące: „d) uwierzytelnianie użytkowników API realizuje się z wykorzystaniem OpenID Connect, e) autoryzację dostępu do zasobów API realizuje się z wykorzystaniem OAuth 2.0, z zastosowaniem mechanizmów i profili odpowiednich do rodzaju klienta oraz sposobu integracji”.

			wymagań i ułatwi ich spójne stosowanie w systemach administracji publicznej.	
104.	**Załącznik nr 5 pkt 1 ppkt 11 lit. c**	**MRiRW**	Proponuje się zmianę zapisu dotyczącego kluczy API tak, aby rozróżnić klucze API od tokenów dostępowych oraz objąć oba mechanizmy zasadami zarządzania ich cyklem życia. Proponowane brzmienie: „Poświadczenia wykorzystywane do dostępu do API, w tym klucze API, tokeny dostępowe oraz tokeny odświeżające, są generowane, przechowywane i przekazywane w sposób zapewniający ich bezpieczeństwo oraz podlegają zarządzaniu cyklem życia, obejmującemu w szczególności określenie okresu ważności, rotację oraz możliwość unieważnienia; w przypadku stosowania tokenów w formacie JSON Web Token (JWT) stosuje się właściwy standard JWT.”. Obecne brzmienie, zgodnie z którym „klucze API są konstruowane zgodnie z zasadami konstrukcji tokenów Web JSON”, łączy dwa różne mechanizmy. Klucz API jest poświadczeniem identyfikującym klienta lub aplikację, natomiast token dostępowy może zawierać informacje dotyczące przyznanego dostępu, jego zakresu i okresu ważności. Token może być zapisany w formacie JWT, ale nie oznacza to, że klucz API powinien być konstruowany według zasad właściwych dla JWT. Zarówno klucze API, jak i tokeny powinny podlegać zarządzaniu przez cały okres ich używania, w tym rotacji i możliwości unieważnienia.	**Uwaga uwzględniona** Zmieniono brzmienie pkt 1 ppkt 11 lit. c aktualnego załącznika nr 4 na następujące: „c) poświadczenia wykorzystywane do dostępu do API, w tym klucze API, tokeny dostępowe oraz tokeny odświeżające, są generowane, przechowywane i przekazywane w sposób zapewniający ich bezpieczeństwo oraz podlegają zarządzaniu cyklem życia, obejmującemu w szczególności określenie okresu ważności, rotację oraz możliwość unieważnienia; w przypadku stosowania tokenów w formacie JSON Web Token (JWT) stosuje się właściwy standard JWT,”.
105.	**Załącznik nr 5 pkt 1 ppkt 11 lit. e-j**	**MRiRW**	Proponuje się zastąpienie szczegółowych wymagań dotyczących białych i czarnych list adresów IP ogólnym obowiązkiem stosowania mechanizmów ochrony API przed nadużyciem, przeciążeniem oraz atakami. Mechanizmy ochrony API zależą od stosowanej infrastruktury. Współczesne rozwiązania wykorzystują m.in. API Gateway, WAF, ochronę DDoS, limity ruchu i mechanizmy dynamicznej analizy zagrożeń. Sztywne wskazanie sposobu zarządzania adresami IP może ograniczać możliwość zastosowania skuteczniejszych mechanizmów bezpieczeństwa.	**Uwaga uwzględniona** Zmieniono brzmienie pkt 1 ppkt 11 lit. e-j aktualnego załącznika nr 4 na następujące: e) stosowane mechanizmy ochrony obejmują co najmniej: - ograniczanie liczby żądań lub wolumenu danych, - różnicowanie poziomu dostępu użytkowników lub kategorii użytkowników, - wykrywanie i ograniczanie ruchu mogącego zagrażać ciągłości działania API, - możliwość czasowego lub trwałego ograniczenia dostępu podmiotom generującym ruch naruszający przyjęte zasady korzystania z API,

				f) zasady ograniczania ruchu oraz korzystania z API są udokumentowane i publicznie dostępne w zakresie niepowodującym obniżenia bezpieczeństwa systemu, g) w przypadku zastosowania ograniczeń skutkujących odrzuceniem żądania API zwraca komunikat zgodny ze standardem HTTP, w szczególności kod odpowiedzi 429 Too Many Requests, wraz z informacją umożliwiającą identyfikację przyczyny ograniczenia, h) dostęp może zostać ograniczony podmiotom generującym ruch, który zgodnie z przyjętymi regułami bezpieczeństwa został zakwalifikowany jako zagrażający bezpieczeństwu lub stabilności API, i) zastosowane mechanizmy ograniczania dostępu podlegają okresowym przeglądom wynikającym z analizy ryzyka, j) podmiot realizujący zadania publiczne udostępniający API stosuje udokumentowane zasady ograniczania transferu danych oraz podejmuje działania służące utrzymaniu i podnoszeniu wydajności API,”.
106.	**Załącznik nr 5 pkt 1 ppkt 3 lit. c**	**MRiRW**	Proponuje się wskazanie, że znak „/” stosowany jako separator zależności hierarchicznej w URI powinien być używany zgodnie z RFC 3986. Odwołanie bezpośrednio do standardu RFC 3986 pozwala jednoznacznie określić sposób stosowania separatora w URI i uniknąć wątpliwości wynikających z dodatkowego wskazywania reprezentacji znaku.	**Uwaga uwzględniona** Wyjaśnienia podano w odpowiedzi na uwagę nr 92.
OSR				
107.	**OSR**	**MI**	Projekt rozporządzenia wprowadza szereg nowych obowiązków technicznych i organizacyjnych, których realizacja będzie wymagała poniesienia istotnych nakładów finansowych przez podmioty realizujące zadania publiczne. W przypadku nieuwzględnienia ww. uwag (tj. nr 7-13), alternatywnie należy zapewnić dedykowany program finansowania lub mechanizm wsparcia umożliwiający sfinansowanie dostosowania systemów	**Uwaga wyjaśniona** Obowiązki, o których mowa w projekcie rozporządzenia wynikają z przepisów ustawy o informatyzacji. Zgodnie z upoważnieniem ustawowym, zawartym w art. 18 ustawy z dnia 17 lutego 2005 r. o informatyzacji działalności podmiotów realizujących zadania publiczne,

			teleinformatycznych do wymagań rozporządzenia. Projekt bowiem nakłada nowe obowiązki obejmujące m.in.: - wdrożenie i utrzymanie API zgodnych z wymaganiami określonymi w załączniku nr 5 do projektu rozporządzenia, - przeprowadzenie ocen interoperacyjności krajowej, - wdrożenie mechanizmów powiadamiania o zmianach danych w czasie rzeczywistym, - zapewnienie pełnej rozliczalności operacji w rejestrach publicznych, - przygotowanie i utrzymywanie planów ciągłości działania oraz odtworzenia po awarii, - zapewnienie dostępności cyfrowej dokumentów. Obowiązki te mogą wymagać modernizacji wielu istniejących systemów, integracji z nowymi usługami, dostosowania architektury danych, przygotowania dokumentacji, przeprowadzenia analiz oraz zakupu usług i kompetencji specjalistycznych. Część tych działań będzie wymagała zaangażowania wykonawców zewnętrznych oraz przeprowadzenia postępowań zakupowych. Jednocześnie w Ocenie Skutków Regulacji wskazano, że koszty dostosowania podmiotów publicznych do nowych wymagań zostały oszacowane łącznie na około 471,5 mln zł, co potwierdza znaczącą skalę obciążeń finansowych związanych z wdrożeniem projektowanych przepisów. Jednak w samym projekcie rozporządzenia nie zapewniono środków na dostosowanie do projektowanych w rozporządzeniu zmian przez IMGW. W związku z powyższym proponuję utworzenie dedykowanego programu finansowania wdrożenia wymagań wynikających z rozporządzenia lub wskazanie w OSR do projektu rozporządzenia źródeł finansowania umożliwiających pokrycie kosztów dostosowania systemów teleinformatycznych podmiotów realizujących zadania publiczne. Ponadto należy uwzględnić, że dostosowanie systemów teleinformatycznych do wymagań określonych w załączniku nr 5 projektu rozporządzenia (w szczególności, jeżeli nie zostaną uwzględnione wymagania wcześniejsze) może wymagać przebudowy istniejących interfejsów API, modyfikacji architektury systemów, zmian w modelach wymiany danych, przygotowania i utrzymania dokumentacji, a także przeprowadzenia testów integracyjnych z systemami podmiotów zewnętrznych. W przypadku podmiotów posiadających rozbudowane środowiska teleinformatyczne koszty takich działań mogą znacząco przekraczać	projekt rozporządzenia określa szczegółowe sposoby realizacji obowiązków wynikających z przepisów ustawowych, tj. art. 13 ust. 1 pkt 1 i 2 oraz art. 14 ust. 1 ustawy o informatyzacji. W związku z tym wydatki podmiotów związane z realizacją zadań określonych w projekcie rozporządzenia zostały ujęte w OSR do projektu ustawy z dnia 25 lipca 2025 r. o zmianie ustawy o informatyzacji działalności podmiotów realizujących zadania publiczne oraz niektórych innych ustaw (Dz.U. oz.1158), jako wynikające z ww. ustawy. W OSR do ww. projektu ustawy znajdują się wyliczenia związane z realizacją obowiązków związanych m.in. wdrożeniem API. Projektowane rozporządzenie uzupełnia regulację ustawową związaną z realizacją obowiązków i nie generuje innych kosztów, poza wydatkami ujętymi w OSR ww. ustawy. Zgodnie z art. 50 ust. 7 ustawy z dnia 27 sierpnia 2009 r. o finansach publicznych wejście w życie przepisów wykonawczych nie może skutkować zmianą limitu wydatków jednostek sektora finansów publicznych określonego w ustawie, na podstawie której wydawane są przepisy wykonawcze.

			nakłady przewidywane dla standardowych systemów administracji publicznej.	
108.	**OSR - pkt 6 „Wpływ na sektor finansów publicznych”**	**MSWiA**	Proponuje się: - weryfikację sposobu oszacowania kosztów dostosowania systemów teleinformatycznych i rejestrów publicznych, z uwzględnieniem zróżnicowania ich skali, złożoności, liczby integracji, wolumenu przetwarzanych danych oraz zakresu zmian wymaganych do spełnienia nowych obowiązków, - aktualizację danych stanowiących podstawę oszacowania kosztów dostosowania systemów teleinformatycznych i rejestrów publicznych albo uzupełnienie kalkulacji o dane dotyczące aktualnego stanu środowisk teleinformatycznych podmiotów objętych regulacją, - ponowną analizę założenia, zgodnie z którym realizacja nowych obowiązków nie będzie stanowiła podstawy do zapewnienia dodatkowych środków finansowych, w szczególności w odniesieniu do podmiotów utrzymujących dużą liczbę złożonych systemów teleinformatycznych i rejestrów publicznych. OSR wskazuje, że podstawą kalkulacji są dane dotyczące systemów i nakładów uzupełniane w SIST w 2022 r. Rozporządzenie ma natomiast wejść w życie w 2027 r. Uwzględnienie jedynie współczynnika inflacji nie odzwierciedla zmian, które w tym czasie zaszły w architekturze systemów, liczbie integracji, wymaganiach dotyczących bezpieczeństwa, dostępności, ciągłości działania czy skali świadczonych usług cyfrowych. Wskazane byłoby wykorzystanie możliwie aktualnych danych lub dodatkowe zweryfikowanie kalkulacji na reprezentatywnej grupie dużych systemów administracji publicznej. Projekt wprowadza szereg nowych lub rozszerzonych obowiązków, dotyczących m.in. API, rozliczalności operacji, informowania o zmianach danych referencyjnych, planów ciągłości działania, dostępności cyfrowej czy oceny interoperacyjności. OSR wskazuje te wymagania jako nowe obciążenia regulacyjne, a jednocześnie zakłada ich finansowanie w ramach istniejących środków. W przypadku podmiotów posiadających rozbudowane środowiska teleinformatyczne może to oznaczać konieczność finansowania dostosowania kosztem innych zadań rozwojowych i utrzymaniowych. Zasadne byłoby uwzględnienie możliwości zapewnienia odpowiednich środków na dostosowanie,	**Uwaga wyjaśniona** Dane o nakładach zebrano także w 2024 roku i nie wpływają one na zmianę wyliczonej mediany nakładów na system.

			adekwatnych do rzeczywistego zakresu wymaganych zmian. Nie można zakładać, że każdy podmiot publiczny będzie posiadał środki na dostosowanie systemów do wymogów przedmiotowych przepisów.	
109.	**OSR pkt 6**	**MSWiA**	4) proponuję dokonanie ponownej analizy założeń finansowych przyjętych w OSR, w szczególności w odniesieniu do dużych i złożonych systemów teleinformatycznych resortu spraw wewnętrznych i administracji. Należy zauważyć, że w pkt 6 OSR do projektu w wierszu źródła finansowania wskazano, że cyt. „*Koszty realizacji zadań ministra właściwego do spraw informatyzacji zostaną sfinansowane w ramach części 27 budżetu państwa poprzez stosowne przesunięcia i zagospodarowanie obecnego potencjału rzeczowego i kadrowego. Regulacje nie będą stanowiły podstawy do ubiegania się o dodatkowe środki finansowe z budżetu państwa na ten cel.*”. W kwestii pozostałych kosztów podmiotów realizujących zadania wynikające z projektu w OSR wskazano w tym zakresie, że cyt. „*Wydatki podmiotów związane z realizacją zadań określonych w projekcie rozporządzenia zostały ujęte jako wydatki wynikające z ustawy z dnia 25 lipca 2025 r. o zmianie ustawy o informatyzacji działalności podmiotów realizujących zadania publiczne oraz niektórych innych ustaw i nie stanowią dodatkowych wydatków poza wskazanymi w ustawie*.”. Podkreślić należy, że OSR nie zawiera odrębnej analizy kosztów dostosowania systemów teleinformatycznych jednostek podległych i nadzorowanych przez ministra właściwego do spraw wewnętrznych (w tym Policji). Zastosowana w OSR metodologia szacowania kosztów opiera się na uśrednionych (medianowych) wartościach nakładów na pojedynczy rejestr publiczny i pojedynczy system teleinformatyczny, wyliczonych na podstawie danych z Systemu Inwentaryzacji Systemów Teleinformatycznych (SIST) z 2022 r., podwojonych jedynie ze względu na większą złożoność systemów administracji rządowej jako kategorii ogólnej (odpowiednio 9292,50 zł/rok/system oraz 4646,25 zł/rok/rejestr). Metodologia ta – ze swej natury uśredniona i oparta na danych sprzed kilku lat – nie odzwierciedla specyfiki, skali ani rzeczywistych kosztów dostosowania rozbudowanych, wyspecjalizowanych systemów teleinformatycznych np. Policji, w szczególności systemów integrujących dane z rejestrami krajowymi i międzynarodowymi	**Uwaga wyjaśniona** Podstawą oszacowania kosztów przyjętych w OSR są dane zgromadzone w Systemie Inwentaryzacji Systemów Teleinformatycznych (SIST), który stanowi jednolite źródło informacji o systemach teleinformatycznych i rejestrach publicznych podmiotów realizujących zadania publiczne. Metodologia kalkulacji została oparta na danych dostępnych w SIST, co zapewnia porównywalność i spójność szacunków dla wszystkich podmiotów objętych projektowaną regulacją. OSR ma charakter szacunkowy i przedstawia skutki regulacji na poziomie ogólnym dla wszystkich podmiotów objętych projektowanym rozporządzeniem. Obowiązki, o których mowa w projekcie rozporządzenia wynikają z przepisów ustawy z dnia 17 lutego 2005 r. o informatyzacji działalności podmiotów realizujących zadania publiczne. Zgodnie z upoważnieniem ustawowym, zawartym w art. 18 ustawy z dnia 17 lutego 2005 r. o informatyzacji działalności podmiotów realizujących zadania publiczne, projekt rozporządzenia określa szczegółowe sposoby realizacji obowiązków wynikających z przepisów ustawowych, tj. art. 13 ust. 1 pkt 1 i 2 oraz art. 14 ust. 1 ustawy z dnia 17 lutego 2005 r. o informatyzacji działalności podmiotów realizujących zadania publiczne. W związku z tym wydatki podmiotów związane z realizacją zadań określonych w projekcie rozporządzenia zostały ujęte w OSR do projektu ustawy z dnia 25 lipca 2025 r. o zmianie ustawy o informatyzacji działalności podmiotów realizujących zadania publiczne oraz niektórych

			oraz podlegających podwyższonym rygorom bezpieczeństwa. Ponadto zmieniające się uwarunkowania rynkowe powodują, że podane w projekcie koszty mogą być nieadekwatne. W tym stanie rzeczy istnieje realne ryzyko, że nałożone na Policję obowiązki o charakterze technicznym i organizacyjnym staną się w praktyce obowiązkami nieposiadającymi odrębnego zabezpieczenia finansowego, których realizacja będzie musiała nastąpić kosztem innych zadań finansowanych z budżetu własnego Policji. Mając na uwadze powyższe w Komendzie Głównej Policji są przygotowywane wyliczenia szczegółowych kosztów realizacji zadań wynikających z wejścia w życie ww. projektu rozporządzenia, które zostaną niezwłocznie przekazane do projektodawcy. *(uzupełnienie odp. przez MSWiA – 09.09.26*) Szacowane wyliczenia kosztów przygotowane przez Komendę Główną Policji uwzględniające: 1) liczbę systemów teleinformatycznych objętych zmianami – 10; 2) liczbę integracji z systemami (jeden system Policji może integrować się z wieloma innymi systemami) – 64; 3) zakres prac wynikający ze skutków zmian wprowadzonych rozporządzeniem, tj.: – analiza i projektowanie zmian, – wdrożenie API wg zał. nr 5 (§ 12), – rozliczalność/notyfikacje w czasie rzeczywistym (§ 8), – plan ciągłości działania i DR (§ 11 ust. 4–8), – dostępność cyfrowa dokumentów (§ 14 ust. 3–4), – ocena interoperacyjności krajowej (§ 4, zał. 4), – dostosowanie formatów plików (§ 14 ust. 1–2), – zarządzanie jakością danych (§ 6), – testy bezpieczeństwa (poza akredytacjami), – akredytacje systemów niejawnych. Dokonując analizy pracochłonności (analiza, projekt architektury, prace programistyczne, testy bezpieczeństwa, opracowanie dokumentacji), na podstawie znanych stawek rynkowych i wiedzy eksperckiej wskazać należy, że: – koszt ogółem przebudowy systemów wyniesie ok. 14,5 mln zł w okresie 2 lat, tj. 7,25 mln zł rocznie, – koszt ogółem utrzymania wyniesie 6 mln zł w okresie 10 lat, tj. 0,6 mln zł rocznie,	innych ustaw (Dz.U. oz.1158), jako wynikające z ww. ustawy. W OSR do ww. projektu ustawy znajdują się wyliczenia związane z realizacją obowiązków związanych m.in. wdrożeniem API. Projektowane rozporządzenie uzupełnia regulację ustawową związaną z realizacją obowiązków i nie generuje innych kosztów, poza wydatkami ujętymi w OSR ww. ustawy. Zgodnie z art. 50 ust. 7 ustawy z dnia 27 sierpnia 2009 r. o finansach publicznych wejście w życie przepisów wykonawczych nie może skutkować zmianą limitu wydatków jednostek sektora finansów publicznych określonego w ustawie, na podstawie której wydawane są przepisy wykonawcze.

			koszt całkowity zmiany wyniesie 20,5 mln zł.	