Projekt z dnia 29 lipca 2026 r.

# R O Z P O R Z Ą D Z E N I E

# R A D Y  M I N I S T R Ó W

z dnia … 2026 r.

**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[1)]**

Na podstawie 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) zarządza się, co następuje:

## Rozdział 1

## Przepisy ogólne

**§ 1.** Rozporządzenie określa szczegółowe sposoby realizacji obowiązków, o których mowa w 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 zakresie:

1) Krajowych Ram Interoperacyjności;
2) minimalnych wymagań dla rejestrów publicznych;
3) minimalnych wymagań dla systemów teleinformatycznych używanych do realizacji zadań publicznych i wymiany danych z podmiotami publicznymi.

**§ 2.** Użyte w rozporządzeniu określenia oznaczają:

1) architektura systemu teleinformatycznego – podstawową organizację systemu teleinformatycznego wraz z jego komponentami, wzajemnymi powiązaniami, środowiskiem pracy i regułami ustanawiającymi sposób jego budowy i rozwoju;

---

[1)] Niniejsze rozporządzenie zostało notyfikowane Komisji Europejskiej w dniu ….. 2025 r. pod numerem 2025/…../PL, zgodnie z § 4 rozporządzenia Rady Ministrów z dnia 23 grudnia 2002 r. w sprawie sposobu funkcjonowania krajowego systemu notyfikacji norm i aktów prawnych (Dz. U. poz. 2039 oraz z 2004 r. poz. 597), które wdraża dyrektywę (UE) 2015/1535 Parlamentu Europejskiego i Rady z dnia 9 września 2015 r. ustanawiającą procedurę udzielania informacji w dziedzinie przepisów technicznych oraz zasad dotyczących usług społeczeństwa informacyjnego (ujednolicenie) (Dz. Urz. UE L 241 z 17.09.2015, str. 1).

2) atrybut – właściwość obiektu;
3) autentyczność – właściwość polegającą na tym, że pochodzenie lub zawartość danych opisujących obiekt są takie, jak deklarowane;
4) dana - wartość atrybutu wyrażona ilościowo lub jakościowo w określonym typie danych;
5) dana referencyjna – daną w rejestrze publicznym, która jest autentycznym i wiążącym źródłem dla innych danych;
6) dostępność – właściwość określającą, że zasób systemu teleinformatycznego jest możliwy do wykorzystania przez uprawnionego użytkownika lub system teleinformatyczny, w czasie zadeklarowanym przez podmiot używający systemu teleinformatycznego do realizacji zadań publicznych;
7) elektroniczna usługa publiczna - działanie wykonywane przez podmiot realizujący zadania publiczne, pozwalające usługobiorcy na spełnienie obowiązku lub zrealizowanie uprawnienia, określonego na gruncie przepisów prawa, za pomocą środków komunikacji elektronicznej;
8) integralność – właściwość polegającą na tym, że zasób systemu teleinformatycznego nie został zmodyfikowany w sposób nieuprawniony;
9) model usługowy – 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);
10) niezaprzeczalność – właściwość określającą zdolność do udowodnienia zaistnienia danego zdarzenia lub działania i jego źródła;
11) niezawodność - stopień, w jakim system teleinformatyczny wykonuje określone funkcje w określonych warunkach przez określony czas;
12) obiekt – wyodrębniony element rzeczywistości, o którym przechowuje się informacje w rejestrze publicznym lub systemie teleinformatycznym używanym do realizacji zadań publicznych;
13) obiekt przestrzenny – obiekt przestrzenny w rozumieniu przepisów ustawy z dnia 4 marca 2010 r. o infrastrukturze informacji przestrzennej (Dz. U. z 2025 r. poz. 242);
14) pielęgnowalność - stopień, w jakim system teleinformatyczny może być modyfikowany w celu poprawy, korekty błędów lub dostosowania do zmian środowiska i wymagań;

15) podmiot – osobę prawną, jednostkę organizacyjną nieposiadającą osobowości prawnej lub organ administracji publicznej;
16) poufność – właściwość zapewniającą, że informacja nie jest udostępniana lub wyjawiana nieupoważnionym osobom fizycznym lub podmiotom;
17) procedura - ustalony sposób wykonania działania lub procesu;
18) proces - zbiór działań wzajemnie powiązanych lub wzajemnie oddziałujących, które realizowane są w celu dostarczenia zamierzonego rezultatu;
19) przenoszalność - stopień, w jakim system teleinformatyczny może być przeniesiony z jednego środowiska sprzętowego, programowego lub organizacyjnego do innego;
20) rozliczalność – właściwość systemu teleinformatycznego pozwalającą przypisać określone działanie w tym systemie do osoby fizycznej lub procesu oraz umiejscowić je w czasie;
21) usługa systemu teleinformatycznego - usługę związana z urządzeniem informatycznym, oprogramowaniem lub danymi przetwarzanymi w systemie teleinformatycznym;
22) ustawa o informatyzacji - ustawę z dnia 17 lutego 2005 r. o informatyzacji działalności podmiotów realizujących zadania publiczne;
23) użyteczność - stopień, w jakim system teleinformatyczny może być używany przez użytkowników do osiągania określonych celów - z efektywnością, skutecznością i satysfakcją w określonym kontekście użycia;
24) wydajność - zdolność systemu teleinformatycznego do realizacji zadań w określonym czasie przy zadanym obciążeniu;
26) zasób systemu teleinformatycznego – urządzenie informatyczne, oprogramowanie lub dane przetwarzane w systemie teleinformatycznym.

Rozdział 2

**Krajowe Ramy Interoperacyjności**

**§ 3**. 1. Podmiot realizujący zadania publiczne stosuje rozwiązania z zakresu interoperacyjności na poziomach: organizacyjnym, semantycznym i technicznym.

2. Stosowanie rozwiązań z zakresu interoperacyjności, o których mowa w ust. 1, nie może naruszać zasady neutralności technologicznej.

3. Interoperacyjność na poziomie organizacyjnym osiągana jest przez:

1) informowanie przez podmiot realizujący zadania publiczne o zakresie funkcjonalnym oraz o sposobie dostępu do elektronicznych usług publicznych, świadczonych przez ten

podmiot, w tym informowanie o tych usługach w formacie nadającym się do odczytu maszynowego, zgodnie z załącznikiem nr 2 do rozporządzenia, w części C, w punkcie 1.1;

2) tworzenie, standaryzację i ujednolicenie procesów oraz procedur na potrzeby realizacji zadań publicznych za pomocą środków komunikacji elektronicznej z uwzględnieniem konieczności zapewnienia poprawnej współpracy podmiotów realizujących zadania publiczne, w tym efektywnej wymiany danych;

3) publikowanie i uaktualnianie na stronie podmiotowej w Biuletynie Informacji Publicznej przez podmiot realizujący zadania publiczne opisów procedur obowiązujących przy załatwianiu spraw z zakresu jego właściwości za pomocą środków komunikacji elektronicznej.

4. Interoperacyjność na poziomie semantycznym osiągana jest przez:

1) stosowanie minimalnych wymagań dla rejestrów publicznych określonych w rozdziale 3;

2) stosowanie struktur danych i znaczenia danych zawartych w tych strukturach, a także słowników, schematów klasyfikacyjnych, taksonomii oraz list kodowych dla danych w rejestrze publicznym, zgodnie z informacjami opublikowanymi w repozytorium interoperacyjności, o którym mowa w art. 12k ustawy o informatyzacji;

3) stosowanie w rejestrach publicznych odwołań do rejestrów publicznych zawierających dane referencyjne w zakresie niezbędnym do realizacji zadań publicznych;

4) stosowanie formatów plików określonych w załącznikach nr 2 i 3 do rozporządzenia.

5. Interoperacyjność na poziomie technicznym osiągana jest przez:

1) stosowanie minimalnych wymagań dla systemów teleinformatycznych używanych do realizacji zadań publicznych i wymiany danych z podmiotami publicznymi, określonych w rozdziale 4;

2) korzystanie z interfejsów programistycznych aplikacji systemów teleinformatycznych używanych do realizacji zadań publicznych, zgodnie z informacjami opublikowanymi w repozytorium interoperacyjności.

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.

7. Interoperacyjność na poziomach wskazanych w ust. 1 osiągana jest również przez stosowanie regulacji zawartych w przepisach odrębnych, a w przypadku ich braku - przez uwzględnianie postanowień odpowiednich norm zatwierdzonych przez międzynarodową,

europejską lub krajową jednostkę normalizacyjną – z uwzględnieniem otwartych standardów i specyfikacji.

**§ 4.** 1. Podmiot realizujący zadania publiczne przeprowadza ocenę interoperacyjności krajowej, o której mowa w art. 12n ust. 1 ustawy o informatyzacji, na poziomach interoperacyjności wskazanych w § 3 ust. 1.

2. Podmiot realizujący zadania publiczne uwzględnia elementy oceny interoperacyjności krajowej stanowiące załącznik nr 4 do rozporządzenia.

Rozdział 3

**Minimalne wymagania dla rejestrów publicznych**

**§ 5**. 1. W rejestrach publicznych wyróżnia się w szczególności następujące typy obiektów:

1) osobę fizyczną;
2) podmiot;
3) obiekt przestrzenny.

2. Dla każdego obiektu, o którym mowa w ust. 1, w obrębie danego typu, nadaje się unikatowy identyfikator.

3. Strukturę identyfikatorów obiektów, o których mowa w ust. 1 pkt 1 i 2, a także pkt 3 w zakresie dotyczącym punktu adresowego i działki ewidencyjnej, z zastrzeżeniem ust. 5 i 6, określa załącznik nr 1 do rozporządzenia.

4. Przepis ust. 2 w związku z ust. 1 pkt 3 nie wyłącza 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 i 1824 oraz z 2025 r. poz. 1019, 1542 i 1792).

5. Jeśli podmiot prowadzi rejestr publiczny obejmujący typ obiektu, jakim są osoby fizyczne nieposiadające numeru PESEL, identyfikacja takiej osoby odbywa się według unikatowego identyfikatora właściwego dla danego rejestru.

6. Jeśli podmiot prowadzi rejestr publiczny obejmujący typ obiektu, jakim są podmioty nieposiadające nadanego numeru identyfikacyjnego REGON, identyfikacja takiego podmiotu odbywa się według unikatowego identyfikatora właściwego dla danego rejestru.

**§ 6.** 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.

2. System teleinformatyczny, za pomocą którego są zbierane lub aktualizowane dane na potrzeby rejestru publicznego, zapewnia stosowanie – w ramach graficznego interfejsu użytkownika i interfejsów programistycznych aplikacji – ustalonych reguł kontroli wprowadzanych danych wraz z odpowiednimi objaśnieniami.

**§ 7**. Zasady dostępu do rejestru publicznego, o których mowa w art. 14 ust. 1 ustawy o informatyzacji, obejmują:

1) aspekt przedmiotowy i podmiotowy uwzględniany przy opracowaniu oraz aktualizowaniu przez podmiot prowadzący rejestr publiczny warunków i procedury dostępu do danych gromadzonych w rejestrze publicznym, o których mowa w art. 14 ust. 1a pkt 3 lit. b ustawy o informatyzacji;
2) aspekt techniczny uwzględniany przy zapewnieniu zasad dostępu do systemu teleinformatycznego określonych w minimalnych wymaganiach dla systemów teleinformatycznych używanych do realizacji zadań publicznych i wymiany danych z podmiotami publicznymi - o ile rejestr publiczny prowadzony jest z wykorzystaniem systemu teleinformatycznego.

**§ 8**. 1. Podmiot prowadzący rejestr publiczny przy użyciu systemu teleinformatycznego zapewnia rozliczalność wszystkich operacji na danych tego rejestru publicznego.

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.

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 przy pomocy interfejsów programistycznych aplikacji systemów teleinformatycznych, przy użyciu których zapewniany jest dostęp do rejestru publicznego.

**§ 9.** Informacje o pojedynczym punkcie kontaktowym dla rejestru publicznego, o którym mowa w art. 14 ust. 1a pkt 4 ustawy o informatyzacji, zawierają w szczególności:

1) adres poczty elektronicznej;
2) adres do doręczeń elektronicznych.

## Rozdział 4

## Minimalne wymagania dla systemów teleinformatycznych używanych do realizacji zadań publicznych i wymiany danych z podmiotami publicznymi

**§ 10**. 1. Dla systemów teleinformatycznych używanych do realizacji zadań publicznych stosuje się rozwiązania oparte na modelu usługowym.

2. W przypadkach uzasadnionych specyfiką podmiotu realizującego zadania publiczne lub świadczonych przez niego elektronicznych usług publicznych dopuszcza się inny model architektury systemu teleinformatycznego.

**§ 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, przy zastosowaniu norm oraz uznanych w obrocie profesjonalnym standardów i metodyk.

2. Zarządzanie usługami systemów teleinformatycznych ma na celu dostarczanie tych usług na gwarantowanym poziomie dostępności i odbywa się w oparciu o udokumentowane procedury.

3. 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.

4. Podmiot realizujący zadania publiczne, świadczący elektroniczne usługi publiczne, ustanawia plan ciągłości świadczenia elektronicznych usług publicznych oraz plan przywracania po awarii tych usług, obejmujące środki organizacyjne i techniczne w celu zapewnienia ich dostępności.

5. Przy tworzeniu planu ciągłości świadczenia oraz planu przywracania po awarii, o których mowa w ust. 4, uwzględnia się:

1) wyniki przeprowadzonych analiz ryzyka;
2) wskazanie elektronicznych usług publicznych i procesów ich realizacji,;
3) wartości docelowych czasów odzyskiwania (Recovery Time Objective, RTO) dla usług i procesów, o których mowa w pkt 2, uznanych za priorytetowe;
4) wartości docelowych punktów odzyskania (Recovery Point Objective, RPO) dla usług i procesów, o których mowa w pkt 2, uznanych za priorytetowe.

6. Procedury planu ciągłości świadczenia elektronicznych usług publicznych oraz planu przywracania po awarii tych usług zawierają w szczególności:

1) zakres ról i odpowiedzialności zespołów, które będą realizowały te plany;
2) zakres działań realizowanych w ramach tych planów;
3) informacje pomocnicze potrzebne do rozpoczęcia działań, w tym kryteria rozpoczęcia działań oraz informacje pomocnicze potrzebne do prowadzenia koordynacji i komunikacji działań zespołów;
4) wartości docelowych czasów odzyskiwania i docelowych punktów odzyskania, o których mowa w ust. 5 pkt 3 i 4;
5) instrukcje i procedury dotyczące wdrażania poszczególnych działań;
6) wymagania dotyczące środków niezbędnych do realizacji planu;
7) wymagania dotyczące sprawozdawczości oraz oceny.

7. Plan ciągłości świadczenia elektronicznych usług publicznych oraz plan przywracania po awarii tych usług są:

1) zatwierdzone w sposób przyjęty w podmiocie realizującym zadania publiczne;
2) ewaluowane w drodze ćwiczeń i testów;
3) poddawane systematycznym przeglądom, a wyniki przeglądów z rekomendacjami zmian przedstawiane do zatwierdzenia kierownictwu podmiotu realizującego zadania publiczne;
4) poddawane aktualizacjom i ich zatwierdzeniu w sposób przyjęty w podmiocie realizującym zadania publiczne w przypadku zmian, które wpływają w istotny sposób na zawartość planów.

8. Wymagania określone w ust. 4-7 uznaje się za spełnione, jeśli plan ciągłości świadczenia elektronicznych usług publicznych oraz plan przywracania po awarii tych usług są ustanowione i realizowane na podstawie normy PN-EN ISO 22301.

**§ 12.** 1. System teleinformatyczny używany do realizacji zadań publicznych jest wyposażony w interfejsy programistyczne aplikacji, zgodne ze specyfikacją, określoną w załączniku nr 5 do rozporządzenia.

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.

3. System teleinformatyczny używany do realizacji zadań publicznych wyposaża się w składniki sprzętowe lub oprogramowanie umożliwiające wymianę danych z innymi

systemami teleinformatycznymi, za pomocą protokołów komunikacyjnych i szyfrujących, określonych w obowiązujących przepisach lub normach zatwierdzonych przez międzynarodową, europejską lub krajową jednostkę normalizacyjną.

4. W przypadku, gdy brak jest przepisów lub norm, o których mowa w ust. 3, stosuje się standardy uznane na poziomie międzynarodowym – z uwzględnieniem otwartych standardów i specyfikacji, w szczególności opracowane przez:

1) Internet Engineering Task Force (IETF) i publikowane w postaci Request For Comments (RFC);
2) World Wide Web Consortium (W3C) i publikowane w postaci W3C Recommendation (REC)

- odpowiednio do potrzeb wynikających z realizowanych zadań oraz bieżącego stanu technik informatycznych.

**§ 13.** 1. Kodowanie znaków w dokumentach wysyłanych z systemu teleinformatycznego używanego do realizacji zadań publicznych lub odbieranych przez taki system, także w odniesieniu do danych wymienianych przez ten system z innymi systemami na drodze teletransmisji, o ile wymiana ta ma charakter wymiany znaków, odbywa się według standardu Unicode UTF-8 określonego przez normę ISO/IEC 10646 wraz ze zmianami lub normę ją zastępującą.

2. W ramach kodowania znaków, o którym mowa w pkt 1, nie stosuje się znacznika kolejności bajtów (Byte Order Mark, BOM) chyba, że konieczność jego zastosowania wynika z udokumentowanej analizy dla systemu teleinformatycznego.

**§ 14.** 1. Udostępnianie danych przetwarzanych w systemie teleinformatycznym używanym do realizacji zadań publicznych odbywa się w co najmniej jednym z formatów plików lub standardów określonych w załączniku nr 2 do rozporządzenia.

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 załącznikach nr 2 i 3 do rozporządzenia.

3. Dokumenty przygotowane w formatach plików określonych w załączniku nr 2 do rozporządzenia, w części A, w punktach 1.2, 1.3, 1.4 i 1.6 oraz elementy graficzne i multimedialne, które są w nich zawarte, są zgodne z wymogami dostępności cyfrowej, określonymi, w odniesieniu do stron internetowych, w załączniku do ustawy z dnia 4 kwietnia

2019 r. o dostępności cyfrowej stron internetowych i aplikacji mobilnych podmiotów publicznych (Dz. U. z 2023 r. poz. 1440), z wyłączeniem pozycji:

1) 2.4.1 – Możliwość pominięcia bloków;
2) 2.4.5 – Wiele dróg;
3) 3.2.3 – Spójna nawigacja;
4) 3.2.4 – Spójna identyfikacja.

4. Wymagania określone w ust. 3 uznaje się za spełnione, gdy podmiot realizujący zadania publiczne zapewnia dostępność cyfrową z uwzględnieniem wymagań określonych w rozdziale 10 Polskiej Normy wprowadzającej normę ETSI EN 301 549 V3.2.1:2021.

**§ 15.** 1. Podmiot realizujący zadania publiczne z wykorzystaniem wymiany danych za pomocą środków komunikacji elektronicznej lub za pomocą pism utrwalonych w postaci elektronicznej, sporządzonych według wzorów dokumentów elektronicznych, w których mają zastosowanie obiekty, o których mowa w § 5 ust. 1, lub obiekty, dla których struktury danych i znaczenie danych zawartych w tych strukturach zostały opublikowane w repozytorium interoperacyjności, stosuje strukturę atrybutów tych obiektów, która jest zgodna ze strukturą określoną w ramach schematów XML udostępnionych w repozytorium interoperacyjności.

2. W stosowanej strukturze, o której mowa w ust. 1, należy zawrzeć w szczególności nazwy i zakresy atrybutów obiektów.

3. Jeżeli z przepisów odrębnych wynika, że stosuje się podzbiór atrybutów obiektu, o którym mowa w § 5 ust. 1, to podmiot realizujący zadania publiczne wykorzystuje typy i zakresy danych określone w schemacie XML opublikowanym w repozytorium interoperacyjności.

**§ 16.** 1. Rozliczalność w systemie teleinformatycznym używanym do realizacji zadań publicznych podlega wiarygodnemu dokumentowaniu w postaci elektronicznych zapisów w dziennikach systemowych (logach).

2. W dziennikach systemowych odnotowuje się działania użytkowników lub oprogramowania polegające na dostępie do:

1) systemu teleinformatycznego z uprawnieniami administracyjnymi;
2) konfiguracji systemu teleinformatycznego, w tym konfiguracji zabezpieczeń;
3) danych, przetwarzanych w systemie teleinformatycznym, podlegających prawnej ochronie, w zakresie wymaganym przepisami prawa.

3. Poza informacjami wymienionymi w ust. 2 w dziennikach systemowych mogą być odnotowywane działania użytkowników lub oprogramowania, a także inne zdarzenia związane z eksploatacją systemu, w postaci:

1) działań użytkowników nieposiadających uprawnień administracyjnych;
2) zdarzeń systemowych nieposiadających krytycznego znaczenia dla funkcjonowania systemu teleinformatycznego;
3) zdarzeń i parametrów środowiska, w którym eksploatowany jest system teleinformatyczny

- w zakresie wynikającym z analizy ryzyka.

4. Informacje w dziennikach systemowych przechowywane są przez okres wskazany w przepisach odrębnych, a w przypadku braku przepisów odrębnych – przez okres uzasadniony i proporcjonalny wobec celu przetwarzania takich informacji.

5. Zapisy dzienników systemowych mogą być gromadzone w odrębnych systemach teleinformatycznych służących do przechowywania lub analizy logów lub na zewnętrznych informatycznych nośnikach danych w warunkach zapewniających bezpieczeństwo informacji.

**§ 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.

## Rozdział 5

## Przepisy przejściowe i końcowe

**§ 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 2 lat 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 2 lat od dnia wejścia w życie niniejszego rozporządzenia.

**§ 20.** Rozporządzenie wchodzi w życie z dniem 23 lutego 2027 r., z wyjątkiem:

1) § 11 ust. 4-8 i § 14 ust. 3 i 4, które wchodzą w życie po upływie 6 miesięcy od dnia ogłoszenia;

2) § 3 ust. 5 pkt 2, § 8 i § 14 ust. 1 i 2, które wchodzą w życie po upływie 12 miesięcy od dnia ogłoszenia.[2)]

**PREZES RADY MINISTRÓW**

Za zgodność pod względem prawnym,
legislacyjnym i redakcyjnym
Magdalena Witkowska-Krzymowska
Dyrektor Departamentu Prawnego
w Ministerstwie Cyfryzacji
/podpisano elektronicznie/

---

2) Niniejsze rozporządzenie było poprzedzone rozporządzeniem 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. z 2024 r. poz. 773), które traci moc z dniem wejścia w życie niniejszego rozporządzenia zgodnie z art. 17 w zakresie art. 1 pkt 19 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)

Załączniki do rozporządzenia Rady Ministrów z dnia ….. (Dz. U. ……)

**Załącznik nr 1**

**IDENTYFIKATORY OBIEKTÓW WYSTĘPUJĄCYCH W REJESTRACH PUBLICZNYCH**

| Lp. | Nazwa obiektu | Identyfikator obiektu | Definicja identyfikatora obiektu | | Pełna nazwa rejestru publicznego zawierającego dane referencyjne opisujące obiekt | Akt prawny stanowiący podstawę prawną funkcjonowania rejestru, o którym mowa w kolumnie 6 | Wyrażenie regularne |
|---|---|---|---|---|---|---|---|
| | | | Długość pola | Typ i zakres danej | | | |
| 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 |
| 1 | Osoba fizyczna posiadająca nadany numer PESEL | Numer PESEL | 11 | Pole znakowe, znaki z zakresu {0..9} | Powszechny Elektroniczny System Ewidencji Ludności | Ustawa z dnia 24 września 2010 r. o ewidencji ludności (Dz. U. z 2025 r. poz. 274) | \d{ll} |

| | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|
| 2 | Podmiot | | Numer identyfikacyjny REGON | 9 albo 14 | | Pole znakowe, znaki z zakresu {0..9} | Rejestr publiczny właściwy dla rodzaju podmiotu. W przypadku podmiotów zarejestrowanych w Krajowym Rejestrze Sądowym rejestrem właściwym jest Krajowy Rejestr Sądowy | Ustawa właściwa dla rodzaju podmiotu | \d{9}\|\d{14} |
| 3 | Obiekt przestrzenny | Punkt adresowy | Identyfikator punktu adresowego | Przestrzeń nazw (namespace)*) | do 26 | Pole znakowe, znaki z zakresu {A..Z, a..z, 0..9, ,.,} | Ewidencja Miejscowości, Ulic i Adresów | Ustawa z dnia 17 maja 1989 r. - Prawo geodezyjne i kartograficzne (Dz. U. z 2024 r. poz. 1290) | PL\.[A-Za-z]{1,6}\.\d{1,6}\.[A-Za-z0-9]{1,8} [A-Za-z0-9]{8}-[A-Za-z0-9]{4}-[A-Za-z0-9]{4}-[A-Za-z0-9]{4}-[A-Za-z0-9]{12} |
| | | | | Identyfikator lokalny (localId) | do 38 | Pole znakowe, znaki z zakresu {A..Z, a..z, 0..9, _,.,–} | | | |

| | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|
| | | | | Identyfikator wersji (versionId) | do 25 | Pole znakowe, znaki z zakresu {T, 0..9, +, -, :} | | | \d{4}-\d\d-\d\dT\d\d:\d\d:\d\d[+\-]\d\d:\d\d |
| | | Działka ewidencyjna | Identyfikator działki ewidencyjnej | Przestrzeń nazw (namespace)*) | do 26 | Pole znakowe, znaki z zakresu {A..Z, a..z, 0..9, ,.,} | Ewidencja Gruntów i Budynków | | PL\.[A-Za-z]{1,6}\.\d{1,6}\.[A-Za-z0-9]{1,8} |
| | | | | Identyfikator lokalny (localId) | do 38 | Pole znakowe, znaki z zakresu {A..Z, a..z, 0..9, _,.,–} | | | [A-Za-z0-9]{8}-[A-Za-z0-9]{4}-[A-Za-z0-9]{4}-[A-Za-z0-9]{4}-[A-Za-z0-9]{12} |
| | | | | Identyfikator wersji (versionId) | do 25 | Pole znakowe, znaki z zakresu {T, 0..9, +, -, :} | | | \d{4}-\d\d-\d\dT\d\d:\d\d:\d\d[+\-]\d\d:\d\d |

*)Przestrzeń nazw składa się z dwóch części oddzielonych kropką:

a) część pierwsza - identyfikator zbioru danych przestrzennych nadany zgodnie z przepisami wydanymi na podstawie art. 13 ust. 5 ustawy z dnia 4 marca 2010 r. o infrastrukturze informacji przestrzennej (Dz. U. z 2025 r. poz. 242),

b) część druga - literowe oznaczenie zasobu informacji przestrzennej, do której należą obiekty, np.: EGiB - dla działki ewidencyjnej, EMUiA - dla punktu adresowego.

**Załącznik nr 2**

**FORMATY ORAZ STANDARDY ZAPEWNIAJĄCE DOSTĘP DO DANYCH UDOSTĘPNIANYCH ZA POMOCĄ SYSTEMÓW TELEINFORMATYCZNYCH UŻYWANYCH DO REALIZACJI ZADAŃ PUBLICZNYCH**

| Lp. | Format plików, rozszerzenie nazwy pliku lub skrócona nazwa standardu | Oryginalna pełna nazwa standardu | Opis standardu | Organizacja określająca format, normę lub standard | Oznaczenie lub nazwa normy albo dokumentu zawierającego specyfikację techniczną wskazanego formatu |
|---|---|---|---|---|---|
| 1 | 2 | 3 | 4 | 5 | 6 |
| A | W celu wymiany danych przez podmioty realizujące zadania publiczne stosuje się: | | | | |
| 1. | Dla danych tekstowych, tekstowo-graficznych lub multimedialnych, stosuje się co najmniej jeden z następujących formatów plików: | | | | |
| 1.1 | txt | | Dokumenty w postaci czystego (niesformatowanego) zbioru znaków | ISO/IEC | ISO/IEC 10646 |

| | | | | | |
|---|---|---|---|---|---|
| | | | zapisanych w standardzie Unicode UTF-8 lub UTF-16 jako pliki typu .txt. | | |
| 1.2 | pdf | Portable Document Format | Dokumenty tekstowo-graficzne jako pliki typu Open Document Format .pdf | ISO/IEC | ISO 32000 |
| 1.3 | odt, fodt; ods, fods; odp, fodp; odg, fodg | Open Document Format for Office Application | Dokumenty w postaci: sformatowany tekst (odt), sformatowany nieskompresowany tekst (fodt), sformatowany arkusz kalkulacyjny (ods), sformatowany nieskompresowany arkusz kalkulacyjny (fods), sformatowana prezentacja multimedialna (odp), sformatowana nieskompresowana prezentacja multimedialna (fodp), sformatowany plik graficzny (odg), sformatowany nieskompresowany plik graficzny (fodg). | ISO/IEC | ISO/IEC 26300 |
| 1.4 | docx, xlsx, pptx | Office Open XML File Formats | Dokumenty w postaci: sformatowany tekst (docx), sformatowany arkusz kalkulacyjny (xlsx), sformatowana prezentacja multimedialna (pptx). | ISO/IEC | ISO/IEC 29500 |

| | | | | | |
|---|---|---|---|---|---|
| 1.5 | csv | Comma Separated Values | Wartości rozdzielone przecinkiem | IETF | RFC 4180 |
| 1.6 | epub | E-book file format | Otwarty standard elektronicznych książek (e-book) | ISO/IEC | ISO/IEC 23736 |
| 2. | Do publikowania otwartych danych stosuje się co najmniej jeden z następujących formatów plików: | | | | |
| 2.1 | RDF/XML | | Model metadanych RDF jako dokument XML. | W3C | RDF 1.1 XML Syntax |
| 2.2 | Turtle | Terse RDF Triple Language | Serializacja prawidłowych grafów RDF. | W3C | RDF 1.1 Turtle |
| 2.3 | N3 | Notation3 | Serializacja modeli RDF. | W3C | Notation3 (N3): A readable RDF syntax |
| 2.4 | JSON-LD | JavaScript Object Notation for Linked Data | Format kodowania połączonych danych w dokumencie tekstowym. | W3C | JSON-LD 1.1 |
| 2.5 | RDFa | Resource Description | Zestaw rozszerzeń do dokumentów opartych na XML pozwalający na osadzanie metadanych w dokumentach internetowych. | W3C | RDFa Core 1.1 – Third Edition |

| | | | | | |
|---|---|---|---|---|---|
| | | Framework in Attributes | | | |
| 3. | Do danych zawierających informację graficzną stosuje się co najmniej jeden z następujących formatów danych: | | | | |
| 3.1 | jpg, jpeg, jpe, jif, jfif | Digital compression and coding of continuous-tone still images | Plik typu jpg (Joint Photographic Experts Group) | ISO/IEC ITU | ISO/IEC 10918 ITU-T T.81, ITU-T T.83, ITU-T T.84, ITU-T T.86 |
| 3.2 | tif, tiff | Tagged Image File Format | Plik typu tif | ISO | ISO 12639 |
| 3.3 | geotiff | GeographicTagged Image File Format | Plik typu geotiff | Open Geospatial Consortium | OGC GeoTIFF standard 1.1 |
| 3.4 | png | Portable Network Graphics | Plik typu png | ISO/IEC | ISO/IEC 15948 |
| 3.5 | svg | Scalable Vector Graphics (SVG) | Plik grafiki wektorowej | W3C | SVG 1.1 W3C Recommendation |

| | | | | | |
|---|---|---|---|---|---|
| 4. | Do danych zawierających informację dźwiękową lub filmową stosuje się odpowiednio co najmniej jeden z następujących formatów plików: | | | | |
| 4.1 | wav, wave, bwf | Broadcast Wave Format | Plik audio | ITU | ITU-R BS.1352-3 |
| 4.2 | mp3 | MP3 File Format | Plik audio | ISO/IEC | ISO/IEC 11172-3<br>ISOI/IEC 13818-3 |
| 4.3 | flac | Free Lossless Audio Codec | Plik audio | Otwarty format, rozwijany i dostępny na licencji GNU. | - |
| 4.4 | mpg, mpeg | MPEG-2 Video Encoding | Plik wizualny z dźwiękiem lub bez | ISO/IEC | ISO/IEC 13818 |
| 4.5 | mp4, m4a, mpeg4 | MPEG-4 Video Encoding | Plik wizualny z dźwiękiem lub bez | ISO/IEC | ISO/IEC 14496 |
| 4.6 | ogg | Ogg Vorbis Audio Format | Plik audio | Xiph.Org Foundation | - |

| | | | | | |
|---|---|---|---|---|---|
| 4.7 | ogv | Theora Video Format | Plik audiowizualny z dźwiękiem lub bez | Xiph.Org Foundation | - |
| 5. | Do kompresji (zmniejszenia objętości) dokumentów elektronicznych stosuje się co najmniej jeden z następujących formatów plików: | | | | |
| 5.1 | zip, zipx | ZIP file format | Format kompresji plików | ISO/IEC | ISO/IEC 21320 |
| 5.2 | tar | Tape Archiver | Format archiwizacji plików (używany zwykle wraz z gz) | ISO/IEC/IEEE | ISO/IEC/IEEE 9945 |
| 5.3 | gz, gzip<br><br>Skompresowane archiwa tar: taz, tgz, tar.gz | GNU ZIP file format | Format kompresji plików | IETF | RFC 1952 |
| 5.4 | 7z | 7-Zip file format | Format kompresji plików | Otwarty format, rozwijany i dostępny na licencji GNU. | - |

| | | | | | |
|---|---|---|---|---|---|
| 6. | Do dokumentów elektronicznych z obszaru budownictwa stosuje się najmniej jeden z następujących formatów plików: | | | | |
| 6.1 | ifc | Industry Foundation Classes | Standard openBIM do wymiany danych i zarządzania obiektami w branży budowlanej. | buildingSMART International | ISO 16739-1 |
| 6.2 | ids | Information Delivery Specification | Standard openBIM definiujący wymagania informacyjne dla modeli BIM. | buildingSMART International | OpenBIM IDS 1.0 |
| 6.3 | bcf | BIM Collaboration Format | Standard umożliwiający komunikację i współpracę przy modelach BIM bez przechowywania pełnej geometrii. | buildingSMART International | OpenBIM BCF 3.0 |
| 7. | Do tworzenia stron internetowych stosuje się co najmniej jeden z następujących formatów plików: | | | | |
| 7.1 | html, htm | Hypertext Markup Language | Standard języka znaczników formatujących strony internetowe HTML 4.01 | W3C/WHATWG | W3C HTML 4.01<br>W3C/WHATWG HTML 5 |
| 7.2 | xhtml, xht | Extensible Hypertext Markup Language | Standard języka znaczników formatujących strony internetowe | W3C/WHATWG | XHTML 5 |

| | | | | | |
|---|---|---|---|---|---|
| 7.4 | css | Cascading Style Sheets | Kaskadowe Arkusze Stylów | W3C | - |
| 8. | Do udostępniania kanału informacyjnego stron internetowych stosuje się standard: | | | | |
| 8.1. | Atom | The Atom Syndication Format | Standard kanału informacyjnego | IETF | RFC 4287 |
| B. | Do określenia struktury i wizualizacji dokumentu elektronicznego stosuje się następujące formaty plików: | | | | |
| 1. | Do definiowania układu informacji polegającego na określeniu elementów informacyjnych oraz powiązań między nimi stosuje się następujące formaty plików: | | | | |
| 1.1 | xml | Extensible Markup Language | Standard uniwersalnego formatu tekstowego służącego do zapisu danych w postaci elektronicznej | W3C | XML 1.1 Second Edition |
| 1.2 | xsd | Extensible Markup Language | Standard opisu definicji struktury dokumentów zapisanych w formacie XML | W3C | XML Schema Definition Language 1.1 |
| 1.3 | gml | Geography Markup Language | Język Znaczników Geograficznych | OGC ISO/IEC | ISO/IEC 19136 |

| | | | | | |
|---|---|---|---|---|---|
| 1.4 | rng | REgular LAnguage for XML Next Generation | Język schematów do języka XML | ISO/IEC | ISO/IEC 19757-2 |
| 2. | Do przetwarzania dokumentów zapisanych w formacie XML stosuje się co najmniej jeden z następujących formatów plików: | | | | |
| 2.1 | xsl, xslt | Extensible Stylesheet Language | Rozszerzalny Język Arkuszy Stylów | W3C | W3C XSL 1.1<br>W3C XSLT 3.0<br>W3C XPath Language 3.1<br>W3C XQuerry 3.1: XML Querry language |
| 3. | Do elektronicznego podpisywania, weryfikacji podpisu, opatrywania pieczęcią elektroniczną i szyfrowania dokumentów elektronicznych stosuje się: | | | | |
| 3.1 | TSL[1)] | Trusted Service Status List | Zaufana lista nadzorowanych lub akredytowanych podmiotów świadczących usługi certyfikacyjne | ETSI | ETSI TS 119 612 |
| 3.2 | XAdES[2)] | XML Advanced Electronic Signatures | Podpis elektroniczny dokumentów w formacie XML | ETSI | ETSI EN 319 132-1 |

| | | | | | |
|---|---|---|---|---|---|
| 3.3 | PAdES[2)] | PDF Advanced Electronic Signatures | Podpis elektroniczny dokumentów w formacie PDF | ETSI | ETSI EN 319 142-1 |
| 3.4 | CAdES[2)] | CMS Advanced Electronic Signatures | Podpis elektroniczny dokumentów w formacie CMS | ETSI | ETSI EN 319 122-1 |
| 3.5 | ASIC[2)] | Associated Signature Containers | Podpis elektroniczny dokumentów wykorzystujący kontener ZIP | ETSI | ETSI EN 319 162-1 |
| 3.6 | XMLsig | XML-Signature Syntax and Processing | Podpis elektroniczny dokumentów w formacie XML | W3C | XML Signature Syntax and Processing Version 1.1 |
| 3.7 | XMLenc | XML Encryption Syntax and Processing | Szyfrowanie dokumentów elektronicznych w formacie XML | W3C | XML Encryption Syntax and Processing Version 1.1 |
| 3.8. | GPG | GNU Privacy | Szyfrowanie dokumentów elektronicznych innych, niż w formacie XML | IETF | RFC 4880 |
| C. | Do opisywania modeli danych dotyczących zadań publicznych stosuje się następujące słowniki i profile aplikacyjne: | | | | |

| | | | | | |
|---|---|---|---|---|---|
| 1.1. | CPSV-AP | Core Public Service Vocabulary Application Profile | Specyfikacja danych służąca do opisywania usług publicznych w formacie nadającym się do odczytu maszynowego. | Komisja Europejska | CPSV-AP 3.2.0<br>Klasy obowiązkowe: Public Service, Public Organisation.<br>Obowiązkowe właściwości tych klas:<br>- dla Public Service: Identifier, Name, Description, Is Grouped By<br>- dla Public Organisation: Identifier, Is Competent Authority Of |

1) Wykorzystanie list TSL w systemach administracji publicznej następuje w oparciu o najnowszą wersję standardu ETSI TS 119 612 oraz europejski system list TSL zgodnie z decyzją wykonawczą Komisji (UE) 2015/1505 z dnia 8 września 2015 r. ustanawiającą specyfikacje techniczne i formaty dotyczące zaufanych list zgodnie z art. 22 ust. 5 rozporządzenia Parlamentu Europejskiego i Rady (UE) nr 910/2014 w sprawie identyfikacji elektronicznej i usług zaufania w odniesieniu do transakcji elektronicznych na rynku wewnętrznym (Dz. Urz. UE L 235 z 09.09.2015, str. 26).

2) Stosowane zgodnie z rozporządzeniem wykonawczym Komisji (UE) 2026/248 z dnia 2 lutego 2026 r. ustanawiającym zasady stosowania rozporządzenia Parlamentu Europejskiego i Rady (UE) nr 910/2014 w odniesieniu do formatów zaawansowanych podpisów elektronicznych i zaawansowanych pieczęci elektronicznych, które mają być uznane przez podmioty sektora publicznego, oraz uchylającym decyzję wykonawczą Komisji (UE) 2015/1506 (Dz. Urz. UE L 2026/248 z 3.2.2026, s 1.).

Objaśnienia skrótów nazw organizacji z kol. 5:

FSF - Free Software Foundation

IETF - Internet Engineering Task Force

ISO - International Standardization Organization

OASIS - Organization for the Advancement of Structured Information Standards

OGC - Open Geospatial Consortium Inc.

OMA - Open Mobile Alliance

W3C - World Wide Web Consortium

ETSI - European Telecommunications Standards Institute

**Załącznik nr 3**

**FORMATY PLIKÓW OBSŁUGIWANE PRZEZ PODMIOT REALIZUJĄCY ZADANIE PUBLICZNE W TRYBIE ODCZYTU**

| Lp. | Rozszerzenie nazwy pliku | Oryginalna pełna nazwa formatu | Opis formatu | Organizacja określająca normę lub standard | Nazwa normy, standardu lub dokumentu normalizacyjnego albo standaryzacyjnego |
|---|---|---|---|---|---|
| 1 | 2 | 3 | 4 | 5 | 6 |
| 1. | dwg, dwf, dxf, dgn | - | Format wymiany danych CAD | Open Design Alliance | - |
| 4. | ics | - | Format wymiany danych CAD | buildingSMART | - |
| 5. | jp2, jpx, jpm, mj2 | Joint Photographic Experts Group 2000 | Format graficzny JPEG2000 | ISO/ IEC | ISO/IEC 15444 |
| 6. | doc, xls, ppt | Microsoft Word<br>Microsoft Excell<br>Microsoft Office PowerPoint | Wewnętrzny standard Microsoft | - | - |
| 7. | rtf | Dokumenty w postaci sformatowanego tekstu | Wewnętrzny standard Microsoft | - | - |

**Załącznik nr 4**

## ELEMENTY OCENY INTEROPERACYJNOŚCI KRAJOWEJ

1) **Metryka oceny:**
   a) nazwa systemu teleinformatycznego używanego do realizacji zadań publicznych lub prowadzenia rejestru publicznego,
   b) nazwa i numer REGON podmiotu realizującego zadania publiczne, który przeprowadza ocenę,
   c) data przeprowadzenia oceny.
2) **Wyniki oceny:**
   a) opis zmian wprowadzanych w systemie teleinformatycznym używanym do realizacji zadań publicznych lub w rejestrze publicznym oddziaływujących na podmioty publiczne w zakresie interoperacyjności na poziomach, o których mowa w § 3 ust. 1 rozporządzenia, obejmujący w szczególności zmiany w metadanych rejestru publicznego i interfejsach programistycznych aplikacji systemu teleinformatycznego używanego do realizacji zadań publicznych,
   b) zidentyfikowane podmioty publiczne, na które będą oddziaływały wprowadzane zmiany, o których mowa w art. 12n ust. 2 pkt 1 ustawy o informatyzacji,
   c) analiza skutków zmian wprowadzanych przez podmiot realizujący zadania publiczne na podmioty publiczne,
   d) opis działań oraz terminów działań podjętych oraz planowanych do podjęcia, przez podmiot realizujący zadania publiczne, w celu minimalizacji lub usunięcia negatywnych skutków zmian na podmioty publiczne,
   e) informacja o negatywnych skutkach zmian na podmioty publiczne, które nie zostaną usunięte w ramach wprowadzania zmian.

**Załącznik nr 5**

# SPECYFIKACJA INTERFEJSU PROGRAMISTYCZNEGO APLIKACJI (API) SYSTEMU TELEINFORMATYCZNEGO UŻYWANEGO DO REALIZACJI ZADAŃ PUBLICZNYCH

API systemu teleinformatycznego używanego do realizacji zadań publicznych jest zgodne z standardem architektury usług REST opisanym w niniejszym załączniku. W przypadkach uzasadnionych specyfiką podmiotu realizującego zadania publiczne lub świadczonych przez niego elektronicznych usług publicznych dopuszcza się stosowanie standardu protokołu komunikacyjnego SOAP opisanego w niniejszym załączniku.

**1. Standard architektury usług REST:**

**1) API systemu teleinformatycznego używanego do realizacji zadań publicznych spełnia wymagania:**

a) zgodne z architekturą usług REST,

b) wykorzystuje format reprezentacji danych zdefiniowany przez standard JavaScript Object Notation (JSON5),

c) zgodne ze standardem notacji JSON Schema,

d) przyjmuje JSON API jako standard komunikatów, obejmujących zapytania i odpowiedzi pomiędzy systemami teleinformatycznymi,

e) kontekst ułatwiający korzystanie z danych w sposób automatyczny jest generowany zgodnie ze standardem JSON-LD,

f) budowa API jest oparta o zasoby,

g) manipulacja zasobami jest oparta o reprezentacje zasobów,

h) zawiera obsługę buforowania, w tym zapewnia obsługę polecenia HEAD,

i) wyposażone jest w jednolity interfejs z unikalną identyfikacją zasobów; dopuszczalne jest istnienie więcej, niż jednego URI wskazującego zasób w przypadkach uzasadnionych (w tym: wersjonowanie API, różne wersje językowe),

j) funkcjonuje w modelu klient-serwer, gdzie klient komunikuje się z serwerem tylko poprzez interfejs API zgodny ze standardem architektury usług REST,

k) zapewnia możliwość wykorzystania samo opisujących się komunikatów,

l) zapewnia informację o strukturze danych,

m) zapewnia dostęp do zasobów w formacie JSON; w uzasadnionych przypadkach opcjonalne jest udostępnianie danych również w formacie XML za pomocą nagłówka "Accept" lub parametru "&format=" w URI.

**2) wymagania dotyczące nazewnictwa zasobów i parametrów operacji API:**

a) stosowane są jednolite reguły nazewnictwa: identyfikatory zasobów muszą jednoznacznie określać konkretny zasób,

b) nazwy zasobów są proste i jednoznacznie wskazują na ich przeznaczenie, zapewniając zrozumiałość dla użytkowników API,

c) nazwy zasobów są oznaczane rzeczownikami, aby jasno wskazywać na ich rodzaj.

d) rzeczowniki używane w nazwach zasobów występują w formie liczby mnogiej,

e) nazwy zasobów nie zawierają czasowników ani opisów czynności w celu jednoznacznego identyfikowania zasobów,

f) nazwy zasobów są precyzyjne i wskazują na konkretny zasób, unikając ogólnych terminów, które wymagają znajomości kontekstu zasobu,

g) identyfikatory zasobów nie zawierają znaków diakrytycznych,

h) nazwy zasobów są zapisane małymi literami w celu uniknięcia niejedno-znaczności nazw w różnych systemach:

- do łączenia fraz złożonych w nazwach zasobów używa się znaku "-" (łącznik, znak wskazanego w tablicy podstawowej znaków UTF-8 na pozycji 45), aby zachować czytelność i spójność,
- nie wolno używać znaku "_" (podkreślenie, znak wskazany w tablicy podstawowej znaków UTF-8 na pozycji 95) lub innych znaków specjalnych do łączenia fraz złożonych w nazwach zasobów;

**3) wymagania dotyczące opisu składni i elementów URI:**

a) URI (Uniform Resource Identifier) jest unikalnym identyfikatorem zasobów, zgodnym z RFC 1736, RFC 1737 oraz zestandaryzowanym zgodnie z RFC 3986,

b) Domena w URI jednoznacznie wskazuje na właściciela API. Domena ta udostępnia funkcjonalność API poprzez subdomenę „api” chyba, że nie jest to możliwe z uzasadnionego powodu,

c) do oznaczania zależności hierarchicznej między zasobami stosuje się znak „/” (ukośnik, znak wskazany w tablicy podstawowej znaków UTF-8 na pozycji 2215). Na końcu URI nie zamieszcza się znaku „/” (ukośnik, znak wskazany w tablicy podstawowej znaków UTF-8 na pozycji 2215),

d) Ścieżki URI są zapisywane wyłącznie z użyciem małych liter oraz cyfr,

e) W URI nie stosuje się rozszerzeń plików oraz nazw formatów plików. Informacje te są przekazywane przez nagłówki HTTP lub w metadanych zasobów;

**4) wymagania dotyczące dostępu do zasobów powiązanych za pomocą URI:**

a) usługa API dostarcza klientowi stan poprzez treść (ciało) komunikatu, kody i nagłówki odpowiedzi,

b) komunikacja między klientem a usługą API odbywa się za pomocą hiperlinków i hipertekstu,

c) API używa techniki HATEOAS (Hypermedia As The Engine Of Application State). Wymagane jest, aby linki zawarte w ciele lub nagłówkach odpowiedzi zawierały identyfikatory URI do zasobów powiązanych,

d) linki do zasobów powiązanych są dostępne zarówno w ciele odpowiedzi, jak i w nagłówkach odpowiedzi API,

e) linki zawarte w ciele lub nagłówkach odpowiedzi jednoznacznie wskazują identyfikatory URI dla zasobów powiązanych;

**5) wymagania dotyczące zarządzania zasobami – filtrowanie, sortowanie oraz stronicowanie:**

a) API umożliwia automatyczne korzystanie z zasobów, z uwzględnieniem potrzeby zarządzania danymi, w celu uzyskania odpowiednio spreparowanego wycinka zamiast pełnego zakresu danych,

b) API udostępnia funkcjonalność filtrowania, sortowania i stronicowania zasobów, pozwalając na zarządzanie danymi zgodnie z określonymi kryteriami,

c) zapytania i odpowiedzi systemu są realizowane zgodnie ze standardem JSON API w wersji 1.0 lub nowszej,

d) w odpowiedziach stosuje się uzupełnienie JSON API o JSON-LD - w celu dodania kontekstu koniecznego do automatycznego przetwarzania danych API,

e) proste stronicowanie, filtrowanie i sortowanie reprezentacji zasobów odbywają się poprzez URI,

f) API może obsługiwać zapytania przesyłane w ciele wiadomości w zakresie szerszym, niż przez URI,

g) zapytania asynchroniczne są obsługiwane przez kody HTTP o numerach 202 i 303,

h) obsługa kwerend SQL jest zabroniona w kontekście zarządzania reprezentacjami zasobów – filtrowaniem, sortowaniem i stronicowaniem;

**6) wymagania dotyczące metadanych:**

a) metadane stanowią integralną część udostępnianych przez API zasobów, stanowiąc element odpowiedzi na zapytania dotyczące reprezentacji danego zasobu - w celu efektywnego opisywania zasobów, umożliwiając zrozumienie ich zawartości oraz skuteczne zarządzanie nimi,

b) zasoby API są opisywane minimalnym zestawem metadanych, z wyłączeniem metadanych, które nie mają zastosowania do konkretnego rodzaju treści,

c) na minimalny zestaw danych składa się URI zasobu, data publikacji zasobu, data modyfikacji zasobu, data zakończenia publikacji zasobu, opis zasobu, słowa kluczowe, zakres czasowy danych, język zasobu, częstotliwość aktualizacji, kodowanie, licencja, katalog oraz suma kontrolna,

d) w przypadku braku metadanych dla określonego rodzaju zasobów nie dołącza się ich do odpowiedzi API,

e) metadane dostarczane przez dostawcę zasobu muszą być zgodne z ustalonymi zasadami nazewnictwa, a także definiowane przy użyciu standardowych rozwiązań, zgodnie z schema.org lub DCMI,

f) w przypadku wprowadzania niestandardowych metadanych dostawca zasobu musi dostarczyć słownik precyzyjnie opisujący, do jakich elementów odnoszą się te metadane;

**7) wymagania dotyczące mechanizmu linków do nawigacji:**

a) API zapewnia funkcjonalność linków do nawigacji, co oznacza dołączenie w ciele zasobu linków (oznaczanych jako „links”), zgodnie z JSON API w wersji 1.0 lub późniejszej,

b) w odpowiedzi na zapytania przesyłane przez użytkowników, API udostępnia stany wraz z zdefiniowanymi w JSON API 1.0 linkami ułatwiającymi poruszanie się między zasobami powiązanymi. Linki są oznaczane zgodnie z ich funkcją: prev (poprzedni), self (bieżący), next (następny), first (pierwszy), last (ostatni);

**8) wymagania dotyczące wersjonowania API:**

a) zmiany w API oznacza się za pomocą standardu wersjonowania semantycznego API,

b) wymagana struktura numeracji to MAJOR.MINOR.PATCH, gdzie:

- MAJOR: zwiększa się przy wprowadzeniu niekompatybilnych zmian interfejsu;
- MINOR: zwiększa się przy dodaniu nowych funkcji w sposób kompatybilny wstecz;

- PATCH: zwiększa się przy wprowadzeniu kompatybilnych poprawek lub drobnych zmian;

c) stosuje się strukturę numeracji zmian odpowiadającą zmianom:
   - MAJOR - usunięcie funkcji lub zmiany, które mogą powodować niekompatybilność wsteczną,
   - MINOR - dodanie nowych funkcji w sposób kompatybilny wstecz lub usprawnienia istniejących funkcji,
   - PATCH - poprawki błędów lub inne drobne zmiany nie wpływające na kompatybilność wsteczną,

d) odwołanie się do wersji API jest obowiązkowe i odbywa się poprzez element URI (/api/vXX/). Dopuszczalne jest odwoływanie się do wersji dodatkowo poprzez parametr URI „v=XX”, dodatkowy nagłówek „apiversion=XX” lub w nagłówku „Accept:”,

e) jeśli wersja API nie została określona, używa się wersji bieżącej (najnowszej stabilnej). Informacje o aktualnej wersji należy udostępnić pod adresem zakończonym frazą "/version",

f) przed planowaniem zmiany wersji należy oznaczyć wersję bieżącą statusem „deprecated”. Należy zakomunikować ten fakt dotychczasowym użytkownikom na stronie internetowej z opisem API oraz w opisie aktualnej wersji dostępnym pod adresem zakończonym frazą "/version", a także określić okres wsparcia, zakończenia wsparcia i zakończenia funkcjonowania bieżącej wersji,

g) poza uzasadnionymi wypadkami nie należy wycofywać obsługi wersji API szybciej, niż dwa lata po powiadomieniu użytkowników,

h) po wyłączeniu obsługi zastąpionej wersji API odwołania do niej muszą być realizowane, w zależności od kontekstu, błędem HTTP o kodzie nr 406 lub 410;

**9) wymagania dotyczące obsługi zdarzeń HTTP:**

a) minimalny zestaw obsługiwanych kodów odpowiedzi:
   - API określa minimalny zestaw obsługiwanych kodów odpowiedzi, zgodny z poniższym wykazem:

| **Grupa kodów** | **Znaczenie** | **Informacja na temat błędu** |
|---|---|---|
| **2xx** | 200 | OK |
| | 201 | Utworzono nowy zasób |
| | 202 | Zaakceptowano zapytanie, odpowiedź jeszcze nie jest gotowa |

| | | |
|---|---|---|
| | 204 | Brak zawartości |
| **3xx** | 301 | Przeniesiono na stałe |
| | 303 | Zobacz inne: odpowiedź na zapytanie dostępna pod innym adresem |
| | 304 | Nie modyfikowano od czasu wskazanego w zapytaniu |
| **4xx** | 400 | Błędne żądanie |
| | 401 | Brak autoryzacji |
| | 403 | Dostęp zabroniony |
| | 404 | Nie znaleziono |
| | 405 | Nieodpowiednia metoda |
| | 406 | Nieakceptowalne – treść nie może zostać przygotowana w sposób zasygnalizowany nagłówkami |
| | 409 | Konflikt |
| | 410 | Zasób usunięty i już nigdy nie będzie dostępny pod tym adresem |
| | 422 | Zapytanie niepoprawne semantycznie |
| | 429 | Zbyt wiele zapytań w jednostce czasu |
| **5xx** | 500 | Wewnętrzny błąd serwera |
| | 502 | Błąd bramki – serwer otrzymał niepoprawną odpowiedź od serwera nadrzędnego |
| | 503 | Usługa czasowo niedostępna |
| | 504 | Przekroczony czas oczekiwania na odpowiedź serwera wewnętrznego. |

- do przesłania informacji o numerze błędu, wykorzystuje się element Status-Line w nagłówku http,
- opis błędów musi zawierać informacje o przyczynie błędu, które są zawarte w ciele odpowiedzi,

b) informacje o błędach w ramach obsługi zdarzeń HTTP:

- ciało odpowiedzi HTTP zawiera następujące informacje objaśniające:

| **Nazwa objaśnienia** | **Identyfikator objaśnienia** |
|---|---|
| **Wiadomość o błędzie** | error-result |
| **Wiadomość objaśniająca przyczynę błędu** | error-reason |
| **Wiadomość objaśniająca możliwe rozwiązanie (opcjonalnie tam, gdzie jest to możliwe)** | error-solution |
| **Kod błędu zdefiniowany przez dostawcę** | error-code |
| **Link do dokumentacji z objaśnieniem numeru błędu dla danej wersji interfejsu** | error-help |

- komunikaty muszą dostarczać konkretną informację zwrotną. Niedopuszczalne są komunikaty, które nie pomagają w rozwiązaniu problemu przez użytkownika. Dostarczony komunikat musi być sformułowany precyzyjnie, w sposób konkretny, możliwy do sprawdzania w kontekście przyczynienia się do rozwiązania problemu, osiągalny (informacje/zalecenia zawarte w komunikacie

powinny być wykonalne przez użytkownika w kontekście informacji, którymi dysponuje);

**10) wymagania dotyczące uwierzytelniania i autoryzacji:**

a) uwierzytelnianie użytkowników API nie jest obowiązkowe tylko w systemie teleinformatycznym, do którego dostęp jest całkowicie otwarty i nie ma przesłanek do wprowadzenia ograniczeń dostępu do danych w nim zawartych,

b) jeżeli dane zawarte w systemie teleinformatycznym podlegają ograniczonemu dostępowi, wówczas API muszą korzystać z systemu uwierzytelniania użytkowników,

c) API nie może być zamknięte dla użytkowników nieuwierzytelnionych. Dla takich użytkowników można wprowadzić odpowiednie ograniczenia w korzystaniu z API. Ograniczenia takie wynikają z polityki bezpieczeństwa danego systemu teleinformatycznego,

d) uwierzytelnianie i autoryzacja użytkowników w API jest oparta o framework OpenID Connect,

e) stosowanie OAuth 2.0 jest dopuszczalne, jednak musi być używane w połączeniu z innymi rozwiązaniami wypełniającymi lukę autoryzacji,

f) wymagane jest stosowanie szyfrowania SSL/TLS w najnowszej obowiązującej wersji w celu zapewnienia bezpieczeństwa komunikacji;

**11) wymagania dotyczące określenia reguł wprowadzania limitów danych per IP i per API-Key:**

a) interfejs API jest zoptymalizowany w taki sposób, aby nie dopuszczać do nadmiernego obciążenia zasobów, co mogłoby uniemożliwić korzystanie z niego przez użytkowników. Jeżeli istnieje taka konieczność, to API musi umożliwiać nałożenie limitów danych per adres IP oraz per klucz API,

b) udostępniony webowy kreator zapytań jest zabezpieczony w zakresie dostępnych na dany moment narzędzi przed potencjalnym nadmiernym obciążaniem zasobów API,

c) klucze API są konstruowane zgodnie z zasadami konstrukcji tokenów Web JSON, domyślnie ustawione są na prawo dostępu tylko do odczytu dla wszystkich zasobów API,

d) w przypadku wprowadzenia ograniczeń, API posiada opracowaną politykę korzystania z API oraz plany korzystania z API przez różne kategorie

użytkowników, w szczególności użytkowników niezarejestrowanych, użytkowników posiadający API-Key oraz użytkowników z białych list,

e) w przypadku wprowadzenia limitów, zostaje utworzona biała lista użytkowników korzystających z API z priorytetem wyższym, niż inni użytkownicy,

f) w przypadku, gdy nie narusza to stabilności systemu, API może być obciążane w stopniu przekraczającym założone plany obciążeń, szczególnie przez użytkowników z białych list,

g) w API są implementowane reguły dławienia użytkowników w przypadku rozpoznania destrukcyjnych ataków typu DoS/DDoS. Wprowadza się stosowanie polityki długoterminowego uznawania adresów IP za wrogie (czarne listy) oraz wprowadza się konieczność implementacji zewnętrznych czarnych list do aktualizacji listy adresów blokowanych,

h) transfer danych jest ograniczany dla użytkowników z czarnej listy adresów IP,

i) wprowadzone są mechanizmy pozwalające ograniczyć transfer danych dla użytkowników generujących transfer i obciążenie zagrażające ciągłości, czy stabilności API,

j) adresy z czarnej listy adresów IP są weryfikowane co najmniej co 6 miesięcy i usuwane z listy w przypadku braku podejrzanego ruchu z danego adresu,

k) ograniczenie transferu jest stosowane dla użytkowników na podstawie dynamicznie aktualizowanych i opublikowanych zasad wynikających z analizy faktycznego sposobu korzystania z API,

l) podmiot realizujący zadania publiczne udostępniający API systemu teleinformatycznego korzysta z mechanizmu ograniczenia transferu danych w oparciu o udokumentowane reguły. Podmiot realizujący zadania publiczne udostępniający API systemu teleinformatycznego podejmuje działania skierowane na podnoszenie wydajności API,

m) podmiot realizujący zadania publiczne udostępniający API systemu teleinformatycznego może ograniczyć niektóre funkcjonalności API ze względu na możliwość generowania zbyt dużych obciążeń dla API. Nałożenie limitów musi skutkować błędem HTTP o kodzie 429 z informacją o polityce limitów oraz opcją dodania do białej listy;

12) **wymagania dotyczące standardu dokumentacji usług API -** dokumentacja API zawiera co najmniej:

a) opis zasobów – opis informacji dostarczanej przez każdy zasób, znaczenia zasobu, punktów dostępowych, metod do każdego punktu dostępowego,

b) opis obsługiwanych metod i punktów dostępowych, wraz z opisem sposobu dostępu do zasobów i dopuszczonych metod interakcji z nimi,

c) parametry obsługiwane przez punkty dostępowe, w szczególności dotyczące metod HTTP (GET, POST, PATCH itp.), nagłówków, ścieżki dostępu (URI), parametrów żądania (query), ciała żądania (body, np.: w formacie JSON), przykłady kodu żądań ilustrujące użycie złożonych, ale nieskomplikowanych zapytań oraz przykłady odpowiedzi – struktury i treści przesyłane klientowi w odpowiedzi na żądania, zapisane w dokumentacji lub odwołujące się do rzeczywistego systemu teleinformatycznego,

d) dokumentacja API stosuje oznaczenia umożliwiające odczyt maszynowy, jest dynamiczna i interaktywna oraz automatycznie generuje przykłady kodu dla bibliotek klienta. Spełnienie tych wymagań możliwe jest poprzez stosowanie standardu OpenAPI w wersji 3.0 lub nowszej oraz używanie narzędzi do generowania dynamicznej i interaktywnej dokumentacji API. Zastosowanie takich narzędzi powinno umożliwiać budowanie kreatorów zapytań do API;

**13) odstępstwa od standardu JSON API -** w związku z koniecznością odciążenia systemów teleinformatycznych:

a) API wspiera wybór pól do dostarczenia klientowi (JSON API: sekcja Sparse Fieldsets),

b) API wspiera sortowanie pól tam, gdzie jest to logicznie uzasadnione rodzajem danych (JSON API: sekcja Sorting),

c) API wspiera filtrowanie (JSON API: sekcja Filtering),

d) API wspiera dokładność informacji o błędach (JSON API: sekcja Error Objects).

**2. Standard protokołu komunikacyjnego SOAP:**

**1) implementowanie protokołu SOAP:**

a) interfejs API korzysta z protokołu Simple Object Access Protocol (SOAP) zgodnie z wytycznymi WS-I,

b) komunikat SOAP jest zgodny ze wskazaną strukturą: Envelope, Header i Body;

**2) bezpieczeństwo:**

a) zaimplementowane są mechanizmy bezpieczeństwa WS-Security, w celu zapewnienia dostępności, poufności, integralności i autentyczności przesyłanych danych,

b) połączenia z API są realizowane przez protokół HTTPS,

c) zaimplementowane są mechanizmy uwierzytelniania użytkowników, pozwalające na jednoznaczne uwierzytelnianie tożsamości klientów API,

d) wymagane jest stosowanie podpisywania i szyfrowania komunikatów zgodnie z WS-Security,

e) zaimplementowano kontrolę dostępu i uprawnień, umożliwiającą zarządzanie tym, które zasoby API są dostępne dla poszczególnych użytkowników i aplikacji;

**3) obsługa błędów SOAP:**

a) wszystkie komunikaty przesyłane między klientem a serwerem muszą być sformułowane zgodnie z formatem SOAP,

b) element ”Fault” musi zawierać podelementy: faultcode, faultstring i faultactor, które dostarczają informacje o rodzaju błędu, opisie błędu i ewentualnym miejscu jego wystąpienia,

c) zaimplementowane są mechanizmy rejestrowania błędów w celu monitorowania i diagnozowania problemów związanych z usługą SOAP,

d) informacje przekazywane w błędach są zabezpieczone;

**4) bezpieczne przekazywanie danych:**

a) komunikaty SOAP są szyfrowane w celu zabezpieczenia zawartości przed nieautoryzowanym dostępem,

b) zapewniono mechanizm uwierzytelniania, który pozwala potwierdzać tożsamość zarówno klienta, jak i serwera, przed rozpoczęciem wymiany komunikatów,

c) wymaganie dotyczące odpowiedniego zarządzania certyfikatami,

d) nagłówki SOAP są chronione przed manipulacją poprzez zastosowanie podpisów cyfrowych i walidację nagłówków,

e) wprowadzono mechanizmy kontroli dostępu do konkretnych usług lub funkcji API na podstawie uprawnień użytkowników,

f) jeśli API jest dostępne z poziomu przeglądarki, to wdrożono ochronę przed atakami typu Cross-Site Scripting (XSS) i Cross-Site Request Forgery (CSRF),

g) w przypadku korzystania z sesji zapewniono bezpieczne zarządzanie sesjami w celu ochrony danych sesyjnych.