Opinia Grupy Roboczej AI - Dane dla AI działającej przy Ministerstwie Cyfryzacji

do

założeń projektu Krajowych Ram Interoperacyjności i Repozytorium Interoperacyjności

Data: 23.05.2025 r.
wersja: FINAL
Grupa Robocza AI (GRAI)
Strumień: DANE w AI

Przygotowany przez: Katarzyna Starosławska, Tomasz Sokół, Paweł Kaczmarski, Elżbieta Wielechowska, Katarzyna Rosińska, Bartłomiej Sulik, Piotr Kulicki, Aleksandra Tomaszewska, Marta Adranowska, Maciej Lewandowski.

Poglądy wyrażone w tym dokumencie zawierają opinie autorów – ekspertów i ekspertek działających pro publico bono w Grupie Roboczej ds. Sztucznej Inteligencji przy Komitecie Rady Ministrów ds. Cyfryzacji w ramach Zespołu Zadaniowego ds. Technologii Przełomowych. W żadnym wypadku nie można ich postrzegać jako oficjalne stanowisko polskiego rządu, ani poszczególnych członków Rady Ministrów.

Spis treści

4.1. HTML i technologie webowe HTML 5: Podstawowy język do tworzenia stron WWW, integrujący się z JavaScript i CSS. Norma: HTML5 W3C Recommendation.

5. Specjalistyczne formaty danych (szeroko stosowane)

Załącznik 3 - Wzór raportu: Zgodność systemów wykorzystywanych przez podmioty publiczne z wymaganiami minimalnymi

Załącznik 4 - Analiza dokumentu założeń projektu Rozporządzenie KRI

Załącznik 5 - analiza uzasadnienia dla projektu założeń projektu rozporządzenia w sprawie KRI

Załącznik 6 - analiza założeń projektu rozporządzenia w sprawie w sprawie repozytorium interoperacyjności

Załącznik 7 - analiza uzasadnienia założeń projektu rozporządzenia w sprawie repozytorium interoperacyjności

Wprowadzenie do dokumentu

Strumień Dane dla AI, będący częścią Grupy Roboczej AI, działającej przy Ministerstwie Cyfryzacji na podstawie decyzji nr 4/2024 Przewodniczącego Komitetu ds. Cyfryzacji w sprawie utworzenia Zespołu zadaniowego do spraw technologii przełomowych, wyraża poprzez niniejszy dokument **stanowisko dotyczące ułatwienia wykorzystywania przez systemy sztucznej inteligencji rozwiązań zgodnych z ustawą o zmianie ustawy o informatyzacji działalności podmiotów realizujących zadania publiczne i rozporządzeniami wykonawczymi do tej ustawy**.

Zlecenie przygotowania ekspertyzy

Dokument powstał na zlecenie Departamentu Projektów i Strategii Ministerstwa Cyfryzacji z dnia 24.01.2025 r., który powierzył Grupie Roboczej ds. Sztucznej Inteligencji (GRAI), Sekcji ds. Dane dla AI, przygotowanie ekspertyzy dotyczącej w szczególności rekomendacji dla:

1. Formatów danych dla systemów sztucznej inteligencji w kontekście nowelizacji rozporządzenia Rady Ministrów w sprawie Krajowych Ram Interoperacyjności, które obejmuje minimalne wymagania dla rejestrów publicznych i wymiany informacji w postaci elektronicznej oraz minimalne wymagania dla systemów teleinformatycznych, zawarte w rozporządzeniu (Dz.U. z 2024 r. poz. 773), dalej określanego jako „Rozporządzenie KRI”.
2. Eksponowania i etykietowania danych w celu ułatwienia ich wykorzystywania przez systemy sztucznej inteligencji, w odniesieniu do metadanych rejestrów publicznych zawartych w art. 12k ust. 3 pkt 1 projektu ustawy o zmianie ustawy o informatyzacji działalności podmiotów realizujących zadania publiczne (UC44), a także zgodnie z założeniami dotyczącymi repozytorium interoperacyjności zawartymi w założeniach projektu rozporządzenia Rady Ministrów w sprawie repozytorium interoperacyjności (dalej „Rozporządzenie ws. Repozytorium Interoperacyjności”).

Celem niniejszego dokumentu jest przedstawienie kompleksowej analizy oraz rekomendacji, które mają na celu zapewnienie odpowiednich ram technicznych i organizacyjnych dla skutecznego wykorzystania sztucznej inteligencji w administracji publicznej oraz poza nią. Dokument ten stanowi ważny krok w realizacji celów Strategii Cyfryzacji Państwa, umożliwiając pełną zgodność z Krajowymi Ramami Interoperacyjności oraz wdrożenie systemów, które wspierają bezpieczną i efektywną wymianę danych w systemach AI.

1. Ogólne uwagi dotyczące założeń projektów rozporządzeń

Założenia projektów Rozporządzenia KRI i Rozporządzenia ws. Repozytorium Interoperacyjności prezentują kompleksowe podejście do modernizacji regulacji w zakresie interoperacyjności, wymiany danych i cyfryzacji administracji publicznej. Poniżej przedstawiono kluczowe wnioski wynikające z analizy:

1.1. Kompleksowość i szczegółowość merytoryczna

Założenia projektów rozporządzeń cechuje wysoki poziom szczegółowości – definiują one m.in. zakres minimalnych wymagań dla systemów teleinformatycznych i rejestrów publicznych, precyzują funkcje repozytorium interoperacyjności oraz określają zasady współdziałania podmiotów publicznych. Takie podejście gwarantuje, że regulacje odpowiadają na aktualne wymagania techniczne i organizacyjne, a także uwzględniają zmiany wynikające z nowych norm unijnych (np. rozporządzenie UE 2024/903, tj. akt w sprawie Interoperacyjnej Europy).

1.2. Silne strony założeń

1.2.1. **Ujednolicenie standardów:** Dokumenty dążą do harmonizacji terminologii i procedur, co jest kluczowe dla zapewnienia interoperacyjności między różnymi systemami administracji publicznej.

1.2.2. **Integracja z normami międzynarodowymi:** Odwołania do norm takich jak ISO/IEC (np. ISO/IEC 42010, ISO/IEC 10646) czy wytycznych Europejskich Ram Interoperacyjności (EIF) podkreślają międzynarodowy charakter regulacji.

1.2.3. **Zorientowanie na praktyczne wdrożenie:** Konsultacje, warsztaty oraz prace zespołów roboczych (m.in. grupa KRMC ds. Nowych KRI) wskazują, że założenia projektów opierają się na realnych potrzebach podmiotów publicznych i praktycznych doświadczeniach z dotychczasowych rozwiązań, w tym europejskich.

1.3. Obszary wymagające poprawy

1.3.1. **Złożoność językowa i strukturalna:** Tekst regulacji bywa bardzo szczegółowy i skomplikowany, co może utrudniać interpretację i wdrożenie przepisów przez osoby nie będące ekspertami IT. Konieczne jest uproszczenie niektórych fragmentów oraz ujednolicenie definicji, aby dokument stał się bardziej przejrzysty.

1.3.2. **Fragmentacja definicji i wymagań:** Chociaż szczegółowe definicje są mocną stroną, ich rozproszenie w wielu częściach

dokumentu może utrudniać szybkie odnalezienie kluczowych informacji. Wskazane byłoby opracowanie centralnego słownika terminologicznego, dostępnego także w formacie maszynowo czytelnym.

1.3.3. **Brak mechanizmów monitoringu:** Pomimo precyzyjnego określenia terminów aktualizacji danych (np. 7 dni od zmiany), brakuje szczegółowych rozwiązań dotyczących automatycznego monitoringu jakości danych i dostępności systemów, co jest kluczowe dla efektywnej integracji z narzędziami analityki predykcyjnej i AI.

1.4. Rekomendacje dla dalszych prac

1.4.1. **Uproszczenie i unifikacja języka:** Zaleca się dokonanie redakcji stylistycznej celem uproszczenia zdań i eliminacji powtórzeń. Ujednolicenie terminologii oraz przygotowanie dedykowanego słownika definicyjnego zwiększy przejrzystość dokumentu.

1.4.2. **Wdrożenie systemów automatycznego monitoringu:** Konieczne jest opracowanie mechanizmów umożliwiających automatyczne walidowanie i raportowanie jakości danych, co powinno obejmować dashboardy, systemy alertowe oraz integrację z narzędziami big data.

1.4.3. **Precyzyjne określenie standardów technicznych:** Wskazanie obowiązkowych formatów danych (np. JSON-LD, XML), norm bezpieczeństwa (TLS 1.3, OAuth 2.0, OpenID Connect) oraz odniesień do międzynarodowych standardów pomoże w zapewnieniu spójności i efektywnej wymiany danych.

1.4.4. **Wsparcie wdrożeniowe:** Należy wyznaczyć harmonogram wdrożenia nowych przepisów z określonymi kamieniami milowymi oraz utworzyć centralny organ nadzorczy, który zapewni wsparcie techniczne i szkolenia dla podmiotów publicznych.

2. Aspekty techniczne i interoperacyjność

Współczesne rozwiązania informatyczne w administracji publicznej muszą spełniać szereg wymagań, które nie tylko gwarantują ich ciągłość działania i bezpieczeństwo, ale również umożliwiają płynną wymianę danych między podmiotami. Poniższy opis dzieli zagadnienie na cztery główne sekcje: minimalne wymagania techniczne, specyfikacje API i wymiana danych, zarządzanie wersjami API oraz zasady interoperacyjności międzynarodowej.

2.1. Minimalne wymagania techniczne dla publicznych systemów teleinformatycznych

Systemy używane do realizacji zadań publicznych powinny być projektowane, wdrażane i eksploatowane zgodnie z określonymi normami, które gwarantują:

2.1.1. **Dostępność** Systemy muszą być dostępne przez określony czas operacyjny (np. 99,9% uptime), co jest kluczowe dla usług publicznych. W praktyce oznacza to wdrożenie rozwiązań takich jak:

2.1.1.1. Redundancja sprzętowa i oprogramowania. Mechanizmy backupu oraz systemy odzyskiwania po awarii (BCP/DRP), oparte na normie ISO 22301.

2.1.2. **Niezawodność** Systemy powinny być odporne na awarie oraz zapewniać szybkie przywracanie funkcjonalności. Wymagania te są często określane na podstawie norm:

2.1.2.1. **ISO/IEC 27001** – dotyczących zarządzania bezpieczeństwem informacji, co obejmuje procedury reagowania na incydenty,

2.1.2.2. **ISO/IEC 20000-1** – dotyczących zarządzania usługami IT, co wpływa na niezawodność świadczenia usług.

2.1.3. **Interoperacyjność techniczna i semantyczna:** Aby systemy mogły współdziałać konieczne są:

2.1.3.1. **Techniczna interoperacyjność:** Użycie wspólnych protokołów komunikacyjnych (np. HTTP/HTTPS, TCP/IP), formatów danych oraz standardowych interfejsów API.

2.1.3.2. **Semantyczna interoperacyjność:** Ujednolicenie definicji danych poprzez stosowanie wspólnych słowników, taksonomii oraz metadanych (np. zgodnych z DCMI czy W3C DCAT), co umożliwia jednoznaczną interpretację informacji przesyłanych między systemami w kraju oraz pomiędzy krajami członkowskimi.

2.2. Specyfikacje API i wymiana danych: Interfejsy API stanowią kluczowy element umożliwiający integrację systemów. Aby spełniały one wymogi nowoczesnych rozwiązań, należy zadbać o następujące aspekty:

2.2.1. Standardy komunikacji API:

2.2.1.1. REST API: API powinno opierać się na zasadach REST, umożliwiając przesyłanie danych w formatach JSON i JSON-LD, które są lekkie, czytelne maszynowo i powszechnie wspierane.

2.2.1.2. **SOAP API:** W specyficznych przypadkach, gdy wymagane są bardziej złożone transakcje lub dodatkowe zabezpieczenia, dopuszczalne jest użycie SOAP, który oferuje standard WS-Security i gwarantuje właściwości transakcyjne (ACID).

2.2.2. Formaty danych: Dane przesyłane przez API powinny być dostępne w otwartych i maszynowo czytelnych formatach, takich jak JSON, XML lub JSON-LD, co ułatwia ich automatyczną analizę i integrację z systemami big data oraz narzędziami AI.

2.3. Zarządzanie wersjami API i otwarte standardy W dynamicznym środowisku IT konieczne jest zapewnienie, że zmiany w interfejsach API nie wpływają negatywnie na działanie istniejących systemów. W tym celu należy stosować:

2.3.1. Mechanizmy wersjonowania API:

2.3.1.1. Wdrożenie standardu semantycznego wersjonowania (MAJOR.MINOR.PATCH) umożliwia kontrolę nad zmianami. Każda zmiana, która wpływa na kompatybilność wsteczną, powinna być odpowiednio oznaczona, a użytkownicy API muszą być o tym informowani (poprzez komunikaty o statusie "deprecated" dla starszych wersji).

2.3.2. Neutralność technologiczną: Projektowane API powinny być niezależne od konkretnej technologii, dzięki czemu podmioty publiczne mogą wybierać rozwiązania najlepiej odpowiadające ich potrzebom, a jednocześnie utrzymać spójność wymiany danych poprzez stosowanie otwartych standardów (np. OpenAPI).

2.3.3. Wymóg otwartych standardów: Stosowanie otwartych standardów dla formatów danych, takich jak JSON, XML, REST, SOAP oraz norm międzynarodowych (ISO, ETSI, W3C) gwarantuje, że rozwiązania pozostaną kompatybilne na przestrzeni czasu oraz umożliwiają łatwą integrację systemów publicznych.

2.4. Zasady interoperacyjności międzynarodowej Aby zapewnić transgraniczną wymianę danych oraz współpracę z partnerami zagranicznymi, krajowe systemy powinny być dostosowane do następujących norm:

2.4.1. Standardy W3C: Normy takie jak HTML5, XML oraz specyfikacje OpenAPI zapewniają, że dane przesyłane i prezentowane przez systemy będą zgodne z globalnymi standardami.

2.4.2. Standardy OGC: W przypadku danych przestrzennych, zastosowanie standardów opracowanych przez Open Geospatial Consortium (np. GeoTIFF, GML) umożliwia integrację z systemami GIS oraz analizę danych geograficznych.

2.4.3. Europejskie Ramy Interoperacyjności (EIF): Dostosowanie krajowych rozwiązań do wytycznych EIF gwarantuje, że systemy publiczne będą spełniały wymagania interoperacyjności na poziomie europejskim, co jest kluczowe dla współpracy transgranicznej. Zalecane jest udostępnianie danych z krajowego repozytorium interoperacyjności w unijnych wytycznych dla danych.

3. **Wytyczne organizacyjne i operacyjne.** W ramach zapewnienia transparentności oraz ułatwienia dostępu do informacji o usługach publicznych, niezbędne jest wdrożenie kompleksowych wytycznych organizacyjnych i operacyjnych, które regulują sposób publikowania danych oraz minimalne wymagania dotyczące publikacji metadanych i repozytoriów interoperacyjności. Poniżej przedstawiono kluczowe założenia i wymagania:

3.1. Publikacja informacji o usługach publicznych w Biuletynie Informacji Publicznej (BIP) oraz systemach agregujących usługi lub metadane usług (takich, jak gov.pl):

3.1.1. Wszystkie instytucje publiczne powinny publikować informacje o świadczonych usługach publicznych w Biuletynie Informacji Publicznej oraz na portalu gov.pl. Dokumentacja takich usług musi być:

3.1.1.1. **Aktualna:** Regularnie aktualizowana, aby odzwierciedlać zmiany w ofercie usług oraz procedurach ich świadczenia.

3.1.1.2. **Kompleksowa:** Zawierać szczegółowe opisy usług, procedur dostępu, kontaktów oraz terminów, w których usługi są dostępne.

3.1.1.3. **Czytelna:** Przedstawiona w sposób umożliwiający łatwe odnalezienie kluczowych informacji zarówno przez użytkowników końcowych, jak i systemy informatyczne wspierające automatyzację przetwarzania danych (np. Core Public Service Vocabulary Application Profile)[1].

3.1.2. Standaryzacja publikacji:

3.1.2.1. Ustalenie jednolitych wytycznych dotyczących formatu i struktury informacji publikowanych w BIP pozwoli na zachowanie spójności i umożliwia automatyczną integrację danych z innymi systemami informacyjnymi. W tym celu zaleca się:

3.1.2.1.1. Używanie otwartych formatów plików (np. HTML5, PDF) zgodnych z międzynarodowymi normami.

3.1.2.1.2. Zdefiniowanie standardowych szablonów dla publikacji informacji o usługach, które obejmują elementy takie, jak nazwa usługi, opis, kryteria dostępu, godziny pracy, dane kontaktowe oraz informacje o ewentualnych zmianach.

3.2. Publikacja metadanych i repozytoriów interoperacyjności

3.2.1. Publikacja metadanych: Każdy podmiot publiczny, który udostępnia dane za pomocą systemów teleinformatycznych, powinien publikować metadane opisujące te dane w sposób maszynowo czytelny. Minimalne wymagania dotyczące publikacji metadanych obejmują:

3.2.1.1. Strukturalność i kompletność: Metadane muszą zawierać kluczowe informacje, takie jak:

3.2.1.1.1. Nazwa zbioru danych.

[1] https://interoperable-europe.ec.europa.eu/collection/semic-support-centre/specifications

3.2.1.1.2. Unikatowy identyfikator (np. numer REGON, PESEL, inny identyfikator właściwy dla danego rejestru).
3.2.1.1.3. Data publikacji i ostatniej aktualizacji.
3.2.1.1.4. Wersja zbioru danych.
3.2.1.1.5. Opis zawartości i struktury danych (np. schemat XML, JSON Schema).
3.2.1.1.6. Informacje o autorze i źródle danych.

3.2.1.2. **Formaty publikacji:** Metadane powinny być udostępniane w formatach umożliwiających automatyczną analizę i integrację, takich jak JSON, XML lub JSON-LD.

3.3. Repozytorium interoperacyjności: Repozytorium interoperacyjności stanowi centralne źródło informacji o udostępnianych danych, API publicznych systemów teleinformatycznych oraz metadanych rejestrów publicznych. Minimalne wymagania dotyczące repozytorium interoperacyjności obejmują:

3.3.1. Dostępność i aktualność: Repozytorium powinno być dostępne całodobowo (z wyjątkiem zaplanowanych przerw serwisowych), a informacje w nim zawarte muszą być regularnie aktualizowane – np. w ciągu 7 dni od wystąpienia zmian.

3.3.2. Standaryzacja formatu danych: Wszystkie dane i metadane publikowane w repozytorium muszą być udostępniane w ustalonych, otwartych formatach (np. JSON-LD, XML), aby umożliwić ich automatyczną integrację z systemami analitycznymi i narzędziami AI.

3.3.3. Mechanizmy wyszukiwania i subskrypcji: Repozytorium powinno umożliwiać zaawansowane wyszukiwanie danych według kryteriów takich, jak:

3.3.3.1. Typ danych (np. rejestry publiczne, informacje o API),
3.3.3.2. Kategorie i statusy danych (np. planowane, użytkowane, wycofane). Ponadto, system powinien wspierać subskrypcję powiadomień, która automatycznie informuje uwierzytelnionych użytkowników o zmianach lub aktualizacjach.

3.3.4. Zasady dostępności: Publikacja metadanych i API powinna być zgodna z zasadami transparentności, co umożliwi łatwy dostęp do informacji zarówno przez instytucje publiczne, jak i użytkowników końcowych. Wymagane jest również zapewnienie, że dane te są dostępne w sposób zgodny z aktualnymi normami dotyczącymi otwartych danych.

4. Bezpieczeństwo i ochrona danych

4.1. Do formułowania zasad rozliczalności i dokumentowania operacji należy przeprowadzić analizy ryzyka.

4.2. Dla celów utrzymania identyfikacji i weryfikacji użytkowników, należy stosować:

4.2.1. wymuszenia implementacji silnych haseł (obejmujących nie mniej niż 12 znaków alfanumerycznych i specjalnych, z przynajmniej jedną małą literą, jedną wielką literą, jedną cyfrą oraz znakiem specjalnym),

4.2.2. w przypadku dostępu do danych generujących istotne z punktu widzenia organizacji ryzyka - uwierzytelnianie wieloskładnikowe, a jeżeli pozwala na to system - rozwiązanie SSO,

4.2.3. szkolenia związane z zasadami polityki haseł w danej organizacji,

4.2.4. bieżące kontrole stosowania przez pracowników zasad nie zapisywania haseł w formie fizycznej, stosowanie protokołu X.509.

4.3. Do zapewnienia bezpieczeństwa ruchu w sieci należy używać szyfrowania za pośrednictwem protokołu TLS:

4.3.1. Do ochrony ruchu sieciowego stosowany jest protokół TLS w wersji nie niższej, niż 1.3.

4.3.2. Do przesyłania logów należy stosować protokół Syslog over TLS.

4.3.3. Dostawca certyfikatu TLS musi być zweryfikowany i znajdować się na liście Narodowego Centrum Certyfikacji.

4.3.4. Minimalny zestaw przechwytywanych danych został określony w załączniku 1 punkt 6.4.1.1.

4.3.5. Dla utrzymania prawidłowej synchronizacji czasu na wszystkich urządzeniach powinna być utrzymywana synchronizacja czasu.

4.3.6. W przypadku urządzeń generujących ruch sieciowy do synchronizacji używany jest protokół NTP, adresy serwerów do synchronizacji czasu przedstawiono w załączniku 6.4.1.2.

4.3.7. Konfiguracja hierarchii protokołu - zastosowanie urządzenia nadrzędnego/urządzeń nadrzędnych dla sieci zależy od zastosowanej architektury sieci.

4.3.8. W przypadku urządzeń pozostających poza ruchem sieciowym, konieczne jest stosowanie synchronizacji czasu systemowego za pomocą sprzętowego zegara czasu rzeczywistego.

4.4. Wobec wszystkich osób, od których pobierane są dane do rejestrów publicznych, należy dopełnić obowiązku informacyjnego, tzn. poinformować je o:

4.4.1. Danych administratora i ewentualnego inspektora ochrony danych (DPO);

4.4.2. Celu i podstawie prawnej przetwarzania;

4.4.3. Na jakiej zasadzie dane mogą być udostępniane

4.4.4. Okresie przechowywania danych

4.4.5. Prawach osoby, np. do wniesienia skargi do Prezesa UODO, dostępu, sprostowania, usunięcia itd.

4.4.6. Czy podanie danych jest obowiązkowe i jakie są konsekwencje niepodania danych.

4.4.7. Profilowaniu, przekazywaniu poza EOG lub niezachodzeniu żadnej z tych okoliczności.

Już na etapie projektowania rejestru publicznego należy przeprowadzić analizę prawną i techniczną zapotrzebowania na informacje i zaimplementować pseudonimizację lub anonimizację. Wszelkie zbierane dane i publikowane dane powinny być ograniczone do tego, co jest niezbędne do osiągnięcia konkretnego celu rejestru.

4.5. W chwili obecnej, nie istnieją standardowe wytyczne dotyczące konkretnych metod anonimizacji. Na podstawie istniejącego konsensusu naukowego rekomendowanymi technikami anonimizacji są, jako najbardziej odporne na ataki wyodrębnienia, powiązania i wnioskowania:
- **4.5.1.** L-dywersyfikacja,
- **4.5.2.** t-bliskość.

4.6. W zależności od potrzeb do celów pseudonimizacji należy zastosować przynajmniej jedną z powyższych technik:
- **4.6.1.** tokenizacja,
- **4.6.2.** szyfrowanie kluczem tajnym,
- **4.6.3.** funkcja skrótu,
- **4.6.4.** funkcja skrótu z kluczem dodatkowym.

Rekomendacje dotyczące funkcji skrótu oraz funkcji skrótu z kluczem dodatkowym znajdują się w punkcie 6.4.2.1.

Wybór technik anonimizacji i pseudonimizacji opiera się na podstawie analizy ryzyka i ewentualnych przepisów lub wytycznych dla konkretnych rejestrów. W przypadku zastosowania anonimizacji szyfrowania kluczem tajnym należy uwzględnić infrastrukturę do zarządzania kluczami tajnymi i potwierdzić jej zgodność z istniejącymi przepisami. Należy prowadzić bieżący przegląd stosowanych zgodności przepisów i rozwiązań, w szczególności w kontekście Zalecenia Komisji (UE) 2024/1101 z dnia 11 kwietnia 2024 r. w sprawie skoordynowanego planu wdrożenia dotyczącego przejścia na kryptografię postkwantową i wynikających z niego planów, wytycznych oraz wymagań. Dla zapewnienia poufności, integralności oraz dostępności danych, podmioty publiczne muszą dysponować Planami Ciągłości Działania oraz Planami Przywracania Po Awarii. Do przygotowania planów konieczne jest wskazanie priorytetowych procesów oraz analizy ryzyk dla danego podmiotu.

4.7. Przy tworzeniu Planów Ciągłości Działania oraz Planów Przywracania Po Awarii należy uwzględnić:
- **4.7.1.** wyniki analiz ryzyk,
- **4.7.2.** wskazanie priorytetowych usług i procesów,
- **4.7.3.** wartości Docelowych Czasów Odzyskiwania (RTO) dla usług i procesów uznanych za priorytetowe,
- **4.7.4.** wartości Docelowych Punktów Odzyskania (RPO) dla usług i procesów uznanych za priorytetowe.

4.8. Procedury do Planów Ciągłości Działania oraz Planów Przywracania Po Awarii muszą zawierać w szczególności:

4.8.1. Zakres ról i odpowiedzialności zespołu, który będzie realizował plan;
4.8.2. Zakres działań mające na celu wdrożenie rozwiązań;
4.8.3. Informacje pomocnicze potrzebne do rozpoczęcia (w tym kryteria rozpoczęcia), działania, koordynacji i komunikacji działań zespołu;
4.8.4. Parametry RTO i RPO;
4.8.5. Instrukcje i procedury dotyczące wdrażania poszczególnych działań;
4.8.6. Wymagania dotyczące sił i środków niezbędnych do realizacji planu;
4.8.7. Wymagania dotyczące sprawozdawczości oraz oceny.

4.9. Plany Ciągłości Działania oraz Plany Przywracania Po Awarii są :
4.9.1. zatwierdzone przez kierownictwo,
4.9.2. ewaluowane w drodze ćwiczeń i testów,
4.9.3. przeglądane, a wyniki przeglądów z rekomendacjami zmian przedstawiane do zatwierdzenia kierownictwu,
4.9.4. poddawane aktualizacjom ad-hoc w przypadku zmian, które wpływają w istotny sposób na zawartość planów.

4.10. W zależności od potrzeb dopuszczalne jest wykonanie następujących rodzajów kopii bezpieczeństwa:
4.10.1. Pełnej - Wszystkich danych.
4.10.2. Przyrostowej – Tylko danych zmienionych od ostatniej wykonanej kopii.
4.10.3. Różnicowej – Tylko danych zmienionych od ostatniej pełnej kopii.

4.11. Wymagania wobec narzędzi do wykonania kopii bezpieczeństwa obejmują:
4.11.1. przeprowadzenie testu integralności danych,
4.11.2. przeprowadzenie testu poprawności wykonania kopii,
4.11.3. zaszyfrowanie wolumenu danych z zastosowaniem rekomendowanych algorytmów (Załącznik 6.4.3).

5. Monitorowanie i raportowanie

5.1. Wskaźniki efektywności:

Poniżej przedstawiono propozycję mierników oceny wdrożenia rozporządzenia, takich, jak czas realizacji spraw, poziom dostępności systemów, liczba incydentów bezpieczeństwa.

Wprowadzenie mierników oceny wdrożenia rozporządzenie pozwoli ocenić zarówno samo wdrożenie, jak i wpływ wdrożenia na obsługę spraw. W tym celu należy wyróżnić trzy podstawowe obszary:

5.1.1. Efektywność wdrożenia rozporządzenia Jako mierniki oceny wdrożenia można wykorzystać wskaźniki interoperacyjności i jakości danych:

5.1.1.1. liczbę procesów wspieranych przez centralne rejestry i usługi współdzielone,

5.1.1.2. odsetek wymienianych danych zgodnych z ustalonymi formatami i standardami (poprzez analizę logów komunikacyjnych, sprawdzanie poprawności wymienianych plików i komunikatów (np. ePUAP, API rejestrów), audyty jakości danych,

5.1.1.3. jakość i spójność baz danych między instytucjami (np. poprzez wyszukiwanie duplikatów danych).

5.1.1.4. Badaniom może podlegać zagregowana liczba rekordów oraz poszczególne rekordy kluczowe dla obiektu.

5.1.2. Efektywność realizacji spraw

5.1.2.1. częstotliwość i skuteczność wymiany informacji (np. liczba dokumentów elektronicznych przetwarzanych między urzędami) na podstawie statystyki logowań i przesyłu dokumentów w ramach centralnej platformy integracyjnej czy dedykowanych API,

5.1.2.2. efektywność przepływu informacji oraz szybkość załatwiania spraw w ramach poszczególnych procedur administracyjnych poprzez zdefiniowanie wskaźników dla rodzajów spraw (sprawy związane z meldunkiem, sprawy związane z podatkiem od nieruchomości, itp).

5.1.2.3. odsetek spraw załatwianych w formie elektronicznej,

5.1.2.4. Net Promoter Score (NPS) – wskaźnik lojalności użytkowników pozwala ocenić liczbę użytkowników, którzy pozostają przy usłudze elektronicznej.

5.1.3. Poziom bezpieczeństwa - może być określany przez następujące parametry:

5.1.3.1. Liczba incydentów bezpieczeństwa;

5.1.3.2. Średni czas wykrycia incydentu (MTTD – Mean Time To Detect);

5.1.3.3. Średni czas reakcji na incydent (MTTR – Mean Time To Respond;)

5.1.3.4. Poziom dostępności systemów IT (uptime).

5.1.4. Mechanizmy raportowania:

5.1.4.1. Ocena zgodności systemów wymaganiami minimalnymi powinna być okresowo raportowana przez podmioty publiczne. W celu zapewnienia spójności i wiarygodności wyników można określić minimalne standardy metodyki audytu (np. oparte na ISO 27001, ITIL). Należy także przygotować wzór raportu. Obowiązek raportowania powinien być wskazany w Rozporządzeniu. Oprócz głównego raportu rocznego/półrocznego wskazane jest raportowanie incydentalne w razie wystąpienia poważnych

awarii, naruszeń bezpieczeństwa czy innych zdarzeń wpływających na zgodność z KRI. Zdarzenia krytyczne powinny być zgłaszane niezwłocznie (w ciągu 24 godzin).

5.1.4.2. W raporcie powinny znaleźć się odniesienia do konkretnych wymagań minimalnych (w zakresie bezpieczeństwa informacji, formatów wymiany danych, dostępności usług, architektury systemowej) oraz wskazanie zgodności elementów infrastruktury z wytycznymi bezpieczeństwa oraz interoperacyjności (np. zastosowanie protokołów szyfrowania, zgodność z otwartymi standardami wymiany danych).

5.1.4.3. W przyszłości warto rozważyć automatyzację zbierania danych do raportu. W obszarach związanych z bezpieczeństwem i dostępnością systemów warto stosować narzędzia monitorujące od początku zbierania danych.

6. Uwagi końcowe i rekomendacje

Ogólne spostrzeżenia

Analiza założeń projektów rozporządzeń wykazała, że planowane regulacje wprowadzają kompleksowe i szczegółowe rozwiązania mające na celu modernizację ram prawnych dotyczących interoperacyjności, wymiany danych oraz cyfryzacji administracji publicznej. Kluczowe elementy, takie jak ustalenie minimalnych wymagań technicznych dla systemów teleinformatycznych, precyzyjne określenie funkcji repozytorium interoperacyjności, a także standaryzacja formatów danych, stanowią solidną podstawę do zapewnienia spójności i automatyzacji procesów. Przy tym warto podkreślić, że uwzględnienie odniesień do norm międzynarodowych (np. ISO/IEC, W3C, ETSI) oraz europejskich wytycznych (EIF) zwiększa kompatybilność i umożliwia transgraniczną wymianę danych.

Rekomendacje strategiczne

- Ujednolicenie i standaryzacja:
  Zaleca się doprecyzowanie definicji kluczowych pojęć na potrzeby tego dokumentu (takich jak „API”, „repozytorium interoperacyjności”, „minimalne wymagania”) oraz stworzenie centralnego słownika terminologicznego w formacie maszynowo czytelnym (np. JSON lub XML). Ujednolicenie terminologii umożliwi łatwiejszą integrację z systemami AI i automatyzację procesów. Proponujemy powtórzenie definicji z nowelizacji ustawy o informatyzacji.

- Monitorowanie jakości danych i automatyzacja:
  Wdrożenie mechanizmów automatycznego monitorowania jakości publikowanych danych, takich jak dashboardy kontrolne i systemy alertowe, pozwoli na bieżąco wykrywać niezgodności i spadki jakości. Należy rozważyć integrację z narzędziami analityki predykcyjnej (dostępnych na rynku czy zbudowanych na potrzeby automatyzacji), aby na podstawie zgromadzonych

wartości dla KPI (np. dostępność, kompletność metadanych, czas reakcji API) można było podejmować szybkie działania naprawcze.

- Bezpieczeństwo i zarządzanie dostępem:
  Konieczne jest używanie nowoczesnych standardów uwierzytelniania i autoryzacji w celu zabezpieczenia systemów przed nieautoryzowanym dostępem oraz zapewnienia pełnej rozliczalności operacji. Ujednolicenie procedur zarządzania uprawnieniami poprzez centralny system tożsamości zwiększy bezpieczeństwo całego środowiska.

- Optymalizacja interfejsów API:
  Systemy publiczne powinny udostępniać swoje API w formatach maszynowo czytelnych (np. JSON-LD, XML) z wdrożonym mechanizmem wersjonowania opartym o semantyczne zasady (MAJOR.MINOR.PATCH). Umożliwia to płynną migrację między wersjami i zachowanie kompatybilności w czasie zmian technologicznych.

- Wsparcie wdrożeniowe i szkolenia:
  Proponuje się utworzenie centralnego organu nadzorującego wdrożenie nowych regulacji, który będzie odpowiadał za harmonogram wdrożenia, przeprowadzał regularne audyty oraz organizował szkolenia dla podmiotów publicznych. To wsparcie pomoże w efektywnym dostosowaniu systemów do nowych wymagań i zapewni ciągłość działania usług.

Wnioski końcowe

Implementacja rekomendowanych rozwiązań przyczyni się do stworzenia nowoczesnych, interoperacyjnych i bezpiecznych systemów informatycznych w administracji publicznej, co ma kluczowe znaczenie dla efektywnej transformacji cyfrowej państwa. Ponieważ istnieje już rozporządzenie KRI, dalsze ujednolicenie formatów danych, wprowadzenie mechanizmów monitorowania jakości oraz zastosowanie otwartych standardów zwiększy automatyzację procesów, umożliwiając lepsze wykorzystanie narzędzi AI w analizie i przetwarzaniu danych.

Kluczowym efektem wdrożenia projektu powinno być podniesienie efektywności świadczenia usług publicznych, zwiększenie przejrzystości operacji administracyjnych oraz poprawa jakości danych, co wpłynie pozytywnie na funkcjonowanie całej administracji publicznej w kontekście współczesnych wymagań technologicznych.

Implementacja tych rekomendacji powinna być monitorowana na bieżąco, a wyniki analiz udostępniane w formie raportów, co umożliwi ciągłe doskonalenie procesów i adaptację do dynamicznie zmieniającego się środowiska technologicznego. zgodnie z wymaganiami określonymi przez projekt nowelizacji Ustawy o informatyzacji:

“Art. 18a. 1. Minister właściwy do spraw informatyzacji dokonuje, nie rzadziej niż raz na 3 lata, przeglądu standardów oraz specyfikacji, o których mowa w przepisach wydanych na podstawie art. 18, w celu ich oceny pod kątem zapewniania interoperacyjności, w tym stwierdzenia:

1) stopnia ich zgodności z aktualnymi opublikowanymi normami zatwierdzonymi przez międzynarodową, europejską lub krajową jednostkę normalizacyjną – z uwzględnieniem otwartych standardów i specyfikacji oraz zasady równego traktowania różnych rozwiązań informatycznych;

2) stopnia ich zgodności z europejskimi ramami interoperacyjności, o których mowa w art. 6 rozporządzenia 2024/903;

3) zakresu i stopnia ich stosowania przez podmioty realizujące zadania publiczne.

2. Minister właściwy do spraw informatyzacji udostępnia raport z przeglądu, o którym mowa w ust. 1, w repozytorium interoperacyjności.”

Załącznik 1 - Rekomendacje techniczne dla kluczowych elementów, takich jak API, metadane, szyfrowanie.

6.4.1.1 Wymagania wobec logów publicznych systemów teleinformatycznych

Lp.	Pole	Opis
1.	Czas	Godzina (*YYYY-MM-DDThh:mm:ss±hh:mm)*
2.	Źródło	Login i adres IP nadawcy
3.	Cel	Login i adres IP odbiorcy
4.	Port i Usługa wywołująca	Port i usługa nadawcy
5.	Port i Usługa docelowa	Port i usługa odbiorcy
6.	Protokół	Stosowany protokół wg modelu ISO/OSI
7.	Akcja	Działanie?
8.	Polityka	Nazwa polityki/reguły

6.4.1.2 Serwery użytkowane do synchronizacji czasu systemowego:

Lp.	Zarządca	Adres	IP
1.	Główny Urząd Miar	tempus1.gum.gov.pl	194.146.251.100
2.	Główny Urząd Miar	tempus2.gum.gov.pl	194.146.251.101

6.4.2 Rekomendowane algorytmy funkcji skrótu

Na podstawie wytycznych zawartych w SP 800-131A rekomendowanymi algorytmami dla funkcji skrótu oraz funkcji skrótu z kluczem niejawnym są:

Lp.	Rodzina Funkcji	Algorytm	Zadanie
1.	SHA-2	SHA2-224	Funkcja skrótu
2.	SHA-2	SHA2-256	Funkcja skrótu
3.	SHA-2	SHA2-384	Funkcja skrótu
4.	SHA-2	SHA2-512	Funkcja skrótu
5.	SHA-3	SHA3-224	Funkcja skrótu
6.	SHA-3	SHA3-256	Funkcja skrótu

7.	SHA-3	SHA3-384	Funkcja skrótu
8.	SHA-3	SHA3-512	Funkcja skrótu
9.	HMAC	HMAC-SHA224	Funkcja skrótu z kluczem niejawnym
10.	HMAC	HMAC-SHA256	Funkcja skrótu z kluczem niejawnym
11.	HMAC	HMAC-SHA384	Funkcja skrótu z kluczem niejawnym
12.	HMAC	HMAC-SHA512	Funkcja skrótu z kluczem niejawnym

6.4.3 Rekomendowane algorytmy szyfrujące do zabezpieczenia kopii zapasowych:

Ani na szczeblu krajowym, ani międzynarodowym nie funkcjonują formalne reguły identyfikujące dane algorytmy jako wymagane do takich, jednakże na podstawie rekomendacji zawartych w standardzie NIST Special Publication 800-57 Part 1 Revision 5 wskazano jako najodpowiedniejsze:

a) Algorytm AES-256-GCM,
b) Algorytm RSA-OAEP.

Załącznik 1 – Kodowanie znaków

Kodowanie znaków jest kluczowym elementem zapewniającym interoperacyjność systemów informatycznych, poprawność wyświetlania treści oraz automatyczną analizę danych. Wybór odpowiedniego kodowania wpływa na kompatybilność między systemami i ułatwia integrację rozwiązań opartych na sztucznej inteligencji.

1. Zalecenia dotyczące kodowania tekstu

1.1. Standard UTF-8

1.1.1. **Stosowanie UTF-8:** UTF-8 jest de facto standardem w aplikacjach internetowych oraz systemach komunikacji elektronicznej, co umożliwia łatwą integrację danych i automatyczną analizę przez narzędzia AI.

1.1.2. **Stosowanie UTF-8 bez BOM:** Zaleca się, aby pliki były kodowane w UTF-8 bez BOM, ponieważ większość nowoczesnych systemów i edytorów poprawnie rozpoznaje to kodowanie, co ułatwia automatyczną analizę danych i zapobiega problemom z parsowaniem,, chyba, że potrzeba użycia BOM wynika z udokumentowanej analizy dla rozwiązania.

1.2. Argumentacja przeciwko UTF-16

1.2.1. Użycie UTF-16 jest marginalne w środowisku aplikacji internetowych, które dominują standardem UTF-8.

1.2.2. Konwersja z UTF-16 do UTF-8 generuje dodatkowe koszty przetwarzania, dlatego preferuje się bezpośrednie stosowanie UTF-8.

1.3. Normy i odniesienia

ISO/IEC 10646: Najnowsza wersja standardu dla Uniwersalnego Zestawu Kodowego (Universal Coded Character Set – UCS), stanowiąca podstawę dla UTF-8. Norma ta stanowi fundament dla globalnej wymiany informacji tekstowej, umożliwiając reprezentację znaków z praktycznie wszystkich systemów pisma, symboli technicznych, matematycznych, a także nowych emoji. W praktyce ISO/IEC 10646 jest ściśle zharmonizowany z Unicode, co oznacza, że oba standardy praktycznie się pokrywają. Znaczenie standardu dla interoperacyjności:

1.3.1. **Globalna kompatybilność -** Dzięki jednoznacznemu przypisaniu punktów kodowych do znaków ISO/IEC 10646 zapewnia, że teksty tworzone w jednym systemie mogą być bezproblemowo odczytywane i przetwarzane w innych systemach, niezależnie od języka czy regionu.

1.3.2. **Wsparcie dla aplikacji i systemów -** Standard jest fundamentem dla wielu protokołów i formatów danych, w tym dla HTML, XML, JSON, a także dla interfejsów API używanych w nowoczesnych aplikacjach. Umożliwia to rozwój międzynarodowych aplikacji, stron internetowych, systemów bazodanowych i narzędzi mobilnych.

1.3.3. **Integracja z narzędziami AI -** Maszynowo czytelna struktura UCS umożliwia efektywne przetwarzanie i analizę danych tekstowych przez systemy sztucznej inteligencji, co jest kluczowe dla zastosowań takich jak przetwarzanie języka naturalnego (NLP) oraz automatyczne tłumaczenia.

Załącznik 2 – Formatowanie danych - rekomendacje

1. **Format danych tabelarycznych**
   - **1.1. CSV (Comma-Separated Values)** CSV jest powszechnie używany przez instytucje publiczne (np. dane.gov.pl) oraz wspierany przez liczne narzędzia analityczne. **Norma: RFC 4180** – opisuje standardowy format CSV, zapewniając spójność interpretacji między systemami.
   - **1.2. TSV (Tab-Separated Values)** TSV wykorzystywany jest w specyficznych przypadkach, gdy dane zawierają przecinki, a separator tabulacji umożliwia ich prawidłowe przetwarzanie. **Normy i wytyczne:** Brak ścisłej normy ISO – interpretacja formatu TSV może się różnić między systemami. W administracji publicznej CSV pozostaje dominującym formatem, jednak TSV może być stosowany wewnętrznie tam, gdzie separator tabulacji jest korzystniejszy.
2. **Formatowanie danych graficznych**
   - **2.1. Format rastrowe (bitmapowe)**
     - **2.1.1. JPG (JPEG):** Format stratny, szeroko stosowany przy publikacji zdjęć. **Norma: ISO/IEC 10918** – standard dotyczący kompresji JPEG.
     - 2.1.2. **HEIC (High Efficiency Image Format):** Nowoczesny format, wykorzystywany głównie w urządzeniach Apple; oferuje wysoką jakość przy mniejszym rozmiarze pliku. **Norma:** Oparty na standardzie **ISO/IEC 23008-12** (część standardu HEIF).
   - **2.2. Format wektorowe**
     - **2.2.1. SVG (Scalable Vector Graphics):** Standard otwarty opracowany przez W3C, umożliwiający skalowalność, interaktywność oraz animacje bez utraty jakości. **Norma: SVG 1.1 W3C Recommendation** (oraz rozwijany standard SVG 2).
     - **2.2.2. PDF (Portable Document Format):** Format dokumentów, który obsługuje zarówno grafikę wektorową, jak i rastrową. **Norma: ISO 32000-1** (pierwsza wersja; nowsze wersje, np. ISO 32000-2, są również dostępne).
3. **Kompresja i wybór formatów**
   - **3.1. Format stratny vs. bezstratny**
     - **3.1.1. Lossy (ze stratami):**
       - 3.1.1.1. **JPG:** Kompresja stratna – **ISO/IEC 10918**.
       - 3.1.1.2. **WEBP (opcja stratna):** Umożliwia redukcję rozmiaru pliku z pewną utratą jakości; specyfikacja opracowana przez Google.
       - 3.1.1.3. **HEIC:** Stosowany, gdy priorytetem jest zmniejszenie rozmiaru przy zachowaniu wysokiej jakości – oparty na **ISO/IEC 23008-12**.
     - **3.1.2. Lossless (bezstratne):**
       - **3.1.2.1. PNG:** Bezstratna kompresja, zachowanie jakości – oparty o specyfikację PNG.

3.1.2.2. **TIFF:** Często używany w profesjonalnej fotografii; TIFF 6.0 Specification jest powszechnie stosowaną referencją (choć nie ma formalnego numeru ISO dla TIFF jako całości).
3.1.2.3. **GIF (statyczny):** Format bezstratny w kontekście pojedynczych obrazów; oparty na specyfikacji GIF89a.
3.1.2.4. **BMP:** Mimo że przestarzały, może być stosowany w specyficznych przypadkach – brak formalnej normy ISO.
3.1.2.5. **RAW:** Format nieskompresowany, różni się w zależności od producenta – brak jednolitej normy.

4. **Standardy sieciowe**
   - **4.1. HTML i technologie webowe HTML5: Podstawowy język do tworzenia stron WWW, integrujący się z JavaScript i CSS. Norma: HTML5 W3C Recommendation.**
   - **4.2. JavaScript (.js):** Język programowania do dynamicznej interakcji na stronach WWW. **Norma: ECMAScript** – standard określany przez ECMA International (np. ECMAScript 2020).
   - **4.3. JSON (JavaScript Object Notation):** Lekki format wymiany danych między serwerem a stroną WWW. **Norma: RFC 8259** (aktualny standard JSON).
   - **4.4. XML (Extensible Markup Language):** Format przeznaczony do strukturalnego przechowywania danych. **Norma: XML 1.0 (Fifth Edition)** – W3C Recommendation.
5. **Specjalistyczne formaty danych (szeroko stosowane)**
   - **5.1. IFC (Industry Foundation Classes):** Standard openBIM do wymiany danych i zarządzania obiektami w branży budowlanej. **Norma: ISO 16739-1:2024 (wersja 4.3_ADD2)**. **Organizacja:** buildingSMART International.
   - **5.2. IDS (Information Delivery Specification):** Standard openBIM definiujący wymagania informacyjne dla modeli BIM. **Norma: OpenBIM IDS 1.0**. **Organizacja:** buildingSMART International.
6. **BCF (BIM Collaboration Format):** Standard umożliwiający komunikację i współpracę przy modelach BIM bez przechowywania pełnej geometrii. **Norma: OpenBIM BCF 3.0**. **Organizacja:** buildingSMART International.

Uzasadnienie:

Wykorzystanie plików w formacie .ifc nie kończy się na realizacji zadania budowlano-inwestycyjnego. Po zakończeniu realizacji budynku (budowli) model ifc stanowi cyfrowe odzwierciedlenie danego obiektu budowlanego i stanowi punkt wyjścia do stworzenia jego cyfrowego bliźniaka, może być szeroko wykorzystywany w procesie zarządzania infrastrukturą (Facility Management).

Modele cyfrowe (zapisywane w formacie .ifc) łączą w sobie informację geometryczne z obszerną bazą danych. Format .ifc jest standardem otwartym, dostępnym na (darmowej) licencji CC (Creative Commons). Jest on określony w standardzie PN-EN ISO 16739.

Jego użycie i wykorzystanie nie wymaga logowania do usługi on-line komercyjnych dostawców.

Dzięki otwartej specyfikacji formatu oraz pełnej kompatybilności modeli BIM z otwartymi danymi geodezyjnymi (GIS) możliwe jest szerokie, międzysektorowe wykorzystanie modeli w formacie ifc. Poniżej wybrane przykłady zastosowań:

- planowanie przestrzenne,
- analizy zagospodarowania terenu,
- analiza naświetlenia pomieszczeń / zaciemnienia budynków,
- analiza dostępności sieci,
- analizy rozprzestrzeniania się hałasu i drgań,
- inteligentne miasto,
- cyfrowe modele miast oparte o rzetelne dane obiektowe,
- integracja z IoT (Internet of Things),
- analizy zużycia wody/ prądu w obiektach (integracja z systemami BMS),
- analizy przemieszczania się pieszych i pojazdów,
- tworzenie trójwymiarowych aplikacji miejskich dla mieszkańców (rezerwacja miejsc parkingowych zgłaszanie usterek i barier architektonicznych),
- gospodarka wodna,
- analizy hydrotechniczne,
- modelowanie i monitorowanie budowli ziemnych,
- symulacje podtopień i powodzi,
- energetyka,
- inteligentne modele sieci przesyłowych,
- symulacje elektrowni,
- obrona cywilna,
- symulacja ewakuacji z wykorzystaniem modeli ewakuacyjnych budynków,
- możliwość dalszego wykorzystania danych z formatów ifc istniejących już w zasobach podmiotów publicznych (jak szpitale, szkoły czy urzędy) do celów obrony cywilnej,
- wykorzystanie w narzędziach VR (wirtualna rzeczywistość) i AR (rozszerzona rzeczywistość) np. do celów szkoleniowych, w akcjach militarnych czy ratunkowych,
- wojsko (np. symulacje akcji militarnych w miastach / na obiektach budowanych),
- możliwość zbudowania zamkniętej bazy modeli informacyjnych obiektów obronnych i obiektów strategicznych (budowlanej infrastruktury krytycznej),
- możliwość wykorzystania formatu ifc w zamkniętych sieciach teleinformatycznych i budowy niezależnych aplikacji,
- wykorzystanie w narzędziach VR (wirtualna rzeczywistość) i AR (rozszerzona rzeczywistość)
- modelowanie procesów przemysłowych,
- automatyka przemysłowa,
- symulacje wykorzystania instalacji i urządzeń.

Wymienione powyżej zastosowania są jedynie przykładami obrazującymi możliwości wykorzystania modeli .ifc. W rzeczywistości katalog możliwych zastosowań plików w

tym formacie bardzo szeroki i cały czas rozbudowywany. Z modelami w formacie .ifc związane są dwa uzupełniające formaty:

.bcf

BCF to format wspierający współpracę i komunikację w oparciu o modele BIM. Zawiera informacje o problemach, uwagach i konfliktach dotyczących elementów modelu, ale nie przechowuje geometrii. Dzięki temu członkowie zespołu mogą wymieniać się uwagami bez konieczności przesyłania całego modelu. Używany do zarządzania zgłoszeniami i zadaniami.

.ids

IDS to specyfikacja dostarczania informacji, która definiuje, jakie dane i w jakiej strukturze muszą zostać dostarczone w modelu BIM. Zapewnia, że dane dostarczane w modelu są zgodne z oczekiwaniami wszystkich interesariuszy projektu. Pomaga uniknąć braków lub nadmiarowych informacji w modelu.

Załącznik 3 - Wzór raportu: Zgodność systemów wykorzystywanych przez podmioty publiczne z wymaganiami minimalnymi

Tabela 1. Systemy teleinformatyczne

(dane przykładowe)

Nazwa systemu	**Funkcjonal-ność**	**Zakres przetwa-rzanych danych**	**Krytyczność**	**Jednostka/ Departa-ment**	**Interopera-cyjność**
System Z	Ewidencja ludności	Dane osobowe	Wysoka	WEL (Wydział Ewidencji Ludności)	Format danych (XML, JSON, XDS...)

Tabela 2. Ocena zgodności z wymaganiami minimalnymi

(dane przykładowe)

Nazwa Systemu	**Format przetwarza-nych danych**	**Protokół komuni-kacyjny**	**Poziom dostęp-ności**	**BCP/DRP**	**Zastoso-wana norma bezpie-czeństwa**	**Ocena**
System Z	XML	TCP/IP	99,7%	BCP	OAuth 2.0	zgodne

Załącznik 4 - Analiza dokumentu założeń projektu Rozporządzenie KRI

1. Przepisy ogólne i definicje

Dobrze przygotowane w dokumencie:

– Założenia projektu rozporządzenia zawierają bardzo szczegółowy zestaw definicji kluczowych pojęć (np. „architektura systemu teleinformatycznego", „autentyczność", „integralność", „dostępność", „URI"), co stanowi solidną bazę dla jednolitego podejścia do interoperacyjności i przetwarzania danych.
– Wprowadzenie standardowych terminów ułatwia późniejszą automatyzację i wdrażanie mechanizmów analizy danych przez systemy AI.

Co należy zmienić:

– Ujednolicić format prezentacji definicji – warto rozważyć przygotowanie wersji maszynowo czytelnej (np. w formacie JSON lub XML) jako załącznika do rozporządzenia lub plik opublikowany przez Ministerstwo Cyfryzacji, aby ułatwić integrację z systemami informatycznymi.

2. Krajowe Ramy Interoperacyjności

Dobrze przygotowane w dokumencie:

Rozdział II precyzyjnie określa, że Krajowe Ramy Interoperacyjności mają ujednolicić normy, standardy, metody i formaty stosowane przez podmioty publiczne, co jest kluczowe przy budowaniu spójnego systemu wymiany danych.

– Ujęcie trzech poziomów interoperacyjności (organizacyjnego, semantycznego i technicznego) stanowi kompleksowe podejście do problematyki. Zasadne byłoby ujęcie także czwartego poziomu interoperacyjności, interoperacyjności prawnej, zgodnie z EIF. Jednak delegacja ustawowa z nowelizacji ustawy o informatyzacji (UC44) nie pozwala na zaadresowanie interoperacyjności prawnej w przygotowywanym rozporządzeniu.

Co należy zmienić:

– Warto wprowadzić konkretne wskaźniki (KPI) oceny interoperacyjności, które umożliwią systematyczną analizę i monitorowanie efektywności wdrożonych rozwiązań – na przykład czas reakcji systemów, współczynnik błędów przy wymianie danych czy zgodność z przyjętymi normami.

KPI	Definicja	Wartość docelowa	Metoda pomiaru
1. Czas odpowiedzi (Response Time)	Czas od wezwania API / usługi do otrzymania pełnej odpowiedzi	≤ 200 ms (95 percentyl)	– APM (Application Performance Monitoring) – e.g. New Relic, Dynatrace – Synthetic (ping-test) co min. 5 min
2. Współczynnik błędów (Error Rate)	% nieudanych lub odrzuconych wywołań względem wszystkich prób	≤ 0,5 %	– Logi serwisów (HTTP status ≥ 500 lub aplikacyjne kody błędów) – Alerty w systemie ELK / Splunk
3. Dostępność usługi (Availability)	Procent czasu, w którym usługa jest osiągalna i działa poprawnie	≥ 99,95 % miesięcznie	– Monitorowanie uptime (Pingdom, Nagios) – Raporty SLA od dostawcy chmury
4. Przezroczystość schematu	% wymienianych komunikatów zgodnych z opublikowanym schematem	100 %	– Walidacja JSON/XML przez CI (JSON Schema, XSD) – Testy automatyczne post-deployment
5. Zgodność semantyczna	% elementów danych poprawnie mapowanych na słowniki KRI	≥ 99 %	– Testy jednostkowe mapowań (np. schemat OWL/RDF) – Ręczna weryfikacja losowego 1 % rekordów

6. Czas propagacji zmian	Średni czas od zmiany w jednym systemie do widoczności w drugim	≤ 5 min	– Mierniki ETL/ESB (czas od CDC do landing zone) – Logi kolejkowania (Kafka, RabbitMQ)
7. Przepustowość (Throughput)	Liczba poprawnie przetworzonych komunikatów na sekundę	≥ 500 msg/s	– Metryki ESB/API Gateway – Stress-testy przed wdrożeniem
8. Spójność danych (Data Consistency Rate)	% rekordów bez konfliktów lub dublowania	≥ 99,9 %	– Testy porównawcze (checksum, hash) między bazami – Narzędzia CDC (Debezium)
9. Obsługa wyjątków (Exception Handling Rate)	% przypadków poprawnie obsłużonych wg procedur awaryjnych	100 %	– Przegląd logów błędów i retry'ów – Testy scenariuszy błędnych danych
10. Częstotliwość audytów norm	Liczba przeglądów zgodności z normami KRI rocznie	≥ 1 (obowiązkowy przegląd ministra)	– Harmonogram w karcie norm i standardów – Raport z każdego przeglądu z listą odchyleń i działań

Co dodać:

– Propozycję mechanizmu ciągłego monitorowania (np. dashboardy, systemy alertów) z wykorzystaniem technologii analityki predykcyjnej opartej na AI, co pozwoli na szybkie wykrywanie niezgodności lub spadków jakości usług.

3. Minimalne wymagania dla rejestrów publicznych

Dobrze przygotowane w dokumencie:

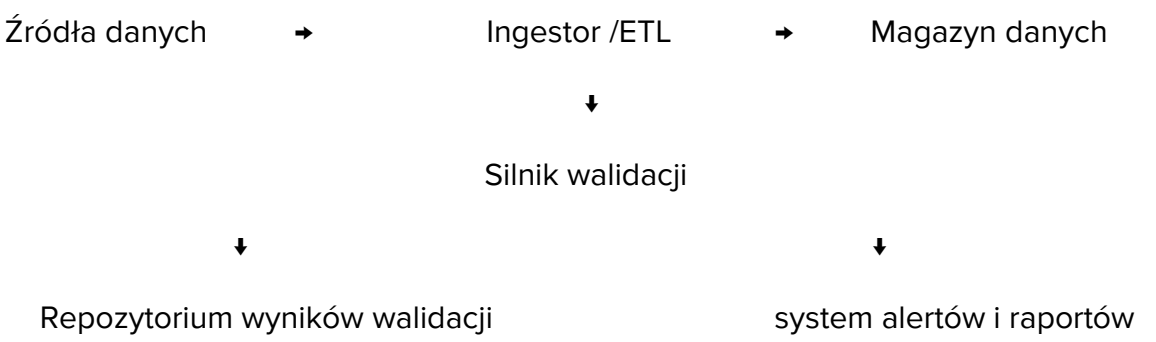
– Rozdział III wyznacza jasne wymagania dotyczące identyfikacji obiektów, struktur identyfikatorów oraz sposobu dokumentowania operacji na danych, co zapewnia spójność i możliwość automatycznego przetwarzania danych przez systemy AI.

– Wskazanie na stosowanie standardów (np. INSPIRE w kontekście danych przestrzennych) stanowi mocny element integracji z międzynarodowymi systemami.

Co dodać:

– Propozycję wdrożenia systemu walidacji danych rejestru, który na bieżąco sprawdza kompletność i aktualność danych, oraz mechanizmy automatycznego raportowania niezgodności.

Proponowana architektura systemu walidacji



1. **Ingestor/ETL**
    - Pobiera dane z rejestru (API, eksport plikowy, bezpośredni dostęp do bazy).
    - Normalizuje format (JSON/XML, UDF ➔ zunifikowany model).
2. **Magazyn Danych**
    - Przechowuje surowe i znormalizowane dane w hurtowni lub Data Lake.
    - Umożliwia historię zmian (audit log).
3. **Silnik Walidacji (Rules Engine)**
    - Definiuje reguły walidacyjne (np. JSON Schema, XPath, wyrażenia regularne, skrypty w Java/Python).

- Typowe reguły:
    - **Kompletność**: żadne pole obowiązkowe nie jest puste.
    - **Spójność**: zależności między polami (np. data zakończenia ≥ data rozpoczęcia).
    - **Aktualność**: na podstawie `updated_at` nie starsze niż X dni.
    - **Format**: wzorce (numer PESEL, NIP, kod pocztowy).

4. **Repozytorium Wyników Walidacji**
    - Baza lub tabela gromadząca: identyfikator rekordu, reguła, status (pass/fail), czas sprawdzenia, komunikat błędu.
5. **System Alertów i Raportów**
    - **Dashboard** KPI: procent rekordów niezgodnych, trendy w czasie.
    - **Alerty automatyczne**: e-mail/SMS/Slack/Tickets (JIRA) przy przekroczeniu progu błędów (np. >1% niezgodnych).
    - **Raporty periodyczne**: dzienne, tygodniowe, miesięczne, z możliwością drążenia (drill-down) wg rejestru.

4. Mechanizmy automatycznego raportowania niezgodności

- **Reguły progowe**: definiujemy progi akceptowalnej ilości błędów (np. do 0,5 % rekordów dziennie).
- **Powiadomienia inkrementalne**: wysyłane, gdy liczba błędów/rodzaj błędu przekroczy próg.
- **Integracja z systemem ticketowym**: tworzenie zadania dla odpowiedzialnego opiekuna rejestru.
- **Interaktywne raporty**: dostęp online, z filtrowaniem po rejestrach, typach błędów i czasie.

4. Minimalne wymagania dla systemów teleinformatycznych

Dobrze przygotowane w dokumencie:
– Rozdział IV szczegółowo określa wymagania funkcjonalne, wydajnościowe, bezpieczeństwa i kompatybilności systemów teleinformatycznych, co jest niezbędne przy tworzeniu środowiska umożliwiającego interoperacyjność .

– Wymagania dotyczące API, w tym stosowanie REST oraz SOAP, a także specyfikacje dotyczące kodowania, zarządzania logami i obsługi błędów, wskazują na wysoki poziom szczegółowości i spójności technicznej.

Co należy zmienić:
– Wskazanie na konieczność regularnego przeglądu i aktualizacji procedur bezpieczeństwa oraz standardów komunikacji, by były zgodne z dynamicznym rozwojem technologii.

5. Przepisy przejściowe i końcowe

Dobrze przygotowane w dokumencie:
– Rozporządzenie zawiera wyraźnie określone terminy wdrożenia poszczególnych przepisów, co umożliwia stopniowe dostosowanie systemów do nowych wymagań .
– Przepisy przejściowe zapewniają ciągłość funkcjonowania rejestrów i systemów, co jest kluczowe dla niezakłóconego działania administracji publicznej.

Co należy zmienić:
- Warto dodać konkretne terminy i kamienie milowe wdrażania nowych rozwiązań, szczególnie w kontekście implementacji interoperacyjności oraz aktualizacji systemów teleinformatycznych p. na Portalu Interoperacyjności i Architektury, można przygotować zestawienie z konkretnymi terminami określonymi w czasie..

Rekomendacje

Automatyzacja i maszynowa czytelność:
– Wszystkie udostępniane dane (definicje, metadane rejestrów, wyniki monitoringu API) powinny być dostępne w formatach umożliwiających automatyczną analizę (np. JSON, XML, JSON-LD).
– Propozycja stworzenia centralnego repozytorium danych technicznych, które wspiera integrację z narzędziami analityki big data oraz systemami AI.

Cel centralnego repozytorium danych technicznych

1. **Ujednolicenie i centralizacja wiedzy**
    - Zebranie wszystkich specyfikacji, opisów i metadanych technicznych w jednym miejscu.
    - Eliminacja „cichych aktów” i rozproszonej dokumentacji, co ułatwia zarządzanie zmianą i audyt.
2. **Wsparcie dla analityki Big Data i AI**

- Umożliwienie narzędziom automatycznego katalogowania i indeksowania źródeł danych.

- Dostęp do informacji o strukturze, jakości, wydajności i zależnościach, niezbędnych do trenowania modeli AI.

3. **Przyspieszenie integracji systemów**

    - Dostarczenie jednolitego API oraz wzorców (template'ów) dla pobierania metadanych i konstrukcji pipeline'ów.

    - Zmniejszenie kosztu „onboardingu" nowych źródeł danych.

Zakres danych technicznych

Kategoria	Przykładowe elementy
Schematy i struktury	• Definicje tabel/kolumn (nazwa, typ, rozmiar, ograniczenia)
• Relacje (klucze obce, asocjacje)	
• Widoki i materializowane widoki	
Metadane semantyczne	• Opisy pól (etykiety, komentarze)
• Mapowania do słowników i ontologii KRI	
• Wersje schematów (wersjonowanie)	
Lineage i zależności	• Źródła danych i ich pochodzenie (pipeline'y ETL/ELT)
• Przepływ danych między systemami	
• Historia transformacji i agregacji	

Jakość i profilowanie	• Statystyki kolumn (null rate, cardinality, rozkłady)
• Wyniki walidacji poprawności i spójności	
• Parametry czyszczenia i reguły standaryzacji	
Wydajność i monitoring	• Czas odpowiedzi zapytań i ETL
• Obciążenie systemów (CPU, pamięć, I/O)	
• Harmonogramy zadań i ich SLA	
API i interfejsy	• Specyfikacje REST/GraphQL/SOAP (OpenAPI, WSDL)
• Klucze uwierzytelniające, zakresy uprawnień (OAuth, JWT)	
• Przykłady zapytań i parametrów	
Modele i konfiguracje AI	• Schematy danych treningowych
• Feature store: definicje cech (features), ich częstotliwość odświeżania	
• Parametry modeli, metryki ewaluacji, artefakty (pickle, ONNX)	

Monitorowanie i analiza jakości danych:

– Wdrożenie mechanizmów monitorujących jakość danych (np. systemy alertujące o niezgodnościach, automatyczne raportowanie KPI) jest kluczowe dla zapewnienia interoperacyjności i efektywności systemów.

– Integracja tych mechanizmów z dashboardami analitycznymi oraz narzędziami do analizy predykcyjnej, co pozwoli na bieżące doskonalenie procesów.

Bezpieczeństwo i zgodność z normami:

– Aktualizacja odniesień do najnowszych standardów bezpieczeństwa (TLS 1.3, OpenID Connect, OAuth 2.0) oraz referencje do międzynarodowych norm, które zapewnią bezpieczną wymianę danych.

– Ujednolicenie dokumentacji technicznej dotyczącej API, aby była zgodna z najlepszymi praktykami (np. OpenAPI 3.0 lub nowszym).

Podsumowanie i konkretne propozycje rozwiązań

1. Wprowadzenie maszynowo czytelnego repozytorium definicji i metadanych, które będzie dostępne dla deweloperów i systemów AI.

2. Ujednolicenie formatów danych i odniesień do norm – z naciskiem na standardy otwarte (JSON, XML, JSON-LD, REST API).

3. Wdrożenie systemów monitoringu jakości danych i API, wspieranych przez narzędzia analityki predykcyjnej.

4. Stworzenie szczegółowych załączników technicznych, które ułatwią implementację nowych wymagań, przy jednoczesnym zachowaniu przejrzystości głównego tekstu rozporządzenia.

5. Ustalenie harmonogramu wdrożenia z kamieniami milowymi oraz utworzenie centralnego organu nadzorującego wdrażanie regulacji.

Załącznik 5 - analiza uzasadnienia dla projektu założeń projektu rozporządzenia w sprawie KRI

I. Cel i potrzeba regulacji

Dobrze przygotowane w dokumencie:

– Dokument jasno określa, że projektowane rozporządzenie ma na celu wdrożenie delegacji ustawowej, wprowadzającej nowe minimalne wymagania dla systemów teleinformatycznych, rejestrów publicznych oraz ustalenie Krajowych Ram Interoperacyjności. To podejście pozwala na podniesienie jakości wymiany danych między podmiotami publicznymi oraz ujednolicenie zasad interoperacyjności, co jest kluczowe przy wdrażaniu rozwiązań AI .

– Uzasadnienie odnosi się do problemów dotychczasowych przepisów – m.in. niskiego poziomu zrozumienia obowiązków, braku spójnych definicji oraz ograniczonego zakresu beneficjentów interoperacyjności.

Co dodać:

– Propozycję określenia standardowych metryk jakości danych, które będą monitorowane przez systemy AI – np. wskaźnik kompletności metadanych czy współczynnik aktualizacji danych.

– Wskazanie na potrzebę integracji z systemami analityki big data, co umożliwi automatyczne raportowanie efektów transformacji cyfrowej.

Co usunąć:

– Część historyczno-legislacyjną dotyczącą poprzednich rozporządzeń, jeżeli nie wpływa ona bezpośrednio na obecne potrzeby transformacji – skrócenie tego fragmentu pozwoli skupić się na celach przyszłościowych.

II. Zakres i uzasadnienie projektowanych przepisów

Dobrze przygotowane w dokumencie:

– Uzasadnienie prezentuje szeroki zakres zmian – od modyfikacji pojęć (np. „wymiana informacji" zmienionej na „wymiana danych") po aktualizację definicji technicznych (np. „architektura systemu teleinformatycznego" według ISO/IEC 42010:2007).

– Praca zespołów roboczych i grupy KRMC ds. Nowych KRI zapewnia, że projekt opiera się na konsultacjach społecznych oraz analizach praktycznych problemów występujących w systemach publicznych.

Co należy zmienić:

– Ujednolicić język definicyjny, tak aby wszystkie pojęcia (np. „model usługowy", „API", „poufność") były nie tylko zgodne z normami, ale też łatwe do automatycznej walidacji przez systemy informatyczne.

– Wprowadzić mechanizmy dokumentacji w formacie maszynowo czytelnym (np. JSON lub XML) dla kluczowych definicji, co ułatwi ich wykorzystanie przez narzędzia AI.

Co dodać:

– Propozycję stworzenia centralnego repozytorium, w którym zostaną umieszczone nie tylko definicje, ale i pełna dokumentacja techniczna (np. wzory identyfikatorów, standardy formatów danych) – co umożliwia deweloperom szybką integrację i automatyzację procesów.

– Konkretny opis hierarchii norm i standardów z odniesieniem do norm międzynarodowych (ISO, ITU, ETSI) oraz europejskich Ram Interoperacyjności, co wzmocni argumentację dotyczącą otwartości standardów.

Co usunąć:

– Fragmenty nadmiernie rozwijające tło legislacyjne, które nie wpływają bezpośrednio na nowe wymagania – tekst może być skrócony, by lepiej skoncentrować się na nowych celach.

III. Szczegółowe rozwiązania dotyczące rejestrów publicznych i systemów teleinformatycznych

Dobrze przygotowane w dokumencie:

– Rozdziały dotyczące minimalnych wymagań dla rejestrów publicznych (Rozdział III) i systemów teleinformatycznych (Rozdział IV) są bardzo szczegółowe. Zawierają one konkretne wytyczne dotyczące identyfikacji obiektów, struktury danych, formatu udostępniania danych oraz zasad działania API, co jest kluczowe dla automatyzacji i wdrożenia narzędzi AI .

Co należy zmienić:

– Należy uwzględnić, że dane udostępniane przez rejestry i systemy powinny być dostępne w formatach umożliwiających automatyczną analizę – np. JSON-LD, XML lub CSV, z pełną dokumentacją strukturalną.

– Doprecyzować wymagania dotyczące integracji systemów – wskazać, że wszystkie interfejsy API powinny być testowalne za pomocą narzędzi automatyzujących proces monitorowania wydajności (np. poprzez narzędzia do testowania API).

Co dodać:

– Propozycję wprowadzenia systemów monitoringu jakości danych, które będą wykorzystywać algorytmy analizy predykcyjnej do wykrywania niezgodności lub spadków jakości udostępnianych danych.

System monitoringu jakości danych: koncepcja rozwiązania

Źródła danych ➜ Ingestor/ETL ➜ Profiling & historia KPI ➜ Silnik predykcji ➜ Detektor anomalii ➜ Dashboard & alerty

- **Ingestor/ETL**: pobiera zmiany (batch/CDC), normalizuje i zapisuje w hurtowni.
- **Profiling & historia KPI**: generuje szereg czasowy metryk jakości (kompletność, spójność, aktualność).
- **Silnik predykcji**: na podstawie danych historycznych prognozuje przyszłe wartości KPI.

- **Detektor anomalii**: porównuje prognozy z rzeczywistymi pomiarami, wskazuje odchylenia.
- **Dashboard & alerty**: wizualizuje trendy i prognozy, wysyła powiadomienia (e-mail/Slack/tickety).

Kluczowe komponenty

– **Profiling danych** Automatyczne zbieranie statystyk (np. % null, unikalność, dystrybucje).
– **Modelowanie czasowe** ARIMA/Prophet do trendów i sezonowości; LSTM do wykrywania nieliniowych wzorców.
– **Detekcja anomalii** Algorytmy bez nadzoru (Isolation Forest, One-Class SVM) oraz proste testy statystyczne (Z-score).
– **Reguły eskalacji** Definicja progów (np. spadek kompletności >2 σ), automatyczne przekazywanie incydentów.
– **System powiadomień** Konfigurowalne kanały (Slack, e-mail, JIRA), z opisem przewidywanego i zaobserwowanego problemu.
– **Interaktywny dashboard** Porównanie historycznych metryk z prognozami, lista aktywnych alertów i ich przyczyn.

– Zalecenie wdrożenia dashboardów kontrolujących parametry takie jak: dostępność, integralność, autentyczność oraz szybkość reakcji API.

Co usunąć:
– Nadmiernie szczegółowe opisy formatów i procedur, które można przekazać w odrębnych aktach wykonawczych lub załącznikach – główny tekst rozporządzenia powinien pozostać czytelny, a szczegóły techniczne opierać się na odniesieniach do standardów.

IV. Wejście w życie przepisów i przepisy przejściowe

Dobrze przygotowane w dokumencie:
– Projekt przewiduje różne terminy wdrożenia poszczególnych przepisów, co umożliwia stopniowe dostosowanie systemów do nowych wymagań – rozwiązanie to minimalizuje ryzyko zakłóceń w funkcjonowaniu administracji publicznej.
– Przepisy przejściowe obejmują zarówno rejestry, jak i systemy teleinformatyczne, co zapewnia ciągłość działania.

Co należy zmienić:
– Rozważyć dodanie szczegółowych kamieni milowych wdrożenia kluczowych elementów, takich jak repozytorium interoperacyjności czy systemy monitoringu API, aby podmioty publiczne miały jasny plan działań.

Co dodać:

– Propozycję utworzenia centralnego organu lub platformy do monitorowania postępów wdrażania nowych przepisów oraz raportowania wyników – co pozwoli na bieżące korekty i wsparcie techniczne.

– Zalecenie przeprowadzenia szkoleń dla pracowników administracji publicznej w zakresie nowych wymagań oraz korzystania z narzędzi automatyzujących kontrolę jakości danych.

Co usunąć:

– Fragmenty dotyczące przepustowości, które nie mają wpływu na efektywność wdrożenia nowych rozwiązań – skrócenie opisu może zwiększyć przejrzystość harmonogramu.

V. Pozostałe informacje i wnioski ogólne

Dobrze przygotowane w dokumencie:

– Uzasadnienie kompleksowo przedstawia tło legislacyjne oraz praktyczne aspekty funkcjonowania dotychczasowych rozporządzeń KRI.

– Podkreślona jest potrzeba poprawy interoperacyjności, standaryzacji i automatyzacji procesów wymiany danych, co jest kluczowe dla wdrażania narzędzi AI oraz analityki big data.

Co należy zmienić:

– Skoncentrować się na praktycznych efektach wdrożenia, takich jak: zwiększenie efektywności obsługi elektronicznych usług publicznych, poprawa jakości danych oraz ujednolicenie procesów administracyjnych.

– Zredukować nadmierne odniesienia do kwestii formalno-prawnych, skupiając się na technicznych i operacyjnych aspektach, które mają bezpośredni wpływ na automatyzację procesów.

Co dodać:

– Propozycję konkretnych działań wdrożeniowych, m.in. pilotażowych projektów integracyjnych w wybranych instytucjach, które pozwolą na przetestowanie nowych ram interoperacyjności przed pełnym wdrożeniem.

– Wskazanie, że wdrożenie rozporządzenia powinno być monitorowane poprzez systemy raportowania z wykorzystaniem narzędzi analityki predykcyjnej oraz dashboardów jakościowych, co umożliwi ciągłe doskonalenie procesów.

Co usunąć:

– Fragmenty opisujące ogólną sytuację ekonomiczną i społeczną, które nie wpływają bezpośrednio na kwestie interoperacyjności i wymiany danych – zwięzłość w tej części ułatwi koncentrację na głównych celach projektu.

Rekomendacje

1. **Repozytorium i maszynowa czytelność danych:**

– Utworzenie centralnego repozytorium zawierającego maszynowo czytelne definicje, schematy danych, metadane rejestrów i specyfikacje API.
– Wdrożenie standardów takich jak JSON-LD, XML lub JSON Schema, co ułatwi integrację z narzędziami analityki big data.

1. **Monitoring jakości danych:**

– Wprowadzenie systemów monitoringu jakości danych, które będą korzystać z algorytmów AI do wykrywania niezgodności, braków lub anomalii.
– Implementacja dashboardów kontrolnych, raportujących kluczowe wskaźniki (dostępność, integralność, autentyczność) oraz automatyczne alerty w przypadku wykrycia nieprawidłowości.

3. **Standaryzacja i automatyzacja:**

– Ujednolicenie formatów danych, metod wymiany informacji oraz standardów API z odniesieniami do norm międzynarodowych (ISO, ETSI, W3C).
– Automatyzacja procesów dokumentowania operacji w systemach (logi, znaczniki czasu) w celu zapewnienia pełnej rozliczalności i możliwości analizy przez systemy AI.

4. **Harmonogram wdrożenia i wsparcie techniczne:**

– Ustalenie szczegółowych kamieni milowych wdrożenia kluczowych elementów rozporządzenia oraz utworzenie centralnego organu nadzorującego wdrożenie, który będzie wspierał podmioty publiczne szkoleniami i wsparciem technicznym.

Podsumowanie

Uzasadnienie założeń projektu rozporządzenia ws. KRI przedstawia kompleksową argumentację za potrzebą nowej regulacji, która ma na celu poprawę interoperacyjności, ujednolicenie standardów wymiany danych oraz automatyzację procesów w administracji publicznej. Z perspektywy danych i AI rekomenduje się:

- Doprecyzowanie definicji i stworzenie maszynowo czytelnego repozytorium kluczowych danych i specyfikacji technicznych.
- Wdrożenie mechanizmów monitoringu jakości danych oraz systemów analityki predykcyjnej, które umożliwią ciągłe doskonalenie usług publicznych.
- Ujednolicenie standardów wymiany danych (np. JSON-LD, REST API) oraz integracja z platformami big data, co ułatwi automatyzację i wdrożenie narzędzi AI.
- Wyznaczenie szczegółowego harmonogramu wdrożenia i zapewnienie wsparcia technicznego dla podmiotów publicznych.

Implementacja powyższych rekomendacji pozwoli nie tylko na spełnienie wymogów delegacji ustawowej, ale również stworzy solidne podstawy dla rozwoju nowoczesnych systemów informacyjnych, umożliwiających efektywną analizę i przetwarzanie danych przy wykorzystaniu narzędzi AI.

Załącznik 6 - analiza założeń projektu rozporządzenia w sprawie w sprawie repozytorium interoperacyjności

I. Przepisy ogólne i definicje (§ 1–2)

Dobrze przygotowane w dokumencie:
– Dokument precyzyjnie określa zakres rozporządzenia, wskazując funkcje repozytorium, sposób kategoryzacji publikowanych informacji oraz metodę realizacji obowiązków podmiotów publicznych.
– Zestaw definicji (takich jak „gestor rejestru publicznego", „metadane rejestru publicznego" czy „podmiot") stanowi solidną podstawę do jednolitego stosowania rozporządzenia, co umożliwia automatyzację przetwarzania danych przez systemy AI.

Co należy zmienić:
– Ujednolicić format prezentacji definicji i rozważyć dołączenie wersji maszynowo czytelnej (np. w formacie JSON lub XML) jako załącznika.
– Doprecyzować niektóre terminy, aby umożliwić automatyczną walidację – np. określić dokładnie strukturę metadanych, którą systemy AI będą mogły analizować bez dodatkowych modyfikacji.

Format np. JSON Schema (lub XSD/SHACL) – obsługiwany natywnie przez narzędzia AI i walidatory.

Core-właściwości

```
 json
{

  "id": "UUID",

  "schemaVersion": "x.y.z",

  "createdAt": "date-time",

  "updatedAt": "date-time",

  "sourceSystem": "string",

  "owner": "string",

  "domain": "string",

  "fieldDefinitions": [ ... ]

}
```

– fieldDefinitions: tablica obiektów z polami name, type, required oraz opcjonalnie pattern/format i properties.

Automatyczna walidacja

- CI/CD → JSON Schema Validator (np. w GitLab CI/Jenkins)
- Podnoś schemaVersion przy zmianach → automatyczna dokumentacja (Swagger/Redoc)

Dobre praktyki

- Namespace'y i prefixy (np. http://kri.gov.pl/meta#)
- Mapowanie do słowników/ontologii (RDF/OWL) w fieldDefinitions
- Przechowywanie historycznych metryk w opcjonalnym qualityMetrics

Propozycje rozwiązań:

1. Stworzyć elektroniczny słownik terminologiczny repozytorium, dostępny w formacie API, który umożliwi integrację z narzędziami analityki big data.
2. W definicjach odnieść się do międzynarodowych norm (np. ISO/IEC 42010 dla architektury systemów), co ujednolici stosowanie pojęć w praktyce.

II. Szczegółowe funkcje repozytorium interoperacyjności (Rozdział II, § 3–6)

Dobrze przygotowane w dokumencie:

– Rozporządzenie dokładnie określa funkcje repozytorium, w tym dwie główne metody dostępu – graficzny interfejs użytkownika (GUI) oraz interfejs programistyczny (API).

– Wprowadzenie wymagań dotyczących oznaczania metadanych (wersja, data publikacji, status) sprzyja zapewnieniu integralności i rozliczalności operacji – kluczowych z punktu widzenia automatyzacji procesów przez systemy AI.

Co należy zmienić:

– Dokładniej określić formaty danych, w jakich mają być publikowane metadane oraz informacje o API (np. JSON, XML, JSON-LD), aby ułatwić ich automatyczną analizę przez narzędzia analityki.

– Ujednolicić proces subskrypcji powiadomień – warto sprecyzować mechanizmy automatycznego pobierania i przetwarzania takich alertów przez systemy monitorujące (tj. subskrypcji mogłyby też dokonać systemy monitorujące, a nie tylko uwierzytelnieni użytkownicy).

Propozycje rozwiązań:

1. W § 3 dodać zapis, że informacje publikowane przez repozytorium muszą być dostępne w formatach przyjaznych maszynom, co umożliwi integrację z platformami AI (warto objąć formatem maszynowy wszystkie dane w repozytorium interoperacyjności).
2. Rozważyć wdrożenie mechanizmu automatycznego monitoringu dostępności repozytorium (np. system alertów) z możliwością generowania raportów w czasie rzeczywistym, co zwiększy kontrolę nad ciągłością usług.

III. Sposób kategoryzacji informacji (Rozdział III, § 7)

Dobrze przygotowane w dokumencie:

– Dokument wprowadza kategoryzację informacji według ustalonych kryteriów (przedmiotowego, podmiotowego, metadanych rejestrów i informacji o API), co sprzyja uporządkowaniu i automatycznemu wyszukiwaniu danych.

– Ustalenie statusów rejestrów (planowany, użytkowany, wycofany) umożliwia dynamiczną kontrolę nad danymi oraz wspiera procesy decyzyjne przy wdrażaniu narzędzi AI.

Co należy zmienić:

– Dokładniej określić zasady przydzielania statusów i kategorię informacji, aby proces ten był jednoznaczny dla systemów informatycznych – może to wymagać wprowadzenia schematów lub modeli danych.

Propozycje rozwiązań:

1. Zaproponować stworzenie schematów XML/JSON opisujących strukturę kategorii i statusów, które będą publikowane wraz z danymi repozytorium.
2. Umożliwić automatyczną aktualizację statusów przez systemy integrujące się z repozytorium.

IV. Szczegółowy sposób prowadzenia repozytorium (Rozdział IV, § 8–9)

Dobrze przygotowane w dokumencie:

– Repozytorium jest określone jako dostępne całodobowo, a informacje o przerwach serwisowych są publikowane – to ważne dla zapewnienia ciągłości usług oraz zaufania użytkowników.

– Uregulowanie uprawnień dla różnych kategorii użytkowników (użytkownik zwykły, uwierzytelniony, reprezentanci, administrator) jest szczegółowe i umożliwia precyzyjne zarządzanie dostępem, co jest kluczowe w systemach opartych na AI, gdzie rozliczalność operacji ma znaczenie.

Co należy zmienić:

– Upewnić się, że mechanizmy uwierzytelniania i zarządzania uprawnieniami są zgodne z najnowszymi standardami bezpieczeństwa (np. OpenID Connect, OAuth 2.0) oraz umożliwiają automatyczną integrację z systemami monitorującymi.

Propozycje rozwiązań:

1. Dodać zapis dotyczący automatycznej aktualizacji listy użytkowników i ich uprawnień przez system zarządzania tożsamością, co umożliwi efektywną integrację z narzędziami analityki big data.
2. Wprowadzić interfejs API do zarządzania subskrypcją powiadomień, który będzie wspierał mechanizmy automatycznego przetwarzania alertów przez systemy AI.

V. Sposób realizacji obowiązków podmiotów publicznych (Rozdział V, § 10–12)

Dobrze przygotowane w dokumencie:

– Rozporządzenie precyzyjnie określa terminy publikacji informacji przez gestora rejestru i podmiot używający systemu teleinformatycznego – najpóźniej w ciągu 7 dni od zmiany, co umożliwia bieżące aktualizacje.

– Wskazane obowiązki, takie jak publikacja statystyk użycia API czy udostępnianie przykładowych zestawów (SDK), sprzyjają transparentności i umożliwiają deweloperom automatyzację procesów integracyjnych.

Co należy zmienić:

– Uzupełnić wymagania o format publikowanych danych – określić, że muszą być zgodne ze standardami maszynowo czytelnymi (np. JSON, XML) i zawierać pełną dokumentację strukturalną.

Propozycje rozwiązań:

1. W § 10 i § 11 dodać zapisy wymagające, aby wszystkie publikowane informacje były uzupełnione o metadane, które umożliwiają automatyczną walidację przez systemy AI.
2. Zaproponować wdrożenie mechanizmu monitorowania i automatycznego raportowania dostępności API, z wykorzystaniem narzędzi do analizy danych w czasie rzeczywistym.

VI. Przepisy przejściowe i końcowe (Rozdział VI, § 13)

Dobrze przygotowane w dokumencie:

– Określenie terminu wejścia w życie (14 dni od ogłoszenia) jest przejrzyste i pozwala na szybką adaptację przepisów.

– Zapewnienie ciągłości usług i możliwość dokonywania zmian w późniejszym terminie jest korzystne z perspektywy elastycznego wdrażania rozwiązań IT.

Co należy zmienić:

– Rozważyć dodanie szczegółowego harmonogramu wdrożenia poszczególnych funkcjonalności repozytorium, aby podmioty publiczne miały jasny plan dostosowania się do nowych wymagań.

Propozycje rozwiązań:

1. Utworzyć dedykowany organ lub platformę monitorującą wdrażanie rozporządzenia, który będzie regularnie raportował postępy wdrożeń.
2. Zapewnić wsparcie szkoleniowe i konsultacyjne dla podmiotów publicznych w zakresie korzystania z repozytorium oraz integracji z systemami zarządzania danymi.

Rekomendacje

1. **Repozytorium jako centralny hub danych:**

– Utworzenie repozytorium interoperacyjności, które nie tylko udostępnia metadane i informacje o API, ale także umożliwia automatyczną integrację z systemami analityki big data oraz AI, np. poprzez udostępnianie danych w formatach JSON-LD lub XML.

2. **Automatyzacja i monitorowanie:**

– Wdrożenie mechanizmów automatycznego monitorowania jakości danych oraz dostępności API, w tym systemów alertowych i dashboardów, co pozwoli na bieżącą analizę i optymalizację procesów.

3. **Standaryzacja i dokumentacja:**

– Ujednolicenie formatów publikowanych informacji, ich dokumentacja oraz udostępnienie szczegółowych specyfikacji w załącznikach do rozporządzenia, co ułatwi integrację z systemami AI i aplikacjami deweloperskimi.

4. **Zarządzanie uprawnieniami i bezpieczeństwem:**

– Upewnić się, że mechanizmy uwierzytelniania, autoryzacji oraz zarządzania uprawnieniami są zgodne z najnowszymi standardami (np. OpenID Connect, OAuth 2.0), co zabezpieczy dane oraz umożliwi automatyczną kontrolę dostępu.

Załącznik 7 - analiza uzasadnienia założeń projektu rozporządzenia w sprawie repozytorium interoperacyjności

I. Cel i potrzeba regulacji

Dobrze przygotowane w dokumencie:

– Dokument jasno określa, że rozporządzenie ma realizować delegację ustawową wynikającą z nowelizacji ustawy o informatyzacji, w szczególności w zakresie określenia funkcji repozytorium interoperacyjności, kategoryzacji informacji oraz sposobu prowadzenia tego repozytorium.

– Uzasadnienie odnosi się do problemów dotychczasowych rozwiązań, wskazując m.in. na „martwy" charakter istniejącego repozytorium oraz niedostosowanie strukturalne do aktualnych wymagań interoperacyjnych. Takie podejście jest kluczowe dla wdrożenia mechanizmów automatycznej analizy danych przez systemy AI.

Co należy zmienić:

– Wzmocnić argumentację poprzez określenie konkretnych wskaźników efektywności, np. liczby aktualizacji danych, wskaźnika błędów wynikających z ograniczeń schematów atomowych lub procentowego wzrostu wykorzystania repozytorium przez podmioty publiczne.

– Ujednolicić pojęcia związane z „danymi” oraz „informacjami” – tak, aby wdrożone mechanizmy mogły automatycznie przetwarzać i walidować przekazywane metadane.

Propozycje rozwiązań:

1. Wprowadzenie zestawu miar jakościowych (np. czas reakcji systemu, kompletność metadanych) oraz mechanizmu raportowania wyników, co umożliwi monitorowanie postępów po wdrożeniu rozporządzenia.

2. Określenie standardów formatów danych (np. JSON-LD, XML) wykorzystywanych w repozytorium, by systemy AI mogły je automatycznie przetwarzać.

II. Analiza stanu funkcjonowania repozytorium interoperacyjności

Dobrze przygotowane w dokumencie:
– Uzasadnienie przedstawia szczegółową ocenę dotychczasowego stanu repozytorium – wskazuje, że jest ono uznawane za „martwe rozwiązanie”, co wynika z braku aktualizacji struktur danych i niedostosowania schematów do rzeczywistych danych publikowanych przez rejestry publiczne.
– Odwołanie do liczby systemów (ponad 1300) oraz rejestrów (prawie 500) podkreśla skalę problemu i konieczność wdrożenia nowego, dynamicznego rozwiązania.

Co należy zmienić:
– Ujednolicić sposób prezentacji danych – np. zapewnić, aby wszystkie publikowane metadane były maszynowo czytelne i zgodne z nowoczesnymi standardami (JSON-LD, XML Schema).
– Wprowadzić mechanizm automatycznego monitorowania zgodności publikowanych struktur z wymaganiami modelu danych, tak aby podmioty były natychmiast informowane o niedopasowaniach.

Propozycje rozwiązań:

1. Wdrożenie automatycznych narzędzi walidacji, które na bieżąco sprawdzą, czy metadane rejestrów i informacji o API spełniają określone normy – możliwe wykorzystanie algorytmów uczenia maszynowego do analizy jakości danych.
2. Zaprojektowanie interfejsu API repozytorium, który umożliwi automatyczne pobieranie, walidację i raportowanie aktualizacji, co poprawi funkcjonalność repozytorium i umożliwi jego efektywną integrację z systemami AI.

III. Zakres i uzasadnienie projektowanych przepisów

Dobrze przygotowane w dokumencie:

– Dokument wyraźnie określa zakres przepisów, obejmujący funkcję repozytorium, sposób kategoryzacji informacji oraz obowiązki podmiotów publicznych związane z udostępnianiem danych.

– Uwzględnienie wyników prac zespołów roboczych oraz warsztatów (od maja 2022 r. po październik 2024 r.) stanowi mocny argument, że projekt opiera się na szerokich konsultacjach i analizie praktycznych problemów.

Co należy zmienić:

– Doprecyzować wymagania dotyczące aktualizacji struktur danych – określić dokładnie, jakie zmiany w modelu danych (syntaktyka/semantyka) muszą być natychmiast publikowane przez gestora.

– Ujednolicić język regulacyjny, aby ułatwić automatyczną interpretację i wdrażanie rozwiązań przez systemy informatyczne. Zalecamy wprowadzenie uproszczonego, kontrolowanego języka naturalnego (CNL), w którym każde założenie czy wymóg zapisujemy w postaci logicznej formuły. Taki sposób zapisu eliminuje niejednoznaczności i pozwala bezpośrednio przekładać przepis na regułę wykonywaną przez silnik biznesowy. Reguły powinny opierać się na ściśle zdefiniowanym modelu składniowym IF–THEN–ELSE, wykorzystującym gotowe predykaty (takie jak exists, matches czy within) oraz podstawowe operatory logiczne AND, OR i NOT. Aby zapewnić spójność terminologiczną, każdy kluczowy wyraz—tak jak „rekord", „usługa" czy „retry"—powinien być opisany we wspólnym słowniku lub ontologii, a wszystkie nazwy muszą odnosić się do tego samego zestawu definicji i namespace'ów. Gotowe reguły serializujemy w ustandaryzowanym formacie JSON lub XML (np. z użyciem RuleML, LegalRuleML czy schematu przypominającego XACML). Dzięki temu definicje przenoszą się bezpośrednio do systemów walidujących i wykonawczych, co skraca czas wdrożenia nowych przepisów, eliminuje błędy interpretacyjne i umożliwia pełną automatyzację kontroli zgodności.

Propozycje rozwiązań:

1. Stworzenie szczegółowych wytycznych (np. w formie załączników technicznych) opisujących wymagania dotyczące aktualizacji metadanych oraz sposobu ich publikacji w repozytorium.
2. Zapewnienie, aby wszystkie przepisy dotyczące publikacji informacji były opatrzone metadanymi umożliwiającymi automatyczną weryfikację – co umożliwia systemom AI bieżące monitorowanie poprawności danych.
    i W praktyce oznacza to, że każdy przepis nakazujący publikację określonej informacji musi zostać wzbogacony o precyzyjny, sformalizowany opis – czyli metadane – które system automatyczny będzie mógł odczytać bez dodatkowej ingerencji człowieka. Takie metadane zawierają m.in. identyfikator przepisu, datę wejścia w życie, zakres obowiązku (jakie dane), format pliku (JSON, XML, PDF), częstotliwość udostępniania oraz lokalizację źródła (np. adres w Biuletynie Informacji Publicznej). Gdy tylko system wykona zaplanowane

zadanie, porównuje ten zestaw wymagań z rzeczywistą publikacją: sprawdza termin dostępności, obecność wszystkich wymaganych pól, zgodność ze wzorcowym schematem, a nawet to, czy dokument nie narusza zasad poufności.

ii Jeśli któryś z warunków nie zostanie spełniony – na przykład plik nie pojawi się w wyznaczonym czasie lub będzie brakować kluczowego elementu – walidator automatycznie generuje raport lub wysyła alarm do odpowiedzialnego organu. Jednocześnie każda zmiana prawa, która wprowadza nowy schemat lub modyfikuje częstotliwość publikacji, zostaje naniesiona na wspólną bazę metadanych, a system zaczyna weryfikować w oparciu o zaktualizowany zestaw reguł. W rezultacie nie tylko znika potrzeba ręcznej interpretacji przepisów, ale uzyskujemy też pełną historię weryfikacji – kiedy i z jakim efektem dany dokument został sprawdzony – co znacznie usprawnia audyt i zarządzanie zgodnością.

IV. Funkcje repozytorium interoperacyjności i wymagania techniczne

Dobrze przygotowane w dokumencie:

– Rozporządzenie szczegółowo opisuje funkcje repozytorium, takie jak dostęp do informacji przez GUI i API, możliwość dodawania oraz subskrypcji powiadomień, co sprzyja automatyzacji procesów i integracji z narzędziami big data.

– Precyzyjne określenie obowiązków podmiotów (gestorów, podmiotów używających systemów) zwiększa transparentność oraz rozliczalność operacji.

Co należy zmienić:

– Doprecyzować formaty, w których muszą być publikowane metadane i informacje o API – wskazać, że powinny być dostępne w formatach maszynowo czytelnych (np. JSON, XML, JSON-LD).

– Ujednolicić mechanizmy subskrypcji powiadomień – określić, jak będą one przekazywane i jakie informacje powinny zawierać, aby były użyteczne dla systemów monitorujących.

Propozycje rozwiązań:

1. Wprowadzić zapis, że wszystkie interfejsy repozytorium muszą udostępniać dane w formacie JSON-LD lub XML, co umożliwi integrację z narzędziami analityki i systemami AI.
2. Rozważyć wdrożenie mechanizmu automatycznego generowania powiadomień (np. poprzez webhooki), który umożliwi natychmiastowe informowanie o aktualizacjach lub błędach w publikowanych danych.

V. Sposób realizacji obowiązków przez podmioty publiczne

Dobrze przygotowane w dokumencie:

– Projekt określa szczegółowo terminy publikacji zmian (7 dni od wystąpienia zmiany) oraz obowiązki podmiotów dotyczące publikowania metadanych i informacji o API, co sprzyja bieżącej aktualizacji repozytorium.
– Wprowadzenie obowiązku publikowania statystyk użycia API i przykładów zestawów SDK wspiera transparentność oraz umożliwia deweloperom automatyczną integrację.

Co należy zmienić:
– Upewnić się, że publikowane informacje są uzupełnione o kluczowe metadane, umożliwiające automatyczną analizę przez systemy AI, np. daty modyfikacji, wersje, statusy.
– Doprecyzować mechanizmy kontroli i weryfikacji jakości publikowanych danych przez ministra, aby proces ten był automatyczny i wspierany narzędziami analityki.

Propozycje rozwiązań:

1. Stworzyć szczegółowe wytyczne (np. w załącznikach) dotyczące struktury publikowanych danych – określić obowiązkowe pola, formaty i metadane, które umożliwią automatyczną walidację.
2. Wdrożyć systemy automatycznego monitorowania i raportowania dostępności API oraz jakości publikowanych danych, które będą integrować się z centralnym panelem kontrolnym ministerstwa.

VI. Wejście w życie przepisów i pozostałe informacje

Dobrze przygotowane w dokumencie:
– Projekt określa termin wejścia w życie (14 dni od ogłoszenia), co zapewnia szybką adaptację nowych przepisów.
– Uzasadnienie zawiera informacje dotyczące zgodności z prawem UE oraz wskazania o braku bezpośredniego wpływu na sytuację ekonomiczną rodzin czy mikroprzedsiębiorców, co jest standardowym elementem tego typu regulacji.

Co należy zmienić:
– Można rozważyć dodanie szczegółowego harmonogramu wdrożenia kluczowych funkcji repozytorium, aby podmioty publiczne miały jasny plan adaptacji do nowych wymagań.

Propozycje rozwiązań:

1. Utworzenie dedykowanego organu lub platformy monitorującej wdrożenie rozporządzenia oraz raportującej postępy wdrożenia kluczowych funkcji repozytorium.
2. Zapewnienie wsparcia szkoleniowego dla podmiotów publicznych w zakresie korzystania z repozytorium oraz integracji z systemami zarządzania danymi.

Rekomendacje

1. **Repozytorium jako centralny hub danych:**

– Upewnić się, że wszystkie dane i metadane publikowane w repozytorium są udostępniane w formatach maszynowo czytelnych (np. JSON-LD, XML) i opatrzone szczegółową dokumentacją.
– Stworzyć interfejs API umożliwiający automatyczną integrację z narzędziami analityki big data oraz systemami AI.

2. **Automatyzacja monitoringu i walidacji:**

– Wdrożyć mechanizmy automatycznego monitorowania jakości danych i dostępności API, z systemami alertów oraz dashboardami do analizy w czasie rzeczywistym.
– Umożliwi to szybkie reagowanie na niezgodności oraz optymalizację procesów publikacji i aktualizacji.

3. **Ujednolicenie standardów i bezpieczeństwa:**

– Wprowadzić zapisy wymagające stosowania nowoczesnych standardów uwierzytelniania i zarządzania uprawnieniami (np. OpenID Connect, OAuth 2.0), co zabezpieczy dostęp do repozytorium i umożliwia automatyczną kontrolę dostępu.
– Ujednolicić standardy publikacji danych, korzystając z odniesień do norm międzynarodowych (ISO, ETSI, W3C).

4. **Wsparcie dla deweloperów i integratorów:**

– Udostępnić zestawy SDK, dokumentację interfejsu API oraz narzędzia do automatycznego generowania kodu, co ułatwi integrację systemów publicznych z repozytorium oraz z narzędziami AI.

Podsumowanie

Założenia projektu rozporządzenia ws. repozytorium interoperacyjności opierają się na solidnych podstawach delegacji ustawowej i odpowiada na realne problemy związane z niedostosowaniem dotychczasowych rozwiązań do współczesnych wymagań interoperacyjnych. Rekomendujemy:

- Doprecyzowanie formatów publikowanych danych i udostępnienie ich w formatach maszynowo czytelnych (np. JSON-LD, XML).
- Wdrożenie mechanizmów automatycznego monitorowania i walidacji jakości danych oraz dostępności API.
- Ujednolicenie procedur zarządzania uprawnieniami z wykorzystaniem nowoczesnych standardów uwierzytelniania i autoryzacji.
- Zapewnienie wsparcia technicznego oraz opracowanie szczegółowego harmonogramu wdrożenia z wyznaczonymi kamieniami milowymi.

Implementacja powyższych rozwiązań pozwoli, że repozytorium interoperacyjności stanie się nowoczesnym, dynamicznym narzędziem wspierającym automatyczną analizę, wymianę i przetwarzanie danych przez systemy AI, co w rezultacie przyczyni się do poprawy jakości usług publicznych.