

OPIS ZAŁOŻEŃ PROJEKTU INFORMATYCZNEGO

Tytuł projektu	Polska Tarcza PNT Moduł 1		
Wnioskodawca	Minister Finansów i Gospodarki		
Beneficjent	Główny Urząd Geodezji i Kartografii (GUGiK)		
Partnerzy	Ministerstwo Obrony Narodowej (MON)		
Źródło finansowania	Budżet państwa: część budżetowa cz. 83 przynależna do cz. 27 oraz środki programu Fundusze Europejskie na Rozwój Cyfrowy 2021-2027, Działanie FERC.04.01 Wzmocnienie cyberbezpieczeństwa oraz rozwój odpornej infrastruktury przetwarzania danych		
Całkowity koszt projektu	27 000 000,00 zł		
Planowany okres realizacji projektu	11-2026 do 10-2028		
Osoba kontaktowa	Szymon Wajda	szymon.wajda@gugik.gov.pl	225322565 501561626

1. POWODY PODJĘCIA PROJEKTU

1.1. Identyfikacja problemu i potrzeb

Projekt wypełnia lukę w cyberodporności państwa dotyczącą usług pozycji, nawigacji i czasu (PNT) opartych na GNSS. Usługi te są krytycznym komponentem procesów cyfrowych, administracyjnych, gospodarczych, naukowych i obronnych, ponieważ zapewniają wiarygodną informację o położeniu, czasie i synchronizacji. System ASG-EUPOS, utrzymywany przez GUGiK, realizuje geodezyjne układy odniesienia w Polsce (PL-ETRF2000, PL-ETRF89) i obsługuje ponad 20 tys. użytkowników, w tym podmioty geodezyjne, budowlane i drogowe.

Problemem jest rosnąca ekspozycja usług PNT na zagrożenia hybrydowe i cyberfizyczne, w szczególności jamming i spoofing GNSS, prowadzące do utraty dostępności i integralności danych, błędnego wyznaczania pozycji, zaburzeń synchronizacji czasu oraz decyzji opartych na niewiarygodnych informacjach. Skutki dotyczą geodezji, transportu, energetyki, telekomunikacji, lotnictwa, zarządzania kryzysowego, infrastruktury krytycznej i obronności.

Obecnie podmioty te nie mają zintegrowanej państwowej warstwy cyberbezpieczeństwa PNT/ GNSS. Brakuje monitoringu jakości sygnału i usług ASG-EUPOS, detekcji, kategoryzacji i lokalizacji zakłóceń, korelacji zdarzeń, jednego obrazu sytuacyjnego, wymiany alertów oraz wsparcia ciągłości działania przy degradacji sygnału. Brak tych produktów powoduje rozbieżność między dojrzałą usługą referencyjną a oczekiwanym modelem odporności państwa. Projekt usuwa tę rozbieżność przez budowę i modyfikację systemów i modułów analitycznych, API, usług statusowych, alertowych i raportowych oraz platformy integracyjnej Polska Tarcza PNT. Monitoring GNSS i ASG-EUPOS zapewni ocenę jakości PNT. Moduły detekcji jammingu i spoofingu umożliwią wykrywanie, klasyfikację i ocenę wpływu incydentów. Platforma integracyjna stworzy jedno źródło danych o zakłóceniach sygnałów GNSS dla GUGiK, MON, służb, JST, regulatorów i operatorów infrastruktury krytycznej. API i feedy alertowe umożliwią dystrybucję informacji, szybsze reagowanie i utrzymanie wiarygodnych usług PiT

Interesariusz	Zidentyfikowany problem	Szacowana wielkość grupy
---------------	-------------------------	--------------------------

Interesariusz	Zidentyfikowany problem	Szacowana wielkość grupy
Pracownicy GUGiK	Brak jednej, zintegrowanej i interoperacyjnej warstwy państwowej do monitorowania jakości GNSS i ASG-EUPOS, automatycznej dystrybucji alertów, obsługi incydentów PNT oraz wymiany danych między resortami i jednostkami realizującymi zadania publiczne. Szacowaną grupę stanowią 20 pracowników IT oraz 200 pracowników nie-IT odpowiedzialnych za utrzymanie jakości danych GNSS i ASG-EUPOS	220
Organy odpowiedzialne za bezpieczeństwo	Brak ciągłego monitorowania jakości PNT/ GNSS, szybkiej detekcji, klasyfikacji i lokalizacji zakłóceń oraz wspólnego obrazu sytuacyjnego dla działań operacyjnych, zarządzania kryzysowego i reagowania. Szacuje się, że bezpośrednimi lub pośrednimi użytkownikami projektowanej warstwy monitorowania, detekcji i ostrzegania PNT może być ok. 10 tys. przedstawicieli Sił Zbrojnych RP, organów odpowiedzialnych za cyberbezpieczeństwo oraz służb mundurowych i ratunkowych. Grupa ta obejmuje w szczególności stanowiska dowodzenia, komórki geoinformacyjne, łączności, cyberbezpieczeństwa, zarządzania kryzysowego, dyspozytorskie, operacyjne i analityczne. Szacunek nie oznacza liczby obecnych kont w ASG-EUPOS, lecz potencjalną liczbę osób korzystających z danych, alertów lub informacji o jakości i wiarygodności usług PNT w ramach realizacji zadań bezpieczeństwa, obronności i reagowania kryzysowego.	10000
Organy regulacyjne i nadzorcze	Brak ustandaryzowanej wymiany informacji o jakości PNT, metryk SLA i feedów alertowych dla sektorów regulowanych oraz ograniczona baza do oceny ryzyka w obszarach telekomunikacji, lotnictwa, kolei, energetyki i dozoru technicznego. Zakłada się, że grupę odbiorców po stronie organów regulacyjnych i nadzorczych stanowi 5 instytucji: UKE, ULC, UTK, URE i UDT. Szacowana liczba przedstawicieli korzystających bezpośrednio z danych, metryk jakości PNT, raportów SLA i feedów alertowych wynosi ok. 80–160 osób, przy wartości roboczej ok. 120 osób. Są to przede wszystkim pracownicy komórek nadzoru, bezpieczeństwa, analiz ryzyka, kontroli, regulacji technicznych, ciągłości działania	120

Interesariusz	Zidentyfikowany problem	Szacowana wielkość grupy
	oraz obsługi incydentów w sektorach telekomunikacji, lotnictwa, kolei, energetyki i dozoru technicznego. Projekt odpowiada na potrzebę ustandaryzowanej wymiany informacji o jakości usług PNT oraz budowy wspólnej podstawy do oceny ryzyka zakłóceń GNSS w sektorach regulowanych.	
Biznes	Zakłócenia GNSS obniżają wiarygodność pomiarów, ciągłość wykorzystania ASG-EUPOS oraz bezpieczeństwo procesów zależnych od precyzyjnej pozycji i czasu. Brak bieżącej informacji o rejonach degradacji sygnału utrudnia zapewnienie jakości materiałów przekazywanych do zasobu geodezyjnego, realizację inwestycji budowlanych i drogowych, sterowanie maszynami, prowadzenie rolnictwa precyzyjnego, obsługę procesów logistycznych oraz wykonywanie zadań JST opartych na danych przestrzennych. W sektorze finansowym i gospodarce cyfrowej brak odpornej dystrybucji czasu oraz informacji o degradacji PNT zwiększa ryzyko zaburzeń synchronizacji transakcji, znakowania czasu, korelacji zdarzeń, rozliczeń i ciągłości usług cyfrowych. W sektorach specjalistycznych brak alternatywnych i odpornych metod PNT oraz wyspecjalizowanej informacji sektorowej ogranicza bezpieczeństwo zastosowań w gospodarce morskiej i offshore, nauce, B+R, metrologii oraz automatyzacji przemysłowej. Grupę odbiorców biznesowych można oszacować na co najmniej na 20 000 aktywnych użytkowników systemu ASG-EUPOS, zależnych od jakości sygnału GNSS, usług PNT oraz wiarygodnej dystrybucji czasu. Grupa ta obejmuje geodetów, wykonawców budowlanych i drogowych, operatorów maszyn, przedsiębiorstwa przemysłowe, rolnictwo precyzyjne, logistykę, banki, domy maklerskie, operatorów płatności, izby rozliczeniowe, dostawców usług cyfrowych, centra danych, operatorów chmury, podmioty gospodarki morskiej i offshore, jednostki naukowe, laboratoria metrologiczne oraz JST realizujące zadania zależne od danych przestrzennych.	20000
Operatorzy infrastruktury	Brak odpornych źródeł czasu i pozycji oraz brak szybkiej informacji o zakłóceniach PNT	5000

Interesariusz	Zidentyfikowany problem	Szacowana wielkość grupy
krytycznej i przedsiębiorstwa sieciowe	zwiększa ryzyko utraty ciągłości działania systemów energetycznych, telekomunikacyjnych, transportowych i centrów przetwarzania danych, Szacuje się, że grupę odbiorców po stronie operatorów infrastruktury krytycznej i przedsiębiorstw sieciowych stanowi ok. 500–1 200 organizacji, w tym operatorzy energetyczni, telekomunikacyjni, transportowi, centra przetwarzania danych, dostawcy usług chmurowych oraz inne przedsiębiorstwa utrzymujące systemy sieciowe i infrastrukturalne. Liczbę przedstawicieli korzystających bezpośrednio z danych o jakości PNT, alertów o zakłóceniach, informacji o degradacji sygnału GNSS oraz metryk ciągłości usług można oszacować na ok. 3 000–8 000 osób, przy wartości roboczej ok. 5 000 osób. Są to przede wszystkim pracownicy centrów nadzoru, dyspozytorni, zespołów utrzymania infrastruktury, bezpieczeństwa, cyberbezpieczeństwa, ciągłości działania, zarządzania kryzysowego i eksploatacji systemów OT/ICT. Projekt odpowiada na potrzebę zapewnienia odpornych źródeł czasu i pozycji oraz szybkiej informacji o zakłóceniach PNT, ograniczając ryzyko utraty ciągłości działania systemów energetycznych, telekomunikacyjnych, transportowych i centrów przetwarzania danych.	
Pracownicy MRiT	Brak narzędzi do ciągłego monitorowania jakości PNT/GNSS oraz możliwości przeciwdziałania skutkom zakłócania sygnału.	10

1.2. Opis stanu obecnego

Obecnie GUGiK realizuje zadania państwowej referencji przestrzennej z wykorzystaniem systemu ASG-EUPOS oraz sieci stacji referencyjnych podstawowej osnowy geodezyjnej klasy fundamentalnej. System działa od 2008 r., utrzymuje geodezyjne układy odniesienia w Polsce i stanowi bazę dla pomiarów GNSS. Jest powiązany z EUREF Permanent Network i zwiększa dokładność pomiarów w geodezji, budownictwie i drogownictwie.

W obecnych procesach przetwarzane są obserwacje GNSS ze stacji permanentnych, dane do realizacji układów odniesienia, dane usługowe ASG-EUPOS oraz informacje niezbędne do zapewnienia dokładności prac geodezyjnych. Poziom digitalizacji jest wysoki w części referencyjnej i usługowej, bo Beneficjent dysponuje dojrzałym systemem teleinformatycznym wykorzystywanym przez szerokie grono odbiorców.

Niewystarczający pozostaje poziom digitalizacji cyberodporności warstwy PNT/GNSS. Brakuje integracji danych z wielu źródeł, wspólnej wizualizacji sytuacji, wymiany alertów oraz technicznego środowiska współdziałania GUGiK z administracją, MON i operatorami infrastruktury krytycznej w zakresie monitorowania, detekcji i reagowania. Potrzebę projektu potwierdza skala jammingu i spoofingu GNSS w Europie Wschodniej i regionie Morza Bałtyckiego oraz 1 543 zgłoszenia zakłóceń GPS/GNSS odnotowane w 2025 r. przez ULC, w tym 1 172 nad terytorium RP.

Projekt odpowiada na te luki. Brak monitoringu jakości GNSS zostanie zaadresowany przez budowę stacji monitorujących i serwisów statusowych. Brak detekcji jammingu i spoofingu rozwiążą moduły analityczne, algorytmy wykrywania anomalii i klasyfikacja incydentów. Brak wspólnego obrazu sytuacyjnego usunie platforma integracyjna Polska Tarcza PNT – Moduł 1. Brak wymiany alertów zostanie rozwiązany przez API, feedy alertowe, raporty sektorowe i wielopoziomowy dostęp do informacji, a brak wsparcia ciągłości działania przez mechanizmy oceny wiarygodności PNT oraz analizy wpływu degradacji sygnału na usługi publiczne, gospodarcze i obronne.

2. EFEKTY PROJEKTU

2.1. Cele i korzyści wynikające z projektu

Cel - 1	Podniesienie poziomu odporności państwa poprzez wdrożenie wokół ASG-EUPOS zintegrowanych systemów monitorowania jakości GNSS i usług ASG-EUPOS, wykrywania i lokalizacji zakłóceń oraz ochrony warstwy fizycznej PNT.
Cel strategiczny	1. Strategia Cyfryzacji Państwa do 2035 r., obszar horyzontalny 1.3 Cyberbezpieczeństwo, cel/kierunek 1.3.3 „Centralne pozyskiwanie i rozwój rozwiązań cyberbezpieczeństwa”. W ramach tego celu Strategia wprost wskazuje działanie „Polska Tarcza PNT”, obejmujące istotne podniesienie poziomu krajowej zdolności wczesnego wykrywania i obsługi incydentów PNT poprzez wdrożenie jednej panoramy PNT dla państwa, natychmiastowe alarmowanie i triage incydentów oraz utrzymanie ciągłości wyznaczania pozycji i czasu w modelu usługowym nawet przy aktywnych zakłóceniach GNSS. 2. Strategia Bezpieczeństwa Narodowego RP 2020 Cel: Odporność państwa i obrona powszechna – podniesienie odporności państwa na zagrożenia, w tym zagrożenia o charakterze hybrydowym; budowanie zdolności do odtwarzania niezbędnych zasobów. 3. Strategia Cyberbezpieczeństwa Rzeczypospolitej Polskiej, przyjęta przez Radę Ministrów 10 marca 2026 r. Cel szczegółowy 1. Rozwój krajowego systemu cyberbezpieczeństwa Cel szczegółowy 3. Podniesienie poziomu odporności systemów informacyjnych w sferze publicznej (w tym militarnej) oraz prywatnej . 4. Krajowy Plan Odbudowy i Zwiększania Odporności – inwestycja C3.1.1 Cyberbezpieczeństwo 5. Narodowy Program Ochrony Infrastruktury Krytycznej Priorytet 1. pogłębienie współpracy między uczestnikami Programu w obszarze ochrony IK, 6. Program Otwierania Danych na lata 2021–2027 Cel 2: poprawa interoperacyjności i jakości danych; działania dotyczące podnoszenia jakości danych oraz automatycznego udostępniania i aktualizowania zasobów danych.

	7. Krajowy Program Kosmiczny na lata 2021–2026 Cel 2. zwiększenie wykorzystania danych satelitarnych przez administrację, naukę, przemysł i społeczeństwo; Cel 3. wykorzystanie technologii satelitarnych do zwiększenia bezpieczeństwa i obronności kraju. 8. Strategia Zrównoważonego Rozwoju Transportu do 2030 roku Cel główny: zwiększenie dostępności transportowej kraju oraz poprawa bezpieczeństwa uczestników ruchu i efektywności sektora transportowego 9. Krajowy Plan Bezpieczeństwa 2026–2028
Korzyść:	Projekt przyniesie kluczową korzyść w postaci utworzenia jednej panoramy PNT dla państwa, czyli wspólnego, zintegrowanego obrazu sytuacji w zakresie jakości sygnałów GNSS, działania usług ASG-EUPOS, występowania zakłóceń oraz wpływu degradacji sygnału na usługi publiczne, gospodarcze, obronne i infrastrukturalne. Obecnie informacje o stanie usług PNT są rozproszone, sektorowe i nie tworzą jednolitego obrazu sytuacyjnego. Projekt pozwoli na przejście od reakcji fragmentarycznej do zarządzania opartego na wspólnych danych, metrykach jakości, mapach degradacji, alertach i analizie wpływu incydentów. Istotną korzyścią będzie natychmiastowe alarmowanie i triage incydentów PNT. System umożliwi szybkie wykrywanie, klasyfikowanie i priorytetyzowanie zdarzeń, takich jak jamming, spoofing, degradacja jakości GNSS, utrata dostępności usług lub anomalie w pracy stacji referencyjnych. Dzięki temu administracja publiczna, MON, służby, regulatorzy, operatorzy infrastruktury krytycznej i wybrane sektory gospodarki uzyskają możliwość szybkiego rozpoznania, czy dane zdarzenie ma charakter lokalny, sektorowy, transgraniczny, przypadkowy czy potencjalnie wrogi. Pozwoli to skrócić czas reakcji, ograniczyć skutki zakłóceń oraz usprawnić koordynację działań między instytucjami. Projekt zwiększy również zdolność państwa do utrzymania ciągłości wyznaczania pozycji i czasu w modelu usługowym, nawet przy aktywnych zakłóceniach GNSS. Oznacza to, że użytkownicy nie będą otrzymywać wyłącznie informacji o awarii lub degradacji, lecz dostęp do uporządkowanych usług wspierających ocenę wiarygodności pozycji i czasu, identyfikację obszarów ryzyka, wybór bezpieczniejszych źródeł danych oraz kontynuację działania procesów zależnych od PNT. Jest to szczególnie ważne dla geodezji, budownictwa, transportu, energetyki, telekomunikacji, finansów, lotnictwa, służb ratunkowych i infrastruktury krytycznej. W efekcie projekt podniesie odporność państwa poprzez zapewnienie wspólnego obrazu sytuacyjnego, szybkiego ostrzegania, lepszego zarządzania incydentami oraz ciągłości usług zależnych od precyzyjnej pozycji i czasu. Korzyści będą miały charakter systemowy: zwiększą bezpieczeństwo danych przestrzennych, ograniczą ryzyko błędów pomiarowych i operacyjnych, poprawią współdziałanie instytucji oraz wzmocnią zdolność administracji i sektorów regulowanych do funkcjonowania w warunkach zakłóceń hybrydowych.
KPI:	KPI 1 – Instytucje publiczne otrzymujące wsparcie na opracowywanie usług, produktów i procesów cyfrowych. KPI 2– Liczba podmiotów wspartych w zakresie cyberbezpieczeństwa. KPI 3– Liczba podmiotów wspartych w zakresie rozwoju usług, produktów i procesów cyfrowych. KPI 4 – Liczba pracowników IT podmiotów wykonujących zadania publiczne

	objętych wsparciem szkoleniowym. KPI 5– Liczba pracowników podmiotów wykonujących zadania publiczne nie będących pracownikami IT, objętych wsparciem szkoleniowym. KPI 6 – Liczba systemów, modułów lub komponentów służących zwiększeniu poziomu bezpieczeństwa informacji. KPI 7 - Użytkownicy nowych i zmodernizowanych publicznych usług, produktów i procesów cyfrowych KPI 8 - Średni czas wykrywania incydentów PNT
Wartość aktualna i docelowa KPI:	KPI 1- 0 KPI 2- 0 KPI 3- 0 KPI 4- 0 KPI 5- 0 KPI 6- 0 KPI 7- 0 KPI 8- nie jest monitorowany KPI 1- 1 KPI 2- 2 KPI 3- 1 KPI 4- 20 KPI 5- 200 KPI 6- 10 KPI 7- 10000 KPI 8- 20
Metoda pomiaru KPI	Pomiar wskaźników produktu będzie prowadzony narastająco w trakcie realizacji projektu, w powiązaniu z odbiorami etapowymi, dokumentacją projektową, protokołami odbioru oraz dokumentacją szkoleniową. Dla każdego KPI określa się następujący sposób pomiaru, źródło danych, częstotliwość pomiaru oraz termin pomiaru wartości docelowej: KPI 1 – Instytucje publiczne otrzymujące wsparcie na opracowywanie usług, produktów i procesów cyfrowych Sposób pomiaru: liczba instytucji publicznych objętych wsparciem w ramach projektu, potwierdzona udziałem w realizacji lub odbiorze produktu cyfrowego. Źródło danych: umowa o dofinansowanie, dokumentacja projektowa, protokoły odbioru produktów, dokumenty potwierdzające udział Beneficjenta w projekcie. Częstotliwość pomiaru: po zakończeniu kluczowych etapów realizacji projektu oraz przy odbiorze końcowym. Termin pomiaru wartości docelowej: do dnia zakończenia rzeczowej realizacji projektu, tj. do 31.10.2028 r. KPI 2 – Liczba podmiotów wspartych w zakresie cyberbezpieczeństwa Sposób pomiaru: liczba podmiotów, które uzyskały wsparcie w zakresie cyberbezpieczeństwa poprzez udział w projekcie, dostęp do produktów projektu, komponentów bezpieczeństwa, procedur, alertów, szkoleń lub rozwiązań wzmacniających odporność PNT/GNSS. Źródło danych: umowa o dofinansowanie, porozumienia lub umowy partnerskie, protokoły odbioru, dokumentacja wdrożeniowa, rejestry udostępnienia produktów projektu. Częstotliwość pomiaru: kwartalnie w trakcie realizacji projektu oraz przy odbiorze końcowym. Termin pomiaru wartości docelowej: do dnia zakończenia rzeczowej realizacji projektu, tj. do 31.10.2028 r.

KPI 3 – Liczba podmiotów wspartych w zakresie rozwoju usług, produktów i procesów cyfrowych
 Sposób pomiaru: liczba podmiotów, które uzyskały wsparcie poprzez wdrożenie lub udostępnienie usług, produktów lub procesów cyfrowych powstałych w projekcie.
 Źródło danych: umowa o dofinansowanie, dokumentacja projektowa, protokoły odbioru, dokumentacja wdrożeniowa, rejestry uruchomionych usług lub produktów cyfrowych.
 Częstotliwość pomiaru: po zakończeniu etapów obejmujących wytworzenie i wdrożenie produktów cyfrowych oraz przy odbiorze końcowym.
 Termin pomiaru wartości docelowej: do dnia zakończenia rzeczowej realizacji projektu, tj. do 31.10.2028 r.

KPI 4 – Liczba pracowników IT podmiotów wykonujących zadania publiczne objętych wsparciem szkoleniowym
 Sposób pomiaru: liczba pracowników IT, którzy ukończyli szkolenie, ćwiczenie lub instruktaż związany z obsługą, utrzymaniem, bezpieczeństwem lub rozwojem produktów projektu.
 Źródło danych: listy obecności, rejestry uczestników szkoleń, raporty z systemu LMS/LRS, certyfikaty ukończenia, testy wiedzy, protokoły realizacji szkoleń.
 Częstotliwość pomiaru: po każdym szkoleniu lub cyklu szkoleniowym oraz zbiorczo kwartalnie.
 Termin pomiaru wartości docelowej: najpóźniej do zakończenia etapu szkoleń i odbioru końcowego projektu, tj. do 31.10.2028 r.

KPI 5 – Liczba pracowników podmiotów wykonujących zadania publiczne nie będących pracownikami IT, objętych wsparciem szkoleniowym
 Sposób pomiaru: liczba pracowników nie-IT, w szczególności operatorów, dyspozytorów, analityków, pracowników komórek operacyjnych, zarządzania kryzysowego, administracji i innych użytkowników instytucjonalnych, którzy ukończyli szkolenie dotyczące korzystania z produktów projektu, interpretacji alertów, raportów i informacji o jakości PNT/GNSS.
 Źródło danych: listy obecności, rejestry uczestników szkoleń, raporty LMS/LRS, ankiety poszkoleniowe, certyfikaty, protokoły realizacji szkoleń.
 Częstotliwość pomiaru: po każdym szkoleniu lub cyklu szkoleniowym oraz zbiorczo kwartalnie.
 Termin pomiaru wartości docelowej: najpóźniej do zakończenia etapu szkoleń i odbioru końcowego projektu, tj. do 31.10.2028 r.

KPI 6 – Liczba systemów, modułów lub komponentów służących zwiększeniu poziomu bezpieczeństwa informacji
 Sposób pomiaru: liczba odebranych i uruchomionych systemów, modułów lub komponentów służących zwiększeniu poziomu bezpieczeństwa informacji, w szczególności w zakresie monitorowania, detekcji, analizy, alertowania, raportowania, integracji danych, kontroli dostępu, rejestrowania zdarzeń i ochrony usług PNT/GNSS.
 Źródło danych: protokoły odbioru, dokumentacja techniczna, dokumentacja powykonawcza, raporty z testów bezpieczeństwa i wydajności, potwierdzenia uruchomienia produkcyjnego.
 Częstotliwość pomiaru: po odbiorze każdego systemu, modułu lub komponentu oraz zbiorczo przy odbiorach etapowych i końcowym.
 Termin pomiaru wartości docelowej: do dnia odbioru końcowego i uruchomienia systemu Polska Tarcza PNT – Moduł 1, tj. do 31.10.2028 r.

KPI 7 - Użytkownicy nowych i zmodernizowanych publicznych usług, produktów i procesów cyfrowych

	Sposób pomiaru: pomiar na podstawie liczby unikalnych kont lub identyfikatorów korzystających z paneli Status GNSS/ASG-EUPOS, portalu ISAC PNT, dashboardów NOC, feedów publicznych, usług ASG-EUPOS. Liczba aktywnych kont lub kluczy API z sektora publicznego raportowana półrocznie. Źródło: IdP/IdM, gateway API, logi SIEM, baza danych ASG-EUPOS. Termin pomiaru wartości docelowej: 12 miesięcy od dnia odbioru końcowego i uruchomienia systemu Polska Tarcza PNT – Moduł 1, tj. do 31.10.2029 r. KPI 8 - Średni czas wykrywania incydentów PNT Sposób pomiaru: Średni czas wykrycia incyduentu PNT, liczony jako czas od zaistnienia incyduentu do powiadomienia o zaistnieniu incyduentu; źródło – logi systemowe oraz raporty z pomiarów terenowych wykonanych w terminie 12 miesięcy od dnia odbioru końcowego i uruchomienia systemu Polska Tarcza PNT – Moduł 1, tj. do 31.10.2029 r.
--	---

2.2. Udostępnione e-usługi

Lp.	Nazwa e-usługi	Typ	Zakres oddziaływania	Poziom dojrzałości e-usługi

2.3. Udostępnione informacje sektora publicznego i zdigitalizowane zasoby

Nie dotyczy

2.4. Produkty końcowe projektu

Nazwa produktu	Planowana data wdrożenia
Raport z inicjalnego testu prywatności	12-2026
Dokumentacja analityczna	01-2027
Projekt architektury Systemu	01-2027
Projekty wykonawcze teletechniczne	04-2027
Infrastruktura teletechniczna stacji referencyjnych i monitorujących	10-2027
Dokumentacja powykonawcza	02-2028
Materiały szkoleniowe	06-2028
Raport z testów wydajności	09-2028
Raport z testów bezpieczeństwa	09-2028
System teleinformatyczny Polska Tarcza PNT - Moduł 1	10-2028
API systemu teleinformatycznego Polska Tarcza PNT - Moduł 1	10-2028

3. KAMIENIE MIŁOWE

Kamienie milowe	Planowany termin osiągnięcia
Przeprowadzone testy prywatności	2026-12-31
Zatwierdzony projekt architektury Systemu	2027-01-31
Rozstrzygnięte postępowanie przetargowe na dostawę urządzeń oraz opracowanie komponentów systemu	2027-05-31
Uruchomione stacje referencyjne i monitorujące	2027-10-30
Rozpoczęte procesy testowania oprogramowania	2028-01-03
Rozpoczęty pilotaż operacyjny	2028-03-01
Uzyskany pozytywny wynik testów wydajności i bezpieczeństwa	2028-08-30
Zakończone szkolenia	2028-10-20
Uruchomiony system teleinformatyczny Polska Tarcza PNT - Moduł 1	2028-10-30

4. KOSZTY

4.1. Koszty ogólne projektu wraz ze sposobem finansowania

Całkowity koszt projektu (netto oraz brutto), w tym	Netto 22 895 622,44 zł Brutto 27 000 000,00 zł	
Procent dofinansowania ze środków UE (brutto)	89,93%	
Procent środków z budżetu państwa (brutto)	10,07%	
Podział całkowitego kosztu projektu na poszczególne lata (netto oraz brutto)	2026	Netto 317 168,80 zł Brutto 317 168,80 zł
	2027	Netto 14 994 315,12 zł Brutto 17 831 209,48 zł
	2028	Netto 7 584 138,52 zł Brutto 8 851 621,72 zł

4.2. Wykaz poszczególnych pozycji kosztowych

Nazwa pozycji kosztowej		Przewidywany koszt brutto	Uzasadnienie pozycji kosztowej (przeznaczenie)
Oprogramowanie	Zakup	16 176 848,46 zł	Pozycja kosztowa jest niezbędna

Nazwa pozycji kosztowej		Przewidywany koszt brutto	Uzasadnienie pozycji kosztowej (przeznaczenie)
	oprogramowania dedykowanego oraz wytworzenie platformy integracyjnej Polska Tarcza PNT Moduł 1		do budowy centralnego, wysokodostępnego środowiska integracji, akwizycji, przetwarzania i wizualizacji danych PNT/GNSS, stanowiącego podstawę „jednej panoramy PNT dla państwa”. Pozycja zawiera koszt zakupu dedykowanych rozwiązań aplikacyjnych w wysokości 13 139 497,46 zł. oraz koszt pracy zespołu programistów i zespołu bezpośrednio zaangażowanego w wytwarzanie oprogramowania w wysokości 3 037 351,00 zł.
Infrastruktura	Sprzęt pomiarowy i teleinformatyczny wraz z montażem oraz instalacją i konfiguracją. Zasoby infrastruktury obliczeniowej (CPU/GPU/NPU, RAM, storage, stos sieciowy, routing, load balancing)	8 290 000,00 zł	Pozycje kosztowe dotyczące sprzętu są niezbędne do budowy rozproszonej, odpornej warstwy pomiarowej i brzegowej projektu, obejmującej odbiorniki GNSS, anteny, sensory, urządzenia czasu, elementy detekcji zakłóceń, osprzęt, montaż, konfigurację oraz utrzymanie lokalizacji. Sprzęt ten zapewni pozyskiwanie wiarygodnych danych źródłowych w terenie, lokalne przetwarzanie sygnałów, weryfikację jakości PNT/GNSS, wykrywanie anomalii oraz zasilanie centralnej platformy integracyjnej danymi w czasie zbliżonym do rzeczywistego. Bez zakupu i instalacji komponentów sprzętowych niemożliwe byłoby osiągnięcie zakładanych zdolności monitorowania, alarmowania, lokalizacji zakłóceń oraz utrzymania ciągłości usług PNT w warunkach degradacji lub aktywnych zakłóceń GNSS. Zasoby infrastruktury obliczeniowej służyć będą do obsługi danych z ASG-EUPOS i systemów dziedzinowych, trenowania oraz uruchamiania modeli AI, a także generowania alertów i raportów w czasie zbliżonym do rzeczywistego. Bez tego komponentu niemożliwe

Nazwa pozycji kosztowej		Przewidywany koszt brutto	Uzasadnienie pozycji kosztowej (przeznaczenie)
			byłoby spójne zarządzanie usługami, szybka kwalifikacja i priorytetyzacja incydentów, interoperacyjna wymiana informacji i utrzymanie ciągłości działania usług PNT przy zakłóceniach GNSS.
Koszty UX i grafiki			
Bezpieczeństwo	Testy bezpieczeństwa rozwiązania	50 000,00 zł	Testy bezpieczeństwa zlecone podmiotowi zewnętrznemu.
Wydajność rozwiązań			
Szkolenia	Szkolenia personelu	465 000,00 zł	Szkolenia są niezbędne do zapewnienia prawidłowego wykorzystania wdrażanych systemów monitorowania, detekcji, alarmowania i analizy jakości PNT/GNSS przez administratorów, operatorów oraz użytkowników instytucjonalnych. Obejmą obsługę platformy, interpretację alertów i raportów, procedury reagowania na incydenty, zarządzanie dostępem, wymianę informacji oraz utrzymanie ciągłości usług w sytuacji zakłóceń GNSS. Bez komponentu szkoleniowego pełne wykorzystanie funkcjonalności projektu, prawidłowa reakcja na incydenty oraz trwałość efektów wdrożenia byłyby istotnie ograniczone. : Materiały szkoleniowe, instrukcje oraz pozostałe materiały edukacyjne opracowane w ramach projektu będą spełniały obowiązujące wymagania dostępności cyfrowej, w tym wymagania WCAG 2.2 na poziomie AA, w zakresie mającym zastosowanie do danego rodzaju materiału.
Działania informacyjno-promocyjne	Tablica informacyjna	5000,00 zł	Wykonanie tablicy informacyjnej zgodnie z zasadami promocji
Koszty zarządzania i wsparcia (w tym	Zespół zarządzający i	2 013 151,54 zł	Koszty zarządzania i wsparcia są niezbędne do zapewnienia

Nazwa pozycji kosztowej		Przewidywany koszt brutto	Uzasadnienie pozycji kosztowej (przeznaczenie)
wynagrodzenia personelu wspomagającego)	administracyjny GUGiK		koordynacji projektu, kontroli harmonogramu, budżetu, ryzyk, jakości produktów oraz zgodności realizacji z wymaganiami programu. Obejmują wynagrodzenia personelu wspomagającego, który będzie nie tylko obsługiwał projekt administracyjnie i rozliczeniowo, lecz także współtworzył rozwiązanie poprzez udział w analizie wymagań, uzgodnieniach z partnerami, testach, odbiorach, przygotowaniu procedur, dokumentacji użytkowej i organizacji wdrożenia. Bez tego zaangażowania skuteczna realizacja złożonego, wielopodmiotowego systemu byłaby obciążona ryzykiem opóźnień, błędów formalnych, niespójności wymagań oraz ograniczonej użyteczności końcowego rozwiązania.

4.3. Koszty ogólne utrzymania wraz ze sposobem finansowania (okres 5 lat)

Całkowity koszt utrzymania trwałości projektu (brutto)	1 926 038,00 zł		Źródło finansowania
Podział całkowitego kosztu utrzymania trwałości projektu na poszczególne lata (netto oraz brutto)	2028	68 412,00 zł (brutto) (55 619,51 zł netto)	krajowe środki publiczne - budżet państwa
	2029	430 991,00 zł (brutto) (350 399,19 zł netto)	krajowe środki publiczne - budżet państwa
	2030	452 541,00 zł (brutto) (367 919,51 zł netto)	krajowe środki publiczne - budżet państwa
	2031	475 168,00 zł (brutto) (386 315,44 zł netto)	krajowe środki publiczne - budżet państwa
	2032	498 926,00 zł (brutto)	krajowe środki

		(405 630,89 zł netto)	publiczne - budżet państwa
--	--	-----------------------	----------------------------

4.4. Planowane koszty ogólne realizacji (w przypadku projektu współfinansowanego – wkład krajowy z budżetu państwa) oraz koszty utrzymania projektu:

- zostaną pokryte w ramach budżetów odpowiednich dysponentów części budżetowych bez konieczności występowania o dodatkowe środki z budżetu państwa
- ~~- będą powodować konieczność przyznania dodatkowych kwot~~

5. GŁÓWNE RYZYKA

5.1. Ryzyka wpływające na realizację projektu

Nazwa ryzyka	Siła oddziaływania	Prawdopodobieństwo wystąpienia ryzyka	Sposób zarządzania ryzykiem
Niepowodzenia wyboru wykonawców w planowanych terminach w ramach postępowań przetargowych	Duża	Średnie	Stały monitoring etapu realizacji, zabezpieczenie w zespole wsparcia w zakresie sprawnego przygotowania i prowadzenia postępowań przetargowych tak, aby ograniczyć ryzyko opóźnień.
Niedoszacowanie kosztów projektu.	Duża	Średnie	Stały monitoring realizacji projektu i poszczególnych etapów, elastyczne reagowanie na warunki rynkowe.
Odejście z pracy / zaangażowanie do innych inicjatyw osób kluczowych dla realizacji projektu. Rotacja na stanowiskach osób zaangażowanych w realizację działań projektowych.	Średnia	Średnie	Zapewnienie odpowiedniej komunikacji w projekcie. System motywacyjny dla zespołu projektowego. Zapewnienie stabilnego zespołu projektowego w całym okresie realizacji projektu.
Ryzyko braku lub opóźnienia integracji z systemami zewnętrznymi: e-CzasPL,	Średnia	Niskie	Analiza udostępnianych mechanizmów API.

Nazwa ryzyka	Siła oddziaływania	Prawdopodobieństwo wystąpienia ryzyka	Sposób zarządzania ryzykiem
Geoportal, IMGW			
Ryzyko powstania ograniczeń w udostępnianiu danych operacyjnych lub wrażliwych, szczególnie danych o źródłach zakłóceń i incydentach	Duża	Średnie	Wdrożenie modelu wielopoziomowego dostępu do informacji, obejmującego klasyfikację danych według poziomu wrażliwości, kontrolę dostępu opartą na rolach, anonimizację lub generalizację danych lokalizacyjnych oraz rozdzielenie warstwy publicznej, sektorowej i operacyjnej systemu. Dane o incydentach PNT/GNSS będą udostępniane w zakresie adekwatnym do potrzeb odbiorców: publicznie w formie statusów, alertów i informacji zagregowanych, a szczegółowo wyłącznie uprawnionym instytucjom. Dodatkowo zostaną wdrożone procedury zatwierdzania komunikatów, rejestracji dostępu, szyfrowania transmisji oraz uzgadniania zasad wymiany informacji z partnerami, co pozwoli pogodzić potrzebę ostrzegania użytkowników z wymogami bezpieczeństwa państwa i ochrony danych operacyjnych.
Ryzyko niezachowania interoperacyjności i jakości danych: różne formaty, częstotliwości, opóźnienia, poziomy ufności, metadane i klasyfikacja zdarzeń.	Średnia	Niskie	Ryzyko to będzie ograniczane poprzez opracowanie wspólnego modelu danych i słowników pojęć, zdefiniowanie minimalnego zakresu metadanych, ujednolicenie klasyfikacji zdarzeń, określenie standardów API i formatów wymiany, a także wdrożenie mechanizmów walidacji, normalizacji, deduplikacji i kontroli jakości danych
Ryzyko opóźnień dostaw wyspecjalizowanego sprzętu (Np. GNSS/RF/ SDR/czasu)	Duża	Średnie	Ryzyko będzie ograniczane przez wczesne rozpoczęcie postępowań zakupowych, analizę rynku przed zamówieniem, dopuszczenie rozwiązań równoważnych, unikanie nadmiernie zamkniętych specyfikacji, podział dostaw na pakiety, utrzymywanie rezerw czasowych oraz wymaganie dostępności serwisu, dokumentacji technicznej i wsparcia producenta
Przekroczenie harmonogramu realizacji projektu	Duża	Niskie	Ryzyko będzie zarządzane poprzez bieżące monitorowanie harmonogramu, identyfikację opóźnień na poziomie

Nazwa ryzyka	Siła oddziaływania	Prawdopodobieństwo wystąpienia ryzyka	Sposób zarządzania ryzykiem
			kamieni milowych i zadań krytycznych oraz wdrażanie działań korygujących, takich jak realokacja zasobów, priorytetyzacja prac, zwiększenie nadzoru nad wykonawcami i uruchamianie rezerw czasowych.
Nieosiągnięcie wskaźników produktu/celu oraz celu projektu	Średnia	Niskie	Ryzyko będzie ograniczane poprzez bieżący monitoring realizacji wskaźników produktu i celu na poziomie harmonogramu, odbiorów etapowych, rejestru ryzyk oraz cyklicznych raportów postępu, z przypisaniem odpowiedzialności za każdy wskaźnik do właścicieli merytorycznych i technicznych. W przypadku identyfikacji odchyłeń wdrażane będą działania korygujące, w szczególności aktualizacja planu prac, zwiększenie nadzoru nad wykonawcami, priorytetyzacja produktów kluczowych dla osiągnięcia wskaźników oraz uruchomienie działań naprawczych przed odbiorem końcowym.

5.2. Ryzyka wpływające na utrzymanie efektów

Nazwa ryzyka	Siła oddziaływania	Prawdopodobieństwo wystąpienia ryzyka	Sposób zarządzania ryzykiem
Nieprzyznanie środków z budżetu państwa na utrzymanie produktów projektu	Duża	Średnie	Zabezpieczenie finansowania kosztów trwałości w budżecie państwa, coroczne planowanie potrzeb utrzymaniowych oraz przypisanie odpowiedzialności za eksploatację i utrzymanie produktów do GUGiK i IŁ-PIB zgodnie z zakresem trwałości projektu. Monitoring kosztów utrzymania i aktualizacja planów rzeczowo-finansowych w okresie trwałości.
Szybkie zestarzenie się technologii oraz nowe metody ataków	Duża	Średnie	Architektura w modelu rozwojowym o ciągłej aktualizacji. Planowanie aktualizacji, badanie trendów, monitorowanie sytuacji przez zespół devops.

Nazwa ryzyka	Siła oddziaływania	Prawdopodobieństwo wystąpienia ryzyka	Sposób zarządzania ryzykiem
cybernetycznych na systemy GPS/GNSS/PNT			
Odejście kluczowych pracowników	Duża	Średnie	Dokumentacja wiedzy, plan sukcesji, prowadzenie ogólnego i specjalistycznego szkolenia wewnętrznego zespołu "gitdevsecops
Brak aktualizacji dokumentacji systemowej	Średnia	Średnie	Regularne przeglądy dokumentacji, bieżące dokumentowanie wprowadzanych zmian w systemie
Wzrost kosztów utrzymania	Duża	Średnie	Budżetowanie na utrzymanie, optymalizacja i monitoring wydatków. Sporządzanie kwartalnych notatek i meldunków dotyczących ewentualnego zwiększenia finansowania projektu z środków budżetu państwa w celu zabezpieczenia prawidłowego rozwoju projektu.
Brak możliwości zatrudnienia osób o odpowiednich kompetencjach, Brak wystarczających środków na utrzymanie projektu	Duża	Niskie	Zgłaszanie z wyprzedzeniem do planów budżetów resortowych (MON, MC, MFiG, MRiT) oraz dysponentów potrzeb finansowych na realizację i utrzymanie projektu. Sporządzanie kwartalnych notatek i meldunków dotyczących ewentualnego zwiększenia finansowania projektu z środków budżetu państwa w celu zabezpieczenia prawidłowego rozwoju projektu.
Ryzyko braku stabilnego zespołu utrzymaniowego po zakończeniu projektu oraz utraty kompetencji domenowych PNT/GNSS/RF/IT.	Duża	Niskie	Ryzyko będzie ograniczane przez zaplanowanie modelu utrzymania już na etapie projektu, wskazanie właścicieli usług i ról operacyjnych, przygotowanie procedur eksploatacyjnych, dokumentacji technicznej, instrukcji reagowania na incydenty oraz planu przekazania wiedzy. Dodatkowo przewiduje się szkolenia administratorów i operatorów, udział personelu utrzymaniowego w testach i odbiorach, budowę bazy wiedzy, zapewnienie wsparcia producentów i wykonawców w okresie powdrożeniowym oraz określenie ścieżek rozwoju kompetencji dla zespołów GUGiK i IŁ
Ryzyko wzrostu	Średnia	Średnie	Ryzyko będzie ograniczane przez

Nazwa ryzyka	Siła oddziaływania	Prawdopodobieństwo wystąpienia ryzyka	Sposób zarządzania ryzykiem
kosztów chmury, licencji, cyberbezpieczeństwa, serwisu sprzętu i integracji API			przygotowanie modelu TCO dla fazy wdrożenia i utrzymania, wprowadzenie limitów zużycia zasobów chmurowych, monitoringu kosztów, mechanizmów skalowania, polityk retencji danych, optymalizacji liczby zapytań API oraz okresowej weryfikacji wykorzystania licencji. Dodatkowo przewiduje się stosowanie konkurencyjnych i przenaszalnych rozwiązań, negocjowanie warunków serwisu i wsparcia na kilka lat, zapewnienie rezerw budżetowych oraz regularny przegląd architektury pod kątem kosztów, bezpieczeństwa i efektywności utrzymania
Ryzyko dezaktualizacji modeli detekcji i klasyfikacji zakłóceń oraz konieczności okresowego strojenia algorytmów AI/ML	Duża	Niskie	Ryzyko będzie ograniczane przez zaplanowanie cyklicznej walidacji skuteczności modeli, okresowe dostrajanie progów detekcji, aktualizację zbiorów uczących, monitorowanie jakości klasyfikacji, testowanie modeli na danych historycznych i bieżących oraz utrzymywanie mechanizmów nadzoru eksperckiego nad wynikami automatycznej analizy. Ponadto przewiduje się wersjonowanie modeli, rejestrowanie decyzji algorytmicznych, możliwość ręcznej korekty klasyfikacji incydentów, procedury ponownego trenowania.

6. OTOCZENIE PRAWNE

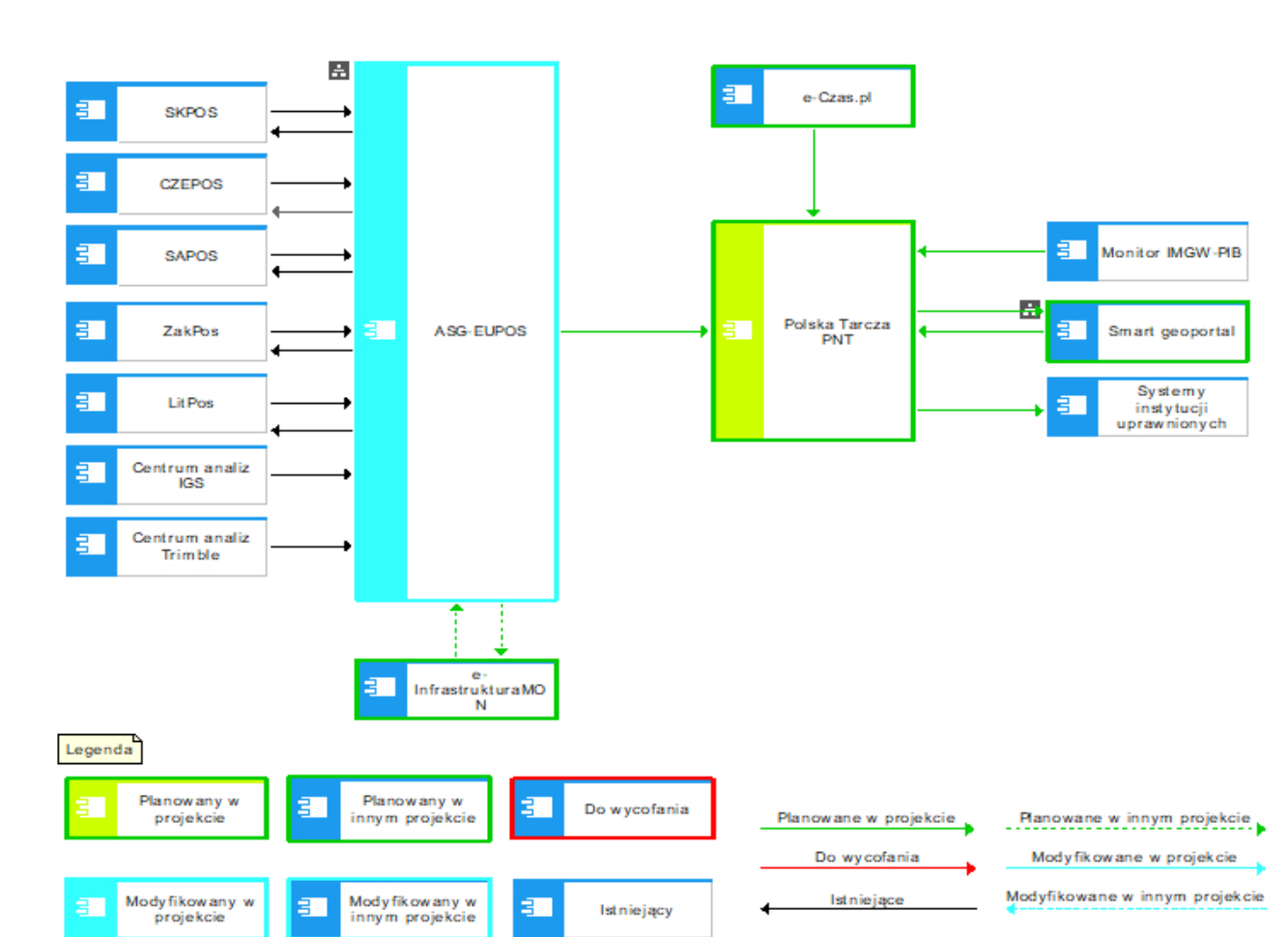
Lp.	Tytuł aktu prawnego	Czy wymaga zmian	Opis zmian (jeśli dotyczy)	Etap prac legislacyjnych (jeśli dotyczy)
1	Ustawa z 17 maja 1989 r. – Prawo geodezyjne i kartograficzne	TAK /NIE		
2	Ustawa z 4 marca 2010 r. o infrastrukturze informacji przestrzennej	TAK /NIE		
3	Rozporządzenie MAC z 16 stycznia 2015 r. w sprawie prac geodezyjnych i kartograficznych	TAK /NIE		

Lp.	Tytuł aktu prawnego	Czy wymaga zmian	Opis zmian (jeśli dotyczy)	Etap prac legislacyjnych (jeśli dotyczy)
	mających znaczenie dla obronności i bezpieczeństwa państwa oraz współdziałania GGK z MON			
4	Ustawa z 5 lipca 2018 r. o Krajowym Systemie Cyberbezpieczeństwa	TAK/NIE		
5	Ustawa z 11 marca 2022 r. o obronie Ojczyzny	TAK/NIE		
6	Rozporządzenie Rady Ministrów z 15 października 2012 r. w sprawie państwowego systemu odniesień przestrzennych	TAK/NIE		
7	Rozporządzenie MRPiT z 6 lipca 2021 r. w sprawie osnów geodezyjnych, grawimetrycznych i magnetycznych	TAK/NIE		
8	Rozporządzenie MRPiT z 7 lipca 2021 r. w sprawie standardów technicznych wykonywania geodezyjnych pomiarów sytuacyjnych i wysokościowych oraz opracowywania i przekazywania wyników tych pomiarów do PZGiK	TAK/NIE		
9	Ustawa o informatyzacji działalności podmiotów realizujących zadania publiczne	TAK/NIE		
10	Rozporządzenie Rady Ministrów w sprawie Krajowych Ram Interoperacyjności, minimalnych wymagań dla rejestrów publicznych i wymiany informacji w postaci elektronicznej oraz minimalnych wymagań dla systemów teleinformatycznych	TAK/NIE		
11	Ustawa o krajowym systemie cyberbezpieczeństwa	TAK/NIE		
12	Ustawa o ochronie baz danych	TAK/NIE		
13	Ustawa o otwartych danych i ponownym wykorzystywaniu informacji sektora publicznego	TAK/NIE		
14	Ustawa o dostępności cyfrowej stron internetowych i aplikacji mobilnych podmiotów publicznych	TAK/NIE		
15	Ustawa o wspieraniu rozwoju usług i sieci telekomunikacyjnych	TAK/NIE		
16	Ustawa o doręczeniach elektronicznych	TAK/NIE		
17	Ustawa o usługach zaufania oraz identyfikacji elektronicznej	TAK/NIE		
18	Ustawa o ochronie informacji niejawnych	TAK/NIE		
19	Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016	TAK/NIE		

Lp.	Tytuł aktu prawnego	Czy wymaga zmian	Opis zmian (jeśli dotyczy)	Etap prac legislacyjnych (jeśli dotyczy)
	r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych),			
20	Rozporządzenie Prezesa Rady Ministrów w sprawie podstawowych wymagań bezpieczeństwa teleinformatycznego	TAK /NIE		
21	Rozporządzenie Prezesa Rady Ministrów w sprawie sporządzania pism w formie dokumentów elektronicznych, doręczania dokumentów elektronicznych oraz udostępniania formularzy, wzorów i kopii dokumentów elektronicznych	TAK /NIE		
22	Rozporządzenie Ministra Cyfryzacji w sprawie profilu zaufanego i podpisu zaufanego,	TAK /NIE		
23	Rozporządzenie Ministra Cyfryzacji w sprawie szczegółowych warunków organizacyjnych i technicznych, które powinien spełniać system teleinformatyczny służący do uwierzytelniania użytkowników	TAK /NIE		
24	Ustawa o narodowym zasobie archiwalnym i archiwach	TAK /NIE		

7. ARCHITEKTURA

7.1. Widok kooperacji aplikacji



Lista systemów wykorzystywanych w projekcie

Lp.	Nazwa systemu	Gestor systemu	Opis systemu	Status	Krótki opis ewentualnej zmiany
1	ASG-EUPOS	Główny Urząd Geodezji i Kartografii	ASG-EUPOS – Aktywna Sieć Geodezyjna EUPOS to system wspierający przenoszenie i utrzymywanie na obszarze Polski geodezyjnych układów odniesienia oraz realizację precyzyjnych pomiarów satelitarnych GNSS. Jego celem jest zapewnienie jednolitej, wiarygodnej i dokładnej państwowej infrastruktury odniesienia przestrzennego, zgodnej z europejskim systemem	Istniejący	Rozszerzenie o monitoring jakości i statusu oraz integrację z nowymi komponentami projektu

Lp.	Nazwa systemu	Gestor systemu	Opis systemu	Status	Krótki opis ewentualnej zmiany
			ETRS89, wykorzystywanej w geodezji, budownictwie, drogownictwie, administracji publicznej i innych zastosowaniach wymagających precyzyjnego określania pozycji. System wykorzystuje obserwacje satelitarne GNSS prowadzone przez sieć stacji referencyjnych rozmieszczonych na terenie Polski. Stacje te stanowią kluczowy element podstawowej osnowy geodezyjnej kraju i umożliwiają świadczenie usług korekcyjnych oraz obliczeniowych, w tym usług czasu rzeczywistego i postprocessingu. ASGEUPOS umożliwia także analizę stanu sygnałów GNSS, co ma znaczenie dla zapewnienia jakości, dokładności i niezawodności pomiarów. Rejestry publiczne: system nie prowadzi rejestrów publicznych. Główne grupy funkcjonalności obejmują: - utrzymywanie i przenoszenie geodezyjnych układów odniesienia na obszarze Polski, - obsługę sieci stacji referencyjnych GNSS, - udostępnianie danych korekcyjnych w czasie rzeczywistym, - świadczenie usług RTK i DGNS, - udostępnianie danych do obliczeń po zakończeniu pomiarów, - obsługę usług postprocessingu, - analizę		

Lp.	Nazwa systemu	Gestor systemu	Opis systemu	Status	Krótki opis ewentualnej zmiany
			obserwacji satelitarnych GNSS, wspieranie oceny jakości i stanu sygnału GNSS, zapewnienie danych dla prac geodezyjnych, kartograficznych, budowlanych i infrastrukturalnych. System integruje się z infrastrukturą referencyjną GUGiK, siecią stacji referencyjnych ASGEUPOS, systemami odbiorców usług GNSS oraz europejskimi strukturami odniesienia geodezyjnego, w tym z rozwiązaniami zgodnymi z ETRS89. W projekcie Polska Tarcza PNT system ASG-EUPOS stanowi bazowy państwowy zasób referencyjny, wokół którego rozwijane są zdolności monitorowania jakości GNSS, wykrywania zakłóceń oraz wzmacniania odporności usług PNT.		
2	Centrum analiz IGS	Międzynarodowy Serwis GNSS	System zagraniczny: Międzynarodowy Serwis GNSS (International GNSS Service - IGS) jest to organizacja naukowo-techniczna zrzeszająca Międzynarodowy Serwis GNSS (International GNSS Service - IGS) jest organizacją naukowo-techniczną zrzeszającą ośrodki badawcze, które obliczają i zapewniają dostęp do wysokiej jakości produktów GNSS obejmujących precyzyjne efemerydy satelitów GNSS, pozycje i prędkości	Istniejący	Brak

Lp.	Nazwa systemu	Gestor systemu	Opis systemu	Status	Krótki opis ewentualnej zmiany
			stacji w globalnej sieci GNSS, parametry ruchu orbitalnego Ziemi (ruch i tempo zmian biegunów, długość dnia) oraz rozwiązania zegarowe dla stacji referencyjnych i satelitów. Celem IGS jest zachowanie jednolitości w opracowaniach GNSS.		
3	Centrum analiz Trimble	Ośrodek techniczny firmy Trimble	System zagraniczny: Centrum analiz firmy Trimble, która jest producentem oprogramowania systemowego pracującego w systemie ASG-EUPOS. Na potrzeby prawidłowej pracy oprogramowania w systemie ASG-EUPOS są transmitowane z centrum analiz Trimble do centrów obliczeniowych ASG-EUPOS w czasie rzeczywistym przybliżone parametry orbit satelitów oraz poprawek do pracy zegarów satelitów.	Istniejący	Brak
4	CZEPOS	Państwowy system Rpubliki Czeskiej	System zagraniczny: Państwowy system stacji referencyjnych Republiki Czeskiej, (CZEPOS), to system wspierający pomiary GNSS na terenie Czech, który podobnie jak ASG-EUPOS posiada stacje referencyjne GNSS oraz centrum zarządzania z którego udostępnia usługi wspomagające i zwiększające dokładność pomiarów GNSS.	Istniejący	Brak
5	e-Czas.pl	Główny Urząd Miar	e-CzasPL to system wspierający niezawodną i wiarygodną dystrybucję czasu urzędowego obowiązującego na terytorium	Planowany	Brak

Lp.	Nazwa systemu	Gestor systemu	Opis systemu	Status	Krótki opis ewentualnej zmiany
			Rzeczypospolitej Polskiej oraz polskiej realizacji czasu UTC(PL). Jego celem jest zapewnienie administracji, obywatelom i podmiotom gospodarczym dostępu do źródła czasu generowanego w oparciu o państwowy wzorzec jednostek miar czasu i częstotliwości. System umożliwia synchronizację systemów komputerowych z czasem urzędowym przez Internet, a także udostępnia usługi monitorowania zgodności czasu użytkownika względem UTC(PL). Rejestry publiczne: system nie prowadzi rejestrów publicznych. Główne grupy funkcjonalności obejmują: - dystrybucję czasu urzędowego i UTC(PL) do systemów teleinformatycznych, - synchronizację czasu przez serwery czasu GUM, - monitorowanie zgodności czasu użytkownika względem UTC(PL), - prezentację czasu urzędowego w aplikacji e- Czas On-line, - udostępnianie informacji o różnicach między czasem systemowym użytkownika a czasem urzędowym, - wspieranie zastosowań wymagających wiarygodnego znakowania czasu, synchronizacji i kontroli poprawności czasu. System integruje się z		

Lp.	Nazwa systemu	Gestor systemu	Opis systemu	Status	Krótki opis ewentualnej zmiany
			systemami użytkowników poprzez usługi sieciowe synchronizacji czasu, w szczególności serwery czasu GUM: tempus1.gum.gov.pl i tempus2.gum.gov.pl. Rozwiązanie może być wykorzystywane przez administrację publiczną, przedsiębiorców, instytucje finansowe, przemysł oraz inne podmioty, dla których kluczowe znaczenie ma wiarygodny czas urzędowy, synchronizacja systemów i potwierdzanie zgodności czasu z UTC(PL).		
6	e-Infrastruktur aMON	Ministerstwo Obrony Narodowej	e-InfrastrukturaMON to system wspierający gromadzenie, przetwarzanie i udostępnianie danych przestrzennych dotyczących infrastruktury wojskowej oraz obsługę elektronicznej komunikacji w sprawach związanych z planowaniem i zagospodarowaniem przestrzennym. Celem systemu jest zapewnienie jednolitej bazy danych przestrzennych zawierającej informacje o infrastrukturze wojskowej, wspierającej procesy analityczne i decyzyjne związane z planowaniem i zagospodarowaniem przestrzennym, a także udostępnienie e-usług umożliwiających elektroniczną obsługę	Planowany	Brak

Lp.	Nazwa systemu	Gestor systemu	Opis systemu	Status	Krótki opis ewentualnej zmiany
			spraw i komunikację z interesariuszami. System nie prowadzi rejestrów publicznych. Główne grupy funkcjonalności – Gromadzenie i udostępnianie danych przestrzennych o infrastrukturze wojskowej – Wsparcie procesów planowania i zagospodarowania przestrzennego – Udostępnianie e-usług umożliwiających elektroniczną obsługę spraw oraz komunikację z interesariuszami – Udostępnianie narzędzi analitycznych wspierających procesy decyzyjne – Analiza danych pozyskiwanych z obserwacji satelitarnych i systemów nawigacji satelitarnej – Udostępnianie informacji o jakości sygnału GNSS – Udostępnianie informacji o warunkach pogody kosmicznej wpływających na technologie GNSS System jest zintegrowany z krajowymi systemami teleinformatycznymi		
7	LitPos	Państwowy system Litwy	System zagraniczny: Państwowy system stacji referencyjnych Litwy (LitPos), to system wspierający pomiary GNSS na terenie Litwy, który podobnie jak ASG-EUPOS posiada stacje referencyjne GNSS oraz centrum zarządzania z	Istniejący	Brak

Lp.	Nazwa systemu	Gestor systemu	Opis systemu	Status	Krótki opis ewentualnej zmiany
			którego udostępnia usługi wspomagające i zwiększające dokładność pomiarów GNSS.		
8	Monitor IMGW-PIB	Instytut Meteorologii i Gospodarki Wodnej - Państwowy Instytut Badawczy	Monitor IMGW-PIB to system wspierający monitorowanie, analizę i prezentację danych meteorologicznych, hydrologicznych oraz klimatycznych na obszarze Polski. Jego celem jest zapewnienie administracji, służbom, przedsiębiorcom i obywatelom dostępu do aktualnych informacji o warunkach pogodowych, stanie wód, zagrożeniach naturalnych oraz danych potrzebnych do zarządzania kryzysowego, ochrony ludności, planowania działań i oceny ryzyka. System gromadzi i udostępnia dane z sieci stacji meteorologicznych i hydrologicznych IMGWPIB oraz innych źródeł pomiarowych. Umożliwia śledzenie bieżących warunków atmosferycznych, poziomów wód, zjawisk ekstremalnych, prognoz i ostrzeżeń. Wspiera decyzje w sytuacjach zagrożenia, w rolnictwie, gospodarce wodnej, transporcie, planowaniu przestrzennym, ochronie środowiska i badaniach klimatycznych. Rejestry publiczne: system nie prowadzi rejestrów publicznych. Główne grupy	Istniejący	Brak

Lp.	Nazwa systemu	Gestor systemu	Opis systemu	Status	Krótki opis ewentualnej zmiany
			funkcjonalności obejmują: - monitoring meteorologiczny, w tym temperatury, opadów, ciśnienia, wiatru i innych parametrów pogodowych, - monitoring hydrologiczny, w tym stanów rzek, jezior i zbiorników wodnych, - prezentację danych pomiarowych w czasie rzeczywistym lub zbliżonym do rzeczywistego, - udostępnianie prognoz pogody i komunikatów, - publikację ostrzeżeń przed burzami, wichurami, powodziami, suszami i intensywnymi opadami, - dostęp do danych historycznych meteorologicznych i hydrologicznych, - wspieranie analiz klimatycznych, naukowych i planistycznych, - wspieranie zarządzania kryzysowego, ochrony ludności i gospodarki wodnej. System integruje się z infrastrukturą pomiarową IMGW-PIB, sieciami stacji meteorologicznych i hydrologicznych, systemami prognozowania, bazami danych historycznych oraz kanałami udostępniania ostrzeżeń i komunikatów. Z systemu korzystają służby ratunkowe, administracja publiczna, rolnicy, planiści, przedsiębiorcy, naukowcy i obywatele potrzebujący wiarygodnych informacji o		

Lp.	Nazwa systemu	Gestor systemu	Opis systemu	Status	Krótki opis ewentualnej zmiany
			pogodzie, wodach i klimacie.		
9	Polska Tarcza PNT	Główny Urząd Geodezji i Kartografii	Polska Tarcza PNT Moduł 1 to system wspierający monitorowanie, ochronę i utrzymanie ciągłości usług wyznaczania pozycji, nawigacji i czasu PNT/GNSS w Polsce. Jego celem jest podniesienie odporności państwa poprzez wdrożenie zintegrowanych narzędzi monitorowania jakości GNSS i usług ASG-EUPOS, wykrywania oraz lokalizacji zakłóceń, a także ochrony fizycznej warstwy usług PNT przed zagrożeniami takimi jak jamming, spoofing i degradacja sygnału. System tworzy wspólne środowisko analityczne i operacyjne dla administracji publicznej, GUGiK, MON, służb, operatorów infrastruktury krytycznej, regulatorów oraz użytkowników usług zależnych od precyzyjnej pozycji i czasu. W projekcie przewidziano komponenty: Status GNSS, Status ASG-EUPOS, MultiPNTPoint, GNSS_signal quality monitoring, Interference Search&Find, Coordinates monitoring, Platforma integracyjna, co przedstawiono w schemacie kluczowych komponentów architektury rozwiązania. Rejestry publiczne: system nie prowadzi rejestrów publicznych.	Planowany	System, który powstanie w ramach projekt

Lp.	Nazwa systemu	Gestor systemu	Opis systemu	Status	Krótki opis ewentualnej zmiany
			Główne grupy funkcjonalności obejmują: - monitorowanie jakości i dostępności sygnałów GNSS, - monitorowanie jakości i dostępności usług ASGEUPOS, - wykrywanie zakłóceń i anomalii PNT/GNSS, - lokalizację źródeł zakłóceń, - analizę wpływu zjawisk słonecznych na sygnały GNSS, - prezentację statusów, alertów, raportów i wizualizacji sytuacyjnych, - integrację danych z wielu źródeł referencyjnych i sektorowych, - wspieranie ciągłości wyznaczania pozycji i dystrybucji czasu, - ochronę usług PNT przed zakłóceniami w fizycznej warstwie cyberprzestrzeni. System integruje się z ASG-EUPOS, systemami monitorowania GNSS, systemami dziedzinowymi administracji publicznej, rozwiązaniami MON, infrastrukturą operatorów usług krytycznych oraz platformami wymiany informacji i alertów. W projekcie pełni rolę centralnej, państwowej warstwy monitorowania i odporności PNT, zapewniającej jedną panoramę sytuacyjną dla usług zależnych od pozycji, nawigacji i czasu.		
10	SAPOS	Państwowy system Niemiec	System zagraniczny: Państwowy system stacji referencyjnych Niemiec (SAPOS), to system	Istniejący	Brak

Lp.	Nazwa systemu	Gestor systemu	Opis systemu	Status	Krótki opis ewentualnej zmiany
			wspierający pomiary GNSS na terenie Niemiec, który podobnie jak ASG-EUPOS posiada stacje referencyjne GNSS oraz centrum zarządzania z którego udostępnia usługi wspomagające i zwiększające dokładność pomiarów GNSS.		
11	SKPOS	Państwowy system Słowacji	System zagraniczny: Państwowy system stacji referencyjnych Słowacji (SKPOS), to system wspierający pomiary GNSS na terenie Słowacji, który podobnie jak ASG-EUPOS posiada stacje referencyjne GNSS oraz centrum zarządzania z którego udostępnia usługi wspomagające i zwiększające dokładność pomiarów GNSS.	Istniejący	Brak
12	Smart geoportal	Główny Urząd Geodezji i Kartografii	Smart Geoportal to system wspierający Główny Urząd Geodezji i Kartografii w pozyskiwaniu, przetwarzaniu, archiwizowaniu i udostępnianiu danych oraz usług geoprzestrzennych i fotogrametrycznych. Celem systemu jest integracja zasobów i usług GUGiK oraz zapewnienie obywatelom, administracji publicznej i przedsiębiorcom dostępu do danych, narzędzi analitycznych i wizualizacji wykorzystywanych m.in. w planowaniu przestrzennym, zarządzaniu kryzysowym, inwestycjach i analizach	Planowany	Brak

Lp.	Nazwa systemu	Gestor systemu	Opis systemu	Status	Krótki opis ewentualnej zmiany
			środowiskowych. System udostępnia informacje z rejestrów centralnych prowadzonych przez Głównego Geodetę Kraju: PRG, PRNG, PRPOG, EZiUDP, BDOT10k i BDOO, oraz stanowi punkt dostępu do rejestrów prowadzonych przez samorządy i inne organy, m.in. EGİB, GESUT, BDOT500, RCN i MPZP. W module PZGiK prowadzone są ewidencja materiałów zasobu, rejestr zgłoszeń prac geodezyjnych i kartograficznych oraz rejestr wniosków o udostępnienie materiałów zasobu. Główne grupy funkcjonalności obejmują: Geoportal 2D i 3D – wyszukiwanie, publikowanie, wizualizację i analizę danych przestrzennych, metadanych i dokumentów PZGiK; PZGiK – obsługę zgłoszeń i wniosków, zakup oraz pobieranie danych i map; CAPAP – przetwarzanie danych, kontrolę ich jakości i spójności oraz udostępnianie analiz, usług i e-learningu; UMM – dostęp do danych PZGiK dla systemów powiadamiania ratunkowego; Wirtualnego Asystenta – wsparcie wyszukiwania informacji, doboru narzędzi analitycznych i dostępności usług. System wymienia dane z krajowymi systemami i rejestrami przez usługi IIP		

Lp.	Nazwa systemu	Gestor systemu	Opis systemu	Status	Krótki opis ewentualnej zmiany
			oraz interfejsy API, WMS, WMTS, WFS, SOAP i REST, m.in. z EMUiA, PRPOG, SZPRNG, SZNMT, SZPRG, ZSIN, systemami powiatowej części PZGiK, EGiB, ePUAP, Węzłem Krajowym, ISOK oraz systemami służb ratunkowych. Nie wymienia danych z systemami zagranicznymi.		
13	Systemy instytucji uprawnionych	MON, organy regulacyjne i nadzorcze, JST, regulatorzy i operatorzy infrastruktury krytycznej	System wielokrotny. Systemy instytucji uprawnionych do korzystania z informacji o zagrożeniach GNSS to systemy wspierające wykorzystanie danych dotyczących jakości, dostępności i bezpieczeństwa sygnałów globalnych systemów nawigacji satelitarnej (GNSS) w działalności operacyjnej instytucji publicznych i innych uprawnionych podmiotów. Celem funkcjonowania tej klasy systemów jest zapewnienie dostępu do informacji o zagrożeniach i zakłóceniach systemów GNSS oraz umożliwienie ich wykorzystania w procesach monitorowania, analizy, podejmowania decyzji i realizacji zadań operacyjnych.	Istniejący	Brak
14	ZakPos	Prywatny system Ukrainy	System zagraniczny: Prywatny system stacji referencyjnych Ukrainy (ZakPos), to system wspierający pomiary GNSS na terenie Ukrainy, który podobnie jak ASG-EUPOS posiada stacje	Istniejący	Brak

Lp.	Nazwa systemu	Gestor systemu	Opis systemu	Status	Krótki opis ewentualnej zmiany
			referencyjne GNSS oraz centrum zarządzania z którego udostępnia usługi wspomagające i zwiększające dokładność pomiarów GNSS.		

Lista przepływów

Lp.	System źródłowy	System docelowy	Zakres wymienianych danych	Sposób wymiany danych	Typ modyfikacji	Typ interfejsu
1	SKPOS	ASG-EUPOS	System SKPOS przesyła do systemu ASG-EUPOS dane obserwacyjne GNSS z przygranicznych stacji referencyjnych. Dane obserwacyjne GNSS	tryb odwołań bezpośrednich	realizowalny inną metodą	NTRIP / RTCM
2	ASG-EUPOS	SAPOS	System ASG-EUPOS przesyła do SKPOS dane obserwacyjne GNSS z przygranicznych stacji referencyjnych. Dane obserwacyjne GNSS	tryb odwołań bezpośrednich	realizowalny inną metodą	NTRIP / RTCM
3	ASG-EUPOS	Polska Tarcza PNT	Dane usługowe i referencyjne ASG-EUPOS, obserwacje GNSS ze stacji referencyjnych,	tryb odwołań bezpośrednich	krytyczny dla sukcesu projektu	usługa REST

Lp.	System źródłowy	System docelowy	Zakres wymienianych danych	Sposób wymiany danych	Typ modyfikacji	Typ interfejsu
			status dostępności usług, parametry jakości korekt, informacje o pracy stacji, dane RTK/ DGNSS/ postprocessing oraz dane potrzebne do monitorowania jakości usług ASG-EUPOS.			
4	ASG-EUPOS	CZEPOS	System ASG-EUPOS przesyła do SKPOS dane obserwacyjne GNSS z przygranicznych stacji referencyjnych . Dane obserwacyjne GNSS	tryb odwołań bezpośrednich	realizowalny inną metodą	NTRIP / RTCM
5	ASG-EUPOS	e-InfrastrukturaMON	System ASG-EUPOS będzie przysyłał do e-infrastruktury MON obserwacje GNSS z wytypowanych stacji referencyjnych systemu ASG-EUPOS Dane obserwacyjne GNSS	tryb odwołań bezpośrednich	realizowalny inną metodą	NTRIP / RTCM
6	ZakPos	ASG-EUPOS	System ZakPos przesyła do systemu ASG-EUPOS dane obserwacyjne	tryb odwołań bezpośrednich	realizowalny inną metodą	NTRIP / RTCM

Lp.	System źródłowy	System docelowy	Zakres wymienianych danych	Sposób wymiany danych	Typ modyfikacji	Typ interfejsu
			GNSS z przygranicznych stacji referencyjnych . Dane obserwacyjne GNSS			
7	Centrum analiz IGS	ASG-EUPOS	Centrum analiz udostępnia na swoich serwerach wyniki obliczeń, a system ASG-EUPOS pobiera je przez internet. Dane: Precyzyjne orbity satelitów oraz poprawki zegarów satelitarnych	kopiowanie danych	Krytyczny dla sukcesu przedsięwzięcia	usługa REST
8	ASG-EUPOS	SKPOS	System ASG-EUPOS przesyła do SKPOS dane obserwacyjne GNSS z przygranicznych stacji referencyjnych . Dane obserwacyjne GNSS	tryb odwołań bezpośrednich	realizowalny inną metodą	NTRIP / RTCM
9	CZEPOS	ASG-EUPOS	System CZEPOS przesyła do systemu ASG-EUPOS dane obserwacyjne GNSS z przygranicznych stacji referencyjnych	tryb odwołań bezpośrednich	realizowalny inną metodą	NTRIP / RTCM

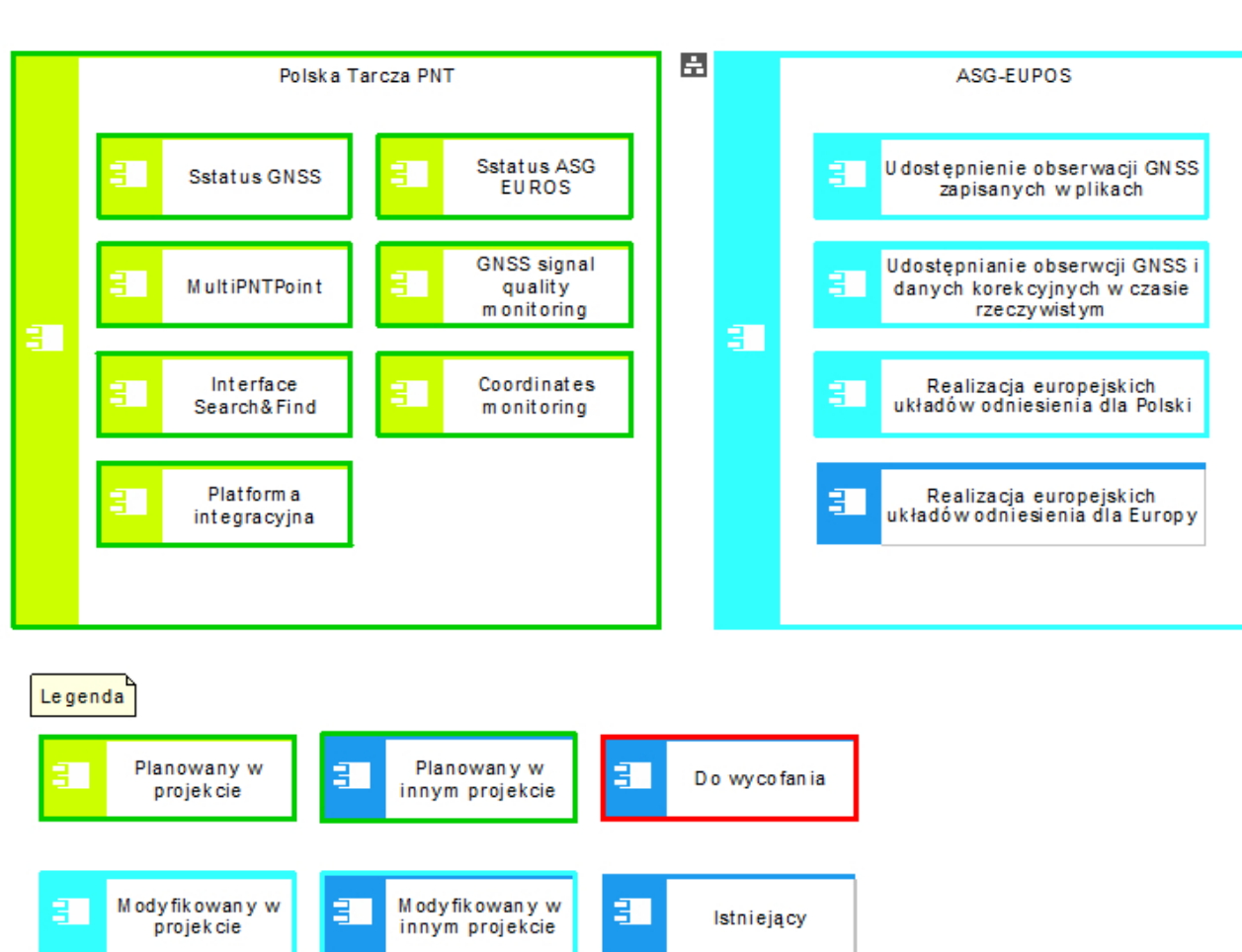
Lp.	System źródłowy	System docelowy	Zakres wymienianych danych	Sposób wymiany danych	Typ modyfikacji	Typ interfejsu
			Dane obserwacyjne GNSS			
10	SAPOS	ASG-EUPOS	System SAPOS przesyła do systemu ASG-EUPOS dane obserwacyjne GNSS z przygranicznych stacji referencyjnych Dane obserwacyjne GNSS	tryb odwołań bezpośrednich	realizowalny inną metodą	NTRIP / RTCM
11	e-InfrastrukturaMON	ASG-EUPOS	Dane w postaci numerycznej lub mapowej z naniesionymi wizualizacjami wyników analiz pozyskanych z e-infrastruktura MON.	tryb odwołań bezpośrednich	realizowalny inną metodą	usługa REST
12	ASG-EUPOS	ZakPos	System ASG-EUPOS przesyła do SKPOS dane obserwacyjne GNSS z przygranicznych stacji referencyjnych. Dane obserwacyjne GNSS.	tryb odwołań bezpośrednich	realizowalny inną metodą	NTRIP / RTCM
13	Centrum analiz Trimble	ASG-EUPOS	Centrum analiz udostępnia na swoich serwerach wyniki obliczeń, a	kopiowanie danych	realizowalny inną metodą	usługa REST

Lp.	System źródłowy	System docelowy	Zakres wymienianych danych	Sposób wymiany danych	Typ modyfikacji	Typ interfejsu
			system ASG-EUPOS pobiera je przez internet. Dane: Precyzyjne orbity satelitów oraz poprawki zegarów satelitarnych			
14	ASG-EUPOS	LitPos	System ASG-EUPOS przesyła do SKPOS dane obserwacyjne GNSS z przygranicznych stacji referencyjnych . Dane obserwacyjne GNSS	tryb odwołań bezpośrednich	realizowalny inną metodą	NTRIP / RTCM
15	LitPos	ASG-EUPOS	System LitPos przesyła do systemu ASG-EUPOS dane obserwacyjne GNSS z przygranicznych stacji referencyjnych . Dane obserwacyjne GNSS	tryb odwołań bezpośrednich	realizowalny inną metodą	NTRIP / RTCM
16	e-Czas.pl	Polska Tarcza PNT	Dane referencyjne czasu urzędowego i UTC(PL), informacje o wiarygodnym źródle czasu, dane synchronizacyjne oraz parametry	tryb odwołań bezpośrednich	Krytyczny dla sukcesu przedsięwzięcia	usługa REST

Lp.	System źródłowy	System docelowy	Zakres wymienianych danych	Sposób wymiany danych	Typ modyfikacji	Typ interfejsu
			umożliwiające kontrolę zgodności czasu wykorzystywanego przez komponenty projektu			
17	Monitor IMGW-PIB	Polska Tarcza PNT	Dane meteorologiczne, hydrologiczne i środowiskowe, w tym informacje o zjawiskach mogących wpływać na propagację sygnałów, warunki pracy infrastruktury terenowej, ocenę ryzyka operacyjnego oraz kontekst dla analiz jakości GNSS.	tryb odwołań bezpośrednich	realizowalny inną metodą	usługa REST
18	Smart geoportal	Polska Tarcza PNT	Dane podstawowe do systemów mapowych prezentujących wyniki analiz Polska Tarcza PNT.	tryb odwołań bezpośrednich	realizowalny inną metodą	usługa REST
19	Polska Tarcza PNT	Systemy instytucji uprawnionych	Dane wynikowe z przeprowadzonych analiz sygnałów GNSS udostępnione w różnych formatach w zależności od rodzaju analiz. Dane w	tryb odwołań bezpośrednich	realizowalny inną metodą	usługa REST

Lp.	System źródłowy	System docelowy	Zakres wymienianych danych	Sposób wymiany danych	Typ modyfikacji	Typ interfejsu
			postaci map z naniesionymi wizualizacjami wyników. W najszerszym zakresie wykorzystanie API i REST.			
20	Polska Tarcza PNT	Smart geoportal	Dane w postaci map z naniesionymi wizualizacjami wyników analiz pozyskanych z Polskiej Tarczy PNT.	tryb odwołań bezpośrednich	realizowalny inną metodą	usługa REST

7.2. Kluczowe komponenty architektury rozwiązania



7.3. Przyjęte założenia technologiczne

Lp.	Obszar	Założenie technologiczne
1.	Infrastruktura	Architektura chmura–mgła–brzeg. System będzie funkcjonował w całości w multi chmurze PL-GRID. Federalizacja klastrów funkcjonujących w różnych chmurach będzie pozytywnie wpływała na aspekty bezpieczeństwa danych, ciągłości działania i dostępności. Architektura Rozwiązania IT zapewnia jego wysoką dostępność oraz mechanizmy wymiany danych z systemami zewnętrznymi poprzez interfejsy integracyjne. Infrastruktura będzie zarządzana w technologii Infrastructure as Code (IaC), co pozwoli na automatyzację wdrożeń, zarządzania konfiguracją oraz łatwe skalowanie zasobów
2.	Sieć i bezpieczeństwo	Wymagana jest redundancja łączności i zasilania oraz integracja z krajową warstwą obsługi incydentów i wymiany informacji. Rozwiązanie ma wspierać kontrolowany dostęp do zasobów operacyjnych. Zapewnienie bezpieczeństwa powierzone zostanie operatorowi chmury PL-GRID.
3.	Standardy wymiany danych	API, interfejsy statusowe i integracyjne dla administracji oraz feedy STIX/TAXII dla wymiany informacji o zagrożeniach. W obszarze czasu projekt wspiera mechanizmy PTP/NTP i Time-as-a-Service.
4.	Systemy operacyjne serwerowe	W projekcie nie zakłada się wskazywania producentów systemów. Dobór systemów będzie podporządkowany bezpieczeństwu, wysokiej dostępności i architekturze platformy centralnej. Za dobór systemów operacyjnych serwerów odpowiedzialny będzie operator chmury PL-GRID.
5.	Bazy danych	W projekcie nie zakłada się wskazywania producenta silnika bazodanowego. Rozwiązanie musi obsługiwać dużą ilość danych telemetrycznych, o zdarzeniach, statusowych i raportowych . Za dobór baz danych odpowiedzialny będzie operator chmury PL-GRID.
6.	Serwery aplikacji	Platforma integracyjna obejmie środowisko chmurowe IaaS oraz projekt platformy kubernetesowej zarządzanej tradycyjnie i „AI READY”. Za dobór serwerów odpowiedzialny będzie operator chmury PL-GRID.
7.	Portale	Warstwa dostępowa obejmuje serwis internetowy Status_ASG-EUPOS oraz wizualizacje „źródła prawdy” dobrane według preferencji użytkowników. Portale opracowane w ramach projektu będą spełniały obowiązujące wymagania dostępności cyfrowej, w tym wymagania WCAG 2.2 na poziomie AA.
8.	Inne	Projekt zakłada wykorzystanie edge computing, SDR, sensorów ADS-B, stacji meteo, wykrywania wyładowań atmosferycznych oraz metod AI/ML do analizy zakłóceń GNSS i incydentów cybernetycznych.

7.4. Opis zasobów danych przetwarzanych w planowanym rozwiązaniu

Czy nowy system będzie tworzył zasoby danych o charakterze rejestru publicznego?

TAK/NIE

Czy nowy system będzie przetwarzał (używał, zmieniał) zawartość innych rejestrów publicznych?

TAK/NIE

7.5. Bezpieczeństwo

Planowany poziom zapewnienia bezpieczeństwa (w rozumieniu przepisów §20 rozporządzenia Rady Ministrów z dnia 12 kwietnia 2012 r. w sprawie Krajowych Ram Interoperacyjności [...] (Dz. U. 2012, poz. 526 z późn. zm.) w zakresie dot. systemu zarządzania bezpieczeństwem informacji:

~~- system nie podlega rygorom KRI – należy wyjaśnić czy istnieją inne normy bezpieczeństwa, które będą spełnione przez system zgodnie z wymogami KRI~~

- dodatkowe zabezpieczenia powyżej wymogów KRI: należy wskazać uzasadnienie

Ze względu na charakter projektu przyjęty zostanie podwyższony poziom ochrony, właściwy dla systemu przetwarzającego dane operacyjne dotyczące jakości PNT/GNSS, zakłóceń, alertów, statusów usług ASG-EUPOS oraz informacji istotnych dla administracji, obronności i infrastruktury krytycznej. Dane będą udostępniane zgodnie z modelem wielopoziomowego dostępu, z rozdzieleniem warstwy publicznej, sektorowej i operacyjnej oraz z ograniczeniem dostępu do informacji wrażliwych, w szczególności dotyczących źródeł zakłóceń i szczegółów incydentów.