

OPIS ZAŁOŻEŃ PROJEKTU INFORMATYCZNEGO

| | | | |
|-------------------------------------|--|--------------------------|-----------|
| Tytuł projektu | Zwiększenie dojrzałości cyfrowej i cyberbezpieczeństwa firm poprzez udostępnienie usług cyfrowych na Biznes.gov.pl | | |
| Wnioskodawca | Minister Rozwoju i Technologii | | |
| Beneficjent | Ministerstwo Rozwoju i Technologii | | |
| Partnerzy | Naukowa Akademicka Sieć Komputerowa | | |
| Źródło finansowania | 1. Budżet Państwa (część budżetowa 20) 2. Krajowy Plan Odbudowy i Zwiększania Odporności, Inwestycja C2.1.1 „E-usługi publiczne, rozwiązania IT usprawniające funkcjonowanie administracji i sektorów gospodarki oraz technologie przełomowe w sektorze publicznym, gospodarce i społeczeństwie”. | | |
| Całkowity koszt projektu | 8 220 752,00 zł | | |
| Planowany okres realizacji projektu | 09-2024 do 06-2026 | | |
| Osoba kontaktowa | Maria Magdoń | maria.magdon@mrit.gov.pl | 504168044 |

1. POWODY PODJĘCIA PROJEKTU

1.1. Identyfikacja problemu i potrzeb

Problemy i potrzeby:

1. Rosnąca liczba cyberataków:

Obecnie codziennie pojawia się około 300 tysięcy nowych programów malware, które stają się coraz bardziej wyrafinowane i trudniejsze do wykrycia. MŚP, które często nie dysponują zaawansowanymi narzędziami i zasobami do skutecznego przeciwdziałania takim zagrożeniom, są szczególnie narażone na ataki, takie jak kradzież danych, wyłączenie serwerów, czy wymuszenia finansowe (ransomware).

2. Niedostateczne zasoby i narzędzia:

Mimo że 95% firm posiada oprogramowanie antywirusowe i systemy zabezpieczeń, tylko 83% regularnie je aktualizuje. Zaledwie 78% firm stosuje bezpieczne hasła, a tylko 55% regularnie tworzy kopie zapasowe danych. Brak odpowiednich zasobów oraz narzędzi do zarządzania i monitorowania bezpieczeństwa informatycznego jest jednym z kluczowych problemów, z którym borykają się MŚP.

3. Brak specjalistycznej wiedzy:

Wielu pracowników MŚP nie ma dostatecznej wiedzy na temat cyberzagrożeń. Aż 78% firm nie uczestniczyło w żadnym szkoleniu z zakresu cyberbezpieczeństwa w poprzednim roku, co czyni ich pracowników jednym z najsłabszych ogniw w strategii ochrony przedsiębiorstw. Dodatkowo, jedynie 15% firm wprowadziło w zeszłym roku nowe rozwiązania w zakresie cyberbezpieczeństwa, co świadczy o braku świadomości oraz wiedzy w tym obszarze.

4. Brak systemowego wsparcia i regulacji:

Jedynie 13% firm posiada formalne dokumenty regulujące politykę cyberbezpieczeństwa, co wskazuje na brak systemowego podejścia do ochrony przed zagrożeniami. Bez odpowiednich regulacji i wsparcia instytucjonalnego MŚP mają trudności w opracowaniu i wdrożeniu skutecznych strategii zabezpieczeń.

Planowane produkty:

1. Usługa analityczna dojrzałości cyfrowej (analiza luk dojrzałości cyfrowej i poziomu

cyberbezpieczeństwa)

2. Usługa pre-kwalifikacji dot. wymagań dla producenta IT, przygotowująca MŚP do spełnienia wymagań Cyber Resilience Act

3. Usługa pre-weryfikacji zgodności z zaleceniami NIS2.

| Interesariusz | Zidentyfikowany problem | Szacowana wielkość grupy |
|-------------------------------|---|--------------------------|
| Przedsiębiorcy z segmentu MŚP | <p>1. Zbyt długi czas wykrywania naruszeń (średni czas od włamania do systemu informatycznego do jego wykrycia wynosi 287 dni, co znacząco opóźnia reakcję na zagrożenie i minimalizację jego skutków).</p> <p>2. Niewystarczające zgłaszanie cyberprzestępstw (w ciągu ostatnich trzech lat ponad 80% przedsiębiorców, którzy doświadczyli cyberataku, nigdy nie zgłosiło tego typu incydentu odpowiednim organom, co utrudnia walkę z cyberprzestępczością na poziomie krajowym)</p> <p>3. Niska samoocena cyberodporności (przedsiębiorcy sami oceniają swoją odporność na cyberzagrożenia jako niską, co wskazuje na potrzebę podniesienia poziomu świadomości i zabezpieczeń)</p> <p>4. Niewystarczający poziom wsparcia ze strony państwa (wyniki pilotażowego Programu Firma Bezpieczna Cyfrowo, uruchomionego przez NASK, MC i MRiT, wykazały, że istnieje konieczność zwiększenia edukacji oraz wsparcia państwa w zakresie cyberbezpieczeństwa, aby skutecznie przeciwdziałać rosnącym zagrożeniom)</p> | 2,65 mln |
| Pracownicy MŚP | <p>1. Brak świadomości zagrożeń cybernetycznych wśród pracowników (pracownicy często nie są świadomi istniejących zagrożeń, co czyni ich podatnymi na ataki cyberprzestępców).</p> <p>2. Niewystarczająca edukacja w zakresie cyberbezpieczeństwa (w firmach brakuje systematycznego kształcenia pracowników w obszarze rozpoznawania i reagowania na cyberzagrożenia).</p> <p>3. Ograniczone zdolności przewidywania i zapobiegania cyberatakam (pracownicy nie posiadają wypracowanych schematów działań, które mogłyby skutecznie ograniczyć ryzyko ataków, co wynika z braku odpowiednich szkoleń i narzędzi).</p> <p>4. Brak spójnych procedur reagowania na cyberzagrożenia (firmy nie mają wdrożonych zdefiniowanych i skutecznych procedur, które pracownicy mogliby stosować w przypadku wykrycia zagrożenia cybernetycznego).</p> | 11,5 mln |

| Interesariusz | Zidentyfikowany problem | Szacowana wielkość grupy |
|------------------------------------|--|--------------------------|
| Ministerstwo Rozwoju i Technologii | MRiT jako instytucja odpowiadająca na potrzeby polskich przedsiębiorców, powinna zrealizować działania wspierające przedsiębiorców w podniesieniu poziomu cyberodporności firm. Działania MRiT powinny być bezpośrednio skorelowane z działaniami legislacyjnymi z zakresu cyberbezpieczeństwa, prowadzonymi przez Ministerstwo Cyfryzacji oraz opierać się na szerokim dostarczeniu do przedsiębiorców z informacjami oraz formą wsparcia merytorycznego m.in. dostosowania firm do wymogów NIS2. | 1 |

1.2. Opis stanu obecnego

Na przestrzeni 2023 i 2024 r. został przeprowadzony pilotażowy program "Firma Bezpieczna Cyfrowo", zrealizowany wspólnie przez MRiT, NASK-PIB oraz MC. W ramach pilotażu została uruchomiona strona internetowa firmabezpiecznacyfrowo.pl, na której użytkownik dokonywał weryfikacji stanu cyberbezpieczeństwa i umiejętności cyfrowych reprezentowanej firmy poprzez wypełnienie elektronicznej ankiety. Na podstawie wyników ankiety, po jej wypełnieniu - generował się poradnik w formacie pdf, zawierający wstępną ocenę mocnych i słabych elementów firmy w zakresie cyberbezpieczeństwa oraz opisane do wykonania zadania dla przedsiębiorcy, których realizacja pozwalała na podejście do procesu certyfikacji "Firma Bezpieczna Cyfrowo". Obecnie e-usługi stanowiące produkty niniejszego projektu nie istnieją. Modyfikacja systemu Biznes.gov.pl, o której również mowa, nastąpi w związku z zaprojektowaniem i wdrożeniem e-usług. Punktem wyjścia dla projektowania e-usług jest ankieta i poradnik, stanowiące produkty pilotażu projektu "Firma Bezpieczna Cyfrowo".

Produkty projektu znacząco wpływają na realizację korzyści, takich jak zwiększenie odporności na cyberzagrożenia dzięki analizie dojrzałości cyfrowej i cyberbezpieczeństwa; zwiększenie zaufania klientów poprzez zgodność z Cyber Resilience Act i NIS2 oraz poprawę jakości usług publicznych poprzez nowoczesne e-usługi na Biznes.gov.pl. Projekt przyczynia się do automatyzacji i przyspieszenia obsługi przedsiębiorców, zwiększając efektywność administracji. Wzmacnia również stabilność gospodarczą poprzez minimalizowanie ryzyka związanego z cyberatakami, co zwiększa bezpieczeństwo operacyjne firm i gospodarki oraz przyciąga inwestycje, wspiera rozwój sektora technologii cyberbezpieczeństwa i podnosi poziom edukacji cyfrowej przedsiębiorców.

2. EFEKTY PROJEKTU

2.1. Cele i korzyści wynikające z projektu

| | |
|------------------|--|
| Cel - 1 | Podniesienie poziomu bezpieczeństwa MŚP oraz stabilności obrotu gospodarczego w Polsce. |
| Cel strategiczny | 1) Strategia Cyberbezpieczeństwa Rzeczypospolitej Polskiej na lata 2019–2024, Cel szczegółowy 3 – Zwiększenie potencjału narodowego w zakresie technologii cyberbezpieczeństwa: Projekt realizowany w partnerstwie z NASK-PIB (wsparcie rozwoju krajowych |

| | |
|-----------------|---|
| | <p>ośrodków badawczych).</p> <p>2) Strategia UE w zakresie cyberbezpieczeństwa na dekadę cyfrową (Shaping Europe's digital future): Strategia podkreśla istotne znaczenie bezpieczeństwa wszystkich elementów łańcucha dostaw, którego wzrost jest możliwy dzięki wdrożeniu przez firmy rekomendacji uzyskanych w efekcie realizacji e-usług planowanych w projekcie.</p> <p>3) Europejska deklaracja praw i zasad cyfrowych, Rozdział V: Bezpieczeństwo, ochrona i wzmocnienie pozycji, Chronione, bezpieczne i pewne środowisko cyfrowe: Projekt wpisuje się w podkreśloną w deklaracji potrzebę zapewnienia cyberbezpieczeństwa w społeczeństwie poprzez dostarczenie narzędzi pozwalających przedsiębiorcom chronić się przed zagrożeniami w cyberprzestrzeni.</p> <p>4) Strategia na rzecz Odpowiedzialnego Rozwoju do roku 2020 (z perspektywą do 2030 r.), Cel szczegółowy III – Skuteczne państwo i instytucje służące wzrostowi oraz włączeniu społecznemu i gospodarczemu, Obszar: E-państwo: Planowane w projekcie e-usługi odpowiadają na potrzebę dostępu do wysokiej jakości usług publicznych za pośrednictwem nowoczesnych rozwiązań informatycznych.</p> <p>5) Program Zintegrowanej Informatyzacji Państwa, cel 4.2.1. Zwiększenie jakości oraz zakresu komunikacji między obywatelami i innymi interesariuszami a państwem oraz cel 4.2.2. Wzmocnienie dojrzałości organizacyjnej jednostek administracji publicznej oraz usprawnienie zaplecza elektronicznej administracji (backoffice): Rozwój systemu Biznes.gov.pl, modułu Konto Przedsiębiorcy o funkcjonalność Bezpieczna Firma.</p> <p>6) Program Krajowy Plan Odbudowy i Zwiększania Odporności (KPO) - Inwestycja C2.1.1 E-usługi publiczne, rozwiązania IT usprawniające funkcjonowanie administracji i sektorów gospodarki oraz technologie przełomowe w sektorze publicznym, gospodarce i społeczeństwie: Wsparcie transformacji cyfrowej MŚP poprzez opracowanie e-usług z zakresu cyberbezpieczeństwa w serwisie Biznes.gov.pl.</p> |
| Korzyść: | <ol style="list-style-type: none"> 1. Zwiększenie odporności na cyberzagrożenia. 2. Zwiększenie zaufania klientów i partnerów biznesowych. 3. Poprawa konkurencyjności. 4. Poprawa jakości usług świadczonych przez instytucje, upowszechnianie najlepszych praktyk w zakresie obsługi biznesu. 5. Podniesienie efektywności, automatyzacja i przyspieszenie obsługi obywateli i przedsiębiorców. 6. Zwiększenie stabilności gospodarczej. 7. Wzrost inwestycji. 8. Przyspieszenie rozwoju sektora technologii cyberbezpieczeństwa. 9. Podniesienie poziomu edukacji i umiejętności cyfrowych. |
| KPI: | <p>KPI 1. Zakończenie procesu opracowywania nowych lub udoskonalania istniejących e-usług.</p> <p>KPI 2. Zakończenie procesu opracowywania nowych lub rozwijania istniejących publicznych systemów informatycznych.</p> <p>KPI 3. Użytkownicy nowych i zmodernizowanych publicznych usług, produktów i procesów cyfrowych.</p> <p>KPI 4. Odsetek firm które wdrożyły otrzymane rekomendacje, spośród tych,</p> |

| | |
|---|---|
| | które zrealizowały e-usługi. |
| Wartość aktualna i docelowa KPI: | KPI 1. 0 KPI 2. 0 KPI 3. 0 KPI 4. 0 KPI 1. 3 KPI 2. 1 KPI 3. 30 000 KPI 4. 15% |
| Metoda pomiaru KPI | KPI 1. Dokumentacja projektowa. Protokół odbioru wdrożonej e-usługi. Jednorazowo, w dniu zakończenia projektu. KPI 2. Dokumentacja projektowa. Protokół odbioru rozwiniętego systemu Biznes.gov.pl. Jednorazowo, w dniu zakończenia projektu. KPI 3. Odczyt informacji z baz danych serwisu Biznes.gov.pl, jest to łączna liczba wykonań zbudowanych w ramach projektu e-usług. 12 miesięcy po zakończeniu projektu. KPI 4. Badanie dot. wpływu wdrożonych rozwiązań z zakresu cyberbezpieczeństwa w MŚP na poziom cyberbezpieczeństwa w gospodarce w kontekście transformacji cyfrowej przedsiębiorstw. |

2.2. Udostępnione e-usługi

| Lp. | Nazwa e-usługi | Typ | Zakres oddziaływania | Poziom dojrzałości e-usługi |
|-----|--|-----|---|-----------------------------|
| 1 | <p>Analiza dojrzałości cyfrowej i cyberbezpieczeństwa.</p> <p>E-usługa zaprojektowana z myślą o poprawie świadomości i umiejętności przedsiębiorców w zakresie cyberbezpieczeństwa. Oferuje interaktywny i spersonalizowany proces diagnozy i edukacji, który przeprowadzi użytkowników przez zagadnienia związane z cyberbezpieczeństwem i wdrożeniem usług cyfrowych. Usługa kończy się przez wygenerowanie spersonalizowanego sprawozdania z elementami poradnika, skupiającego się na konkretnych działaniach, które użytkownik powinien podjąć, aby osiągnąć podstawowy poziom cyberbezpieczeństwa firmy. Jest to rozbudowa usługi przygotowanej w ramach pilotażowego projektu edukacji i certyfikacji „Firma Bezpieczna Cyfrowo”, realizowanego przez MRiT oraz NASK-PIB.</p> | A2B | Przedsiębiorcy [MŚP] Pracownicy MŚP (rocznie ok 40000 transakcji) | Personalizacja |
| 2 | <p>Pre-weryfikacja NIS2.</p> <p>E-usługa pozwoli na weryfikację, czy</p> | A2B | Przedsiębiorcy [MŚP] Pracownicy MŚP | Personalizacja |

| Lp. | Nazwa e-usługi | Typ | Zakres oddziaływania | Poziom dojrzałości e-usługi |
|-----|--|-----|--|-----------------------------|
| | firma podlega pod zakres regulacji NIS2, zaoferuje spersonalizowane rekomendacje oraz wsparcie w procesie dostosowania do wymagań dyrektywy. Na podstawie zebranych danych, w e-usłudze generowane będą spersonalizowane rekomendacje, które będą dostosowane do specyfiki i potrzeb konkretnego przedsiębiorstwa, użytkownik zostanie również poinformowany o obowiązkach spoczywających na firmie oraz uzyska możliwość zgłoszenia się do programu certyfikacji wraz z przewypełnieniem odpowiedniej dokumentacji. | | (rocznie ok 20000 transakcji) | |
| 3 | Pre-kwalifikacja CRA E-usługa zaprojektowana specjalnie dla małych i średnich przedsiębiorstw, aby przeprowadzić je przez wymagania Cyber Resilience Act (CRA) i wspierać je w procesie ich implementacji. Usługa ta stanowić będzie kompleksowe narzędzie, które nie tylko edukuje, ale również ułatwia zrozumienie i zastosowanie przepisów CRA w praktyce biznesowej. Usługę zakończy możliwość wygenerowania deklaracji zgodności, która będzie podsumowaniem wdrożonych środków i gotowości do spełnienia wymagań CRA, użytkownik zostanie również poinformowany o obowiązkach spoczywających na firmie np. w zakresie dokumentacji technicznej oraz uzyska możliwość zgłoszenia się do programu certyfikacji wraz z przewypełnieniem odpowiedniej dokumentacji. | A2B | Przedsiębiorcy [MŚP] Pracownicy MŚP (rocznie ok 5000 transakcji) | Personalizacja |

2.3. Udostępnione informacje sektora publicznego i zdigitalizowane zasoby

Nie dotyczy

2.4. Produkty końcowe projektu

| Nazwa produktu | Planowana data wdrożenia |
|--|--------------------------|
| Materiały informacyjno-promocyjne | 06-2026 |
| Pozytywny raport z testów/audytu bezpieczeństwa | 06-2026 |
| Pozytywny raport z audytu dostępności cyfrowej | 06-2026 |
| Pozytywny raport z badań UX | 06-2026 |
| Raport z badania dot. wpływu wdrożonych rozwiązań z zakresu cyberbezpieczeństwa w MŚP na poziom cyberbezpieczeństwa w gospodarce w kontekście transformacji cyfrowej przedsiębiorstw | 06-2026 |
| Dokumentacja wytworzonej architektury rozwiązania składającego zaświadczenia/deklaracje | 06-2026 |
| Zmodyfikowany system Biznes.gov.pl | 06-2026 |
| Pozytywny raport z audytu dostępności cyfrowej | 06-2026 |
| Zmodyfikowane API Biznes.gov.pl | 06-2026 |

3. KAMIENIE MIŁOWE

| Kamienie milowe | Planowany termin osiągnięcia |
|--|------------------------------|
| Udostępniony prototyp usługi analizy dojrzałości cyfrowej i cyberbezpieczeństwa na środowisku testowym Biznes.gov.pl | 2025-04-30 |
| Odebrana usługa analizy dojrzałości cyfrowej i cyberbezpieczeństwa na środowisku produkcyjnym Biznes.gov.pl | 2025-06-30 |
| Udostępniony prototyp usługi pre-kwalifikacji NIS-2 na środowisku testowym Biznes.gov.pl | 2025-12-31 |
| Udostępniony prototyp usługi pre-kwalifikacji CRA na środowisku testowym Biznes.gov.pl | 2026-01-31 |
| Odebrana usługa pre-kwalifikacji NIS-2 na środowisku produkcyjnym Biznes.gov.pl | 2026-06-30 |
| Odebrana usługa pre-kwalifikacji CRA na środowisku produkcyjnym Biznes.gov.pl | 2026-06-30 |
| Odebrany rozbudowany system Biznes.gov.pl | 2026-06-30 |
| Przeprowadzony audyt dostępności cyfrowej | 2026-06-30 |

4. KOSZTY

4.1. Koszty ogólne projektu wraz ze sposobem finansowania

| | | |
|---|---|---|
| Całkowity koszt projektu (netto oraz brutto), w tym | Netto 7 368 817,04 zł Brutto 8 220 752,00 zł | |
| Procent dofinansowania ze środków UE (brutto) | 89,63% | |
| Procent środków z budżetu państwa (brutto) | 10,37% | |
| Podział całkowitego kosztu projektu na poszczególne lata (netto oraz brutto) | 2024 | Netto 2 267 328,32 zł Brutto 2 529 462,15 zł |
| | 2025 | Netto 3 400 992,48 zł Brutto 3 794 193,23 zł |
| | 2026 | Netto 1 700 496,24 zł Brutto 1 897 096,62 zł |

4.2. Wykaz poszczególnych pozycji kosztowych

| Nazwa pozycji kosztowej | | Przewidywany koszt brutto | Uzasadnienie pozycji kosztowej (przeznaczenie) |
|-------------------------|--|---------------------------|---|
| Oprogramowanie | 1. badanie dotyczące wpływu wdrożenia rozwiązań z zakresu cyberbezpieczeństwa w MŚP na poziom cyberbezpieczeństwa w gospodarce w kontekście transformacji cyfrowej przedsiębiorstw; 2. zakup usługi wsparcia ze strony konsultantów Centrum Pomocy Przedsiębiorcy procesu realizacji e-usług przez przedsiębiorców (dotyczy etapu testowania e-usług na środowisku testowym, przed wdrożeniem na środowisko | 4 196 188,00 zł | Badanie służy jakościowej ocenie korzyści z wdrożenia e-usług. Wsparcie konsultantów dla przedsiębiorców w procesie testowania e-usług wpłynie znacząco na wzrost jakości e-usług dostarczonych na produkcję. Funkcjonalność Bezpieczna Firma oraz budowane e-usługi wraz z architekturą rozwiązania do składania zaświadczeń/ deklaracji oraz dostępu do spersonalizowanych materiałów umożliwiają przedsiębiorcom efektywne zarządzanie zgodnością z przepisami. Koszty osobowe osób odpowiedzialnych za opracowanie, wdrożenie i koordynację kluczowych elementów projektu. |

| Nazwa pozycji kosztowej | | Przewidywany koszt brutto | Uzasadnienie pozycji kosztowej (przeznaczenie) |
|-------------------------|--|---------------------------|---|
| | produkcyjne) 3. rozbudowa Konta Przedsiębiorcy o funkcjonalność Bezpieczna Firma oraz wzmocnienie; poziomu cyberbezpieczeństwa systemu Biznes.gov.pl; 4. budowa e-usług w konfiguratorze; 5. wytworzenie architektury rozwiązania składającego; zaświadczenia/ deklaracje (zmiana/ przebudowa architektury systemu Biznes.gov.pl) ; Dodatkowo koszty osobowe Analityka biznesowego, Specjalisty ds. CRA. | | |
| Infrastruktura | 1. zakup licencji typu Windows Server Standard i SQL. 2 zakup macierzy dyskowych | 560 000,00 zł | Zakup licencji Windows Server Standard i SQL jest niezbędny do stabilnego działania systemu a zakup macierzy dyskowej związany z koniecznością składowania zaświadczeń/ deklaracji powstałych w ramach realizowanych przez użytkowników usług. |
| Koszty UX i grafiki | 1. projektowanie interfejsów graficznych; 2. audyt dostępności; 3. projektowanie doświadczeń użytkownika (UX Costs całkowite); 4. opracowanie treści informacyjnych, | 390 000,00 zł | Rozbudowywanie intuicyjnego, dostępnego i efektywnego systemu Biznes.gov.pl, aby ułatwić użytkownikom korzystanie z nowych e-usług. Audyt dostępności zapewnia zgodność z wymogami prawnymi, umożliwiając dostęp do systemu osobom z różnymi potrzebami, co jest niezbędne dla szerokiego wykorzystania produktów projektu. |

| Nazwa pozycji kosztowej | | Przewidywany koszt brutto | Uzasadnienie pozycji kosztowej (przeznaczenie) |
|--|---|---------------------------|---|
| | tekstów i komunikatów w e-usługach i Koncie Przedsiębiorcy | | |
| Bezpieczeństwo | 1. Zlecenie audytu bezpieczeństwa. 2. Koszt osobowy Specjalisty ds. cyberbezpieczeństwa oraz specjalisty ds. NIS-2 | 956 188,00 zł | Audyt bezpieczeństwa Biznes.gov.pl jest kluczowy dla ochrony danych użytkowników oraz zgodności z wymaganiami prawnymi systemu Biznes.gov.pl. Specjalista ds. cyberbezpieczeństwa pełni kluczową rolę merytoryczną w zakresie wiedzy z obszaru projektowanych e-usług. |
| Wydajność rozwiązań | 1. Zlecenie wykonania audytu wydajności systemu. 2. Koszty osobowe Analityka systemowego. | 498 094,00 zł | Audyt wydajności dla weryfikacji czy system Biznes.gov.pl funkcjonuje optymalnie, co minimalizuje ryzyko przestojów i problemów z wydajnością, szczególnie przy zwiększonym obciążeniu po wdrożeniu nowych funkcjonalności. Analityk systemowy dla wdrożenia budowanych usług zgodnie z architekturą systemu Biznes.gov.pl. |
| Szkolenia | | | |
| Działania informacyjno-promocyjne | 1. Opracowanie key visual projektu 2. Organizacja info-webinarów dla przedsiębiorców 3. Przygotowanie cyfrowych materiałów informacyjnych dot. produktów projektu | 246 000,00 zł | Budowanie rozpoznawalności i świadomości istnienia projektowanych e-usług oraz skuteczne dotarcia do grupy docelowej z informacjami o projekcie i jego korzyściach zwiększa zaangażowanie wśród przedsiębiorców. Dzięki tym działaniom, projekt zyska większą widoczność, co przełoży się na szersze wykorzystanie udostępnionych usług a tym samym osiągnięcie celu stawianego w projekcie |
| Koszty zarządzania i wsparcia (w tym wynagrodzenia personelu wspomagającego) | Koszty osobowe zarządu kierownika i zastępcy kierownika projektu, asystenta. | 1 374 282,00 zł | Koszty osobowe zarządu kierownika, zastępcy kierownika projektu oraz asystenta są niezbędne do skutecznego zarządzania projektem, koordynacji działań zespołu oraz zapewnienia terminowej realizacji zadań. Kierownictwo projektu jest |

| Nazwa pozycji kosztowej | | Przewidywany koszt brutto | Uzasadnienie pozycji kosztowej (przeznaczenie) |
|-------------------------|--|---------------------------|--|
| | | | kluczowe dla podejmowania strategicznych decyzji, zarządzania ryzykiem oraz monitorowania postępów. Asystent wspiera administracyjnie procesy, co pozwala na efektywniejsze wykorzystanie zasobów i koncentrację na kluczowych zadaniach projektu. |

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

| Całkowity koszt utrzymania trwałości projektu (brutto) | 1 325 363,40 zł | | Źródło finansowania |
|---|-----------------|---|---|
| Podział całkowitego kosztu utrzymania trwałości projektu na poszczególne lata (netto oraz brutto) | 2026 | 150 000,00 zł (brutto) (121 951,22 zł netto) | krajowe środki publiczne - budżet państwa |
| | 2027 | 315 000,00 zł (brutto) (256 097,56 zł netto) | krajowe środki publiczne - budżet państwa |
| | 2028 | 330 750,00 zł (brutto) (268 902,44 zł netto) | krajowe środki publiczne - budżet państwa |
| | 2029 | 347 287,50 zł (brutto) (282 347,56 zł netto) | krajowe środki publiczne - budżet państwa |
| | 2030 | 182 325,90 zł (brutto) (148 232,50 zł netto) | krajowe środki 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 |
|---|--------------------|---------------------------------------|--|
| Brak wystarczających środków na realizację projektu | Duża | Średnie | <ol style="list-style-type: none"> 1. Opracowanie architektury rozwiązania wraz z planem nakładów i kosztów realizacji produktów projektu. 2. Stała kontrola pracochłonności wytwarzania oprogramowania. 3. Bieżący monitoring poziomu realizacji nakładów i kosztów w kontekście przyjętych założeń. |
| Nieosiągnięcie wskaźników projektu oraz celu projektu | Średnia | Niskie | <ol style="list-style-type: none"> 1. Bieżący, regularny monitoring wskaźników postępu w projekcie. 2. Transparentna komunikacja z interesariuszami oraz elastyczność w dostosowywaniu planów. 3. Cykliczny monitoring harmonogramu realizacji produktów w projekcie. 4. Elastyczne zarządzanie zasobami. 5. Eskalowanie problemów na poziom kierownictwa instytucji. 6. Systematyczność w podejściu do zarządzania ryzykiem pozwoli na minimalizowanie negatywnego wpływu na projekt i zwiększenie szans na osiągnięcie założonych celów. |
| Brak możliwości integracji systemów informatycznych | Średnia | Niskie | <ol style="list-style-type: none"> 1. Inwentaryzacja systemów i rozwiązań połączeń międzysystemowych. 2. Analiza technologii i standardów wymiany danych w systemach informatycznych. 3. Opracowanie architektury współpracy systemów i wymiany danych. |
| Zaburzenia w komunikacji w ramach projektu | Mała | Niskie | <ol style="list-style-type: none"> 1. Opracowania planu komunikacji w projekcie. 2. Cykliczne raportowanie zgodne z Planem komunikacji w zakresie statusu projektu, oraz ryzyk. |
| Brak wystarczających zasobów kadrowych do realizacji projektu | Mała | Niskie | <ol style="list-style-type: none"> 1. Zaangażowanie do realizacji projektów członków zespołu projektowego MRiT oraz NASK. 2. Elastyczne zarządzanie zasobami. |
| Przekroczenie harmonogramu realizacji projektu | Duża | Wysokie | <ol style="list-style-type: none"> 1. Opracowanie planu i harmonogramu realizacji poszczególnych zadań w projekcie. 2. Bieżący monitoring harmonogramu |

| Nazwa ryzyka | Siła oddziaływania | Prawdopodobieństwo wystąpienia ryzyka | Sposób zarządzania ryzykiem |
|---|--------------------|---------------------------------------|---|
| | | | realizacji projektu. 3. Elastyczne zarządzanie zasobami. 4. Skuteczna komunikacja z interesariuszami. |
| Brak strategicznych decyzji projektowych lub opóźnienia w ich uzyskaniu | Duża | Niskie | 1. Reprezentatywna i decyzyjna struktura Komitetu Sterującego projektu. 2. Eskalowanie problemów na poziom kierownictwa instytucji. 3. Cykliczne raportowanie zgodne z Planem komunikacji w zakresie statusu projektu, decyzji koniecznych do podjęcia oraz ryzyk. |
| Brak zainteresowania przedsiębiorców udostępnionymi usługami | Duża | Wysokie | W projekcie zaplanowano działania informacyjne skierowane do MŚP, wsparte synergią z projektem "Kampania edukacyjno-informacyjna dla przedsiębiorców, upowszechniająca korzyści płynące z technologii cyfrowych" finansowanym z Funduszy Europejskich na Rozwój Cyfrowy (FERC), działanie 2.5, gdzie jednym z podstawowych problemów zidentyfikowanych w ramach projektu jest niewystarczająca liczba przedsiębiorstw posiadająca wysoki poziom cyberbezpieczeństwa a planowane działania mające zwiększać poziom cyberbezpieczeństwa MŚP obejmują m.in. kampanie edukacyjno-informacyjne, kampanie internetowe oraz kampanie PR. |

5.2. Ryzyka wpływające na utrzymanie efektów

| Nazwa ryzyka | Siła oddziaływania | Prawdopodobieństwo wystąpienia ryzyka | Sposób zarządzania ryzykiem |
|---|--------------------|---------------------------------------|---|
| Brak wystarczających zasobów finansowych do utrzymania i eksploatacji produktów | Średnia | Niskie | 1. Analiza niezbędnych zasobów oraz źródła finansowania eksploatacji produktów końcowych projektu po ich wdrożeniu i zakończeniu projektu. 2. Zaplanowanie źródła i wysokości finansowania utrzymania i eksploatacji produktów końcowych projektu w planie |

| Nazwa ryzyka | Siła oddziaływania | Prawdopodobieństwo wystąpienia ryzyka | Sposób zarządzania ryzykiem |
|---|--------------------|---------------------------------------|--|
| końcowych projektu. | | | budżetowym po 2029 r. 3. Monitorowanie kosztów utrzymania i eksploatacji produktów końcowych projektu |
| Bardzo duży poziom wykorzystania uruchomionych usług elektronicznych przez grupy docelowe | Średnia | Niskie | 1. Dokonanie dokładnej inwentaryzacji zasobów teleinformatycznych i określenie ich wydajności. 2. Rozbudowa w celu umożliwienia przyjęcia większej liczby użytkowników niż zakładana na etapie projektowania. |

6. OTOCZENIE PRAWNE

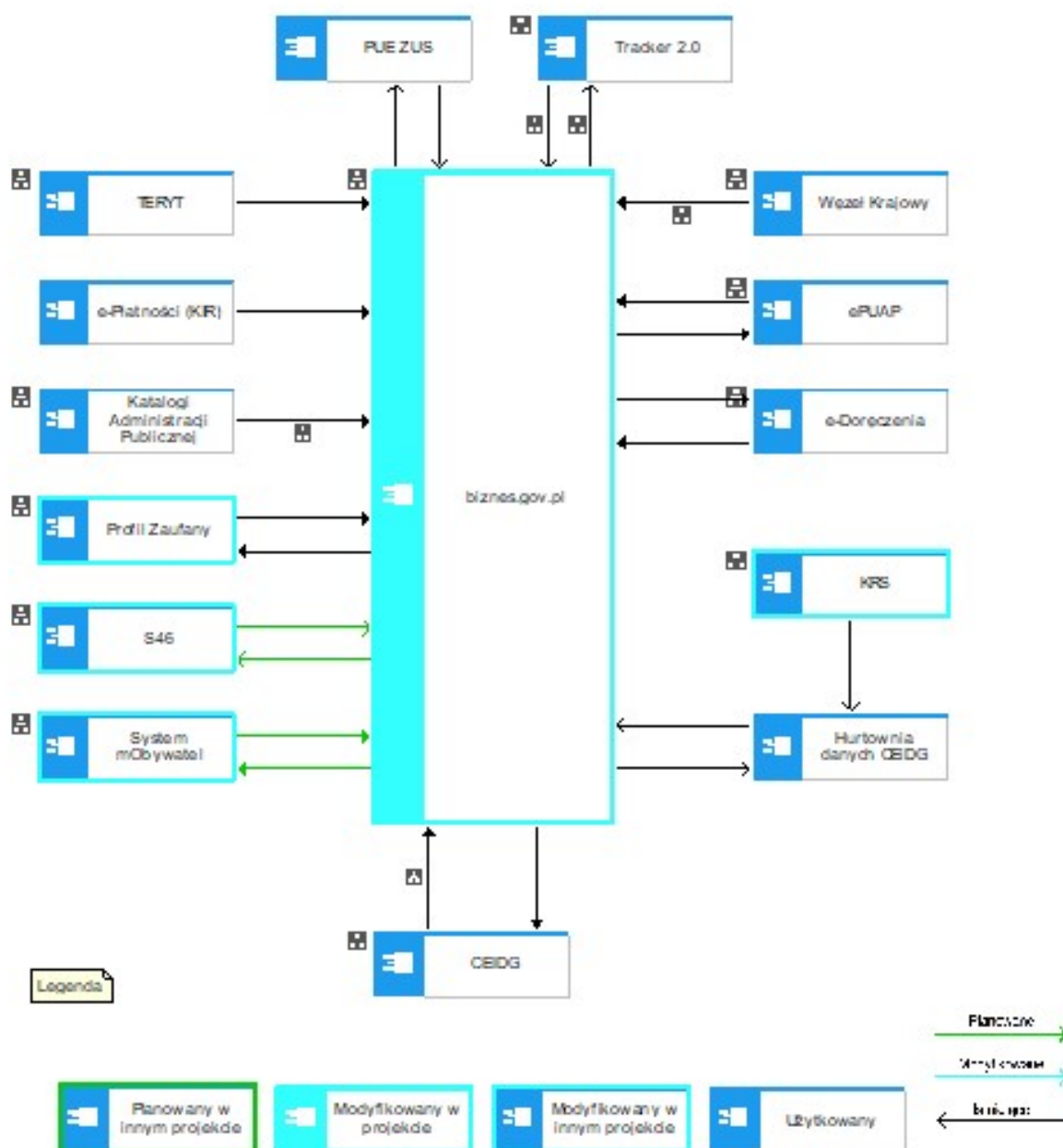
| Lp. | Tytuł aktu prawnego | Czy wymaga zmian | Opis zmian (jeśli dotyczy) | Etap prac legislacyjnych (jeśli dotyczy) |
|-----|---|------------------|----------------------------|--|
| 1 | Dyrektywa Parlamentu Europejskiego i Rady (UE) 2022/2555 z dnia 14 grudnia 2022 r. w sprawie środków na rzecz wysokiego wspólnego poziomu cyberbezpieczeństwa na terytorium Unii, zmieniająca rozporządzenie (UE) nr 910/2014 i dyrektywę (UE) 2018/1972 oraz uchylająca dyrektywę (UE) 2016/1148 (dyrektywa NIS 2) | TAK/NIE | | |
| 2 | Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2023/2854 z dnia 13 grudnia 2023 r. w sprawie zharmonizowanych przepisów dotyczących sprawiedliwego dostępu do danych i ich wykorzystywania oraz w sprawie zmiany rozporządzenia (UE) 2017/2394 i dyrektywy (UE) 2020/1828 (akt w sprawie danych) | TAK/NIE | | |
| 3 | Rozporządzenie Parlamentu Europejskiego i Rady w sprawie horyzontalnych wymogów cyberbezpieczeństwa w odniesieniu do produktów z elementami cyfrowymi i zmieniające rozporządzenie (UE) 2019/1020 (Cyber Resilience Act) | TAK/NIE | | |
| 4 | Ustawa z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa | TAK/NIE | | |

| Lp. | Tytuł aktu prawnego | Czy wymaga zmian | Opis zmian (jeśli dotyczy) | Etap prac legislacyjnych (jeśli dotyczy) |
|-----|---|------------------|----------------------------|--|
| 5 | Ustawa z dnia 17 lutego 2005 r. o informatyzacji działalności podmiotów realizujących zadania publiczne | TAK/NIE | | |
| 6 | Rozporządzenie Rady Ministrów z dnia 21 maja 2024 r. w sprawie Krajowych Ram Interoperacyjności, minimalnych wymagań dla rejestrów publicznych i wymiany informacji w postaci elektronicznej oraz minimalnych wymagań dla systemów teleinformatycznych | TAK/NIE | | |
| 7 | Ustawa z dnia 27 lipca 2001 r. o ochronie baz danych | TAK/NIE | | |
| 8 | Ustawa z dnia 11 sierpnia 2021 r. o otwartych danych i ponownym wykorzystywaniu informacji sektora publicznego | TAK/NIE | | |
| 9 | Ustawa z dnia 4 kwietnia 2019 r. o dostępności cyfrowej stron internetowych i aplikacji mobilnych podmiotów publicznych | TAK/NIE | | |
| 10 | Ustawa z dnia 7 maja 2010 r. o wspieraniu rozwoju usług i sieci telekomunikacyjnych | TAK/NIE | | |
| 11 | Ustawa z dnia 18 listopada 2020 r. o doręczeniach elektronicznych | TAK/NIE | | |
| 12 | Ustawa z dnia 5 września 2016 r. o usługach zaufania oraz identyfikacji elektronicznej | TAK/NIE | | |
| 13 | Rozporządzenie Ministra Cyfryzacji z dnia 29 czerwca 2020 r. w sprawie profilu zaufanego i podpisu zaufanego | TAK/NIE | | |
| 14 | Rozporządzenie Ministra Cyfryzacji z dnia 5 października 2016 r. w sprawie szczegółowych warunków organizacyjnych i technicznych, które powinien spełniać system teleinformatyczny służący do uwierzytelniania użytkowników | TAK/NIE | | |
| 15 | Ustawa z dnia 10 maja 2018 r. o ochronie danych osobowych | TAK/NIE | | |
| 16 | Rozporządzenie Prezesa Rady Ministrów z dnia 20 lipca 2011 r. w sprawie podstawowych wymagań bezpieczeństwa teleinformatycznego | TAK/NIE | | |
| 17 | Obwieszczenie Prezesa Rady Ministrów z dnia 5 stycznia 2018 r. w sprawie ogłoszenia jednolitego tekstu rozporządzenia Prezesa Rady Ministrów w sprawie sporządzania i doręczania dokumentów elektronicznych oraz udostępniania formularzy, wzorów i kopii | TAK/NIE | | |

| Lp. | Tytuł aktu prawnego | Czy wymaga zmian | Opis zmian (jeśli dotyczy) | Etap prac legislacyjnych (jeśli dotyczy) |
|-----|---|------------------|----------------------------|--|
| | dokumentów elektronicznych | | | |
| 18 | Ustawa z dnia 14 lipca 1983 r. 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 | Biznes.gov.pl | Ministerstwo Rozwoju i Technologii | <p>Biznes.gov.pl to serwis przeznaczony dla osób zamierzających rozpocząć i prowadzących działalność gospodarczą. Celem portalu jest pomoc w realizacji spraw związanych z zakładaniem i prowadzeniem i zamykaniem działalności oraz udostępnienie narzędzi upraszczających formalny proces założenia i prowadzenia firmy.</p> <p>W serwisie dostępne są opisy usług publicznych oraz formularze pozwalające na ich realizację w sposób zdalny. Za pomocą serwisu, osoby prowadzące firmę mogą składać wnioski do instytucji państwowych drogą elektroniczną, a także załatwiać swoje biznesowe sprawy przez internet. Serwis łączy w sobie wiele usług i funkcji nie tylko dla przedsiębiorców, ale także dla administracji państwowej. Przedsiębiorcy znajdą tutaj szczegółowe informacje o obowiązujących przepisach prawa, wymaganych procedurach i formalnościach związanych z zakładaniem i prowadzeniem działalności gospodarczej w Polsce oraz odniesienie do analogicznych informacji dotyczących pozostałych krajów Unii Europejskiej. Serwis spełnia też rolę wyszukiwarki danych kontaktowych wszystkich instytucji obsługujących przedsiębiorców. Daje praktyczne instrukcje, jak</p> | Modyfikowany | <p>Modyfikacja systemu Biznes.gov.pl będzie polegać na stworzeniu w module Konto Przedsiębiorcy funkcjonalność i Bezpieczna Firma, która będzie umożliwiać dostęp do spersonalizowanych: wyników analizy poziomu cyberbezpieczeństwa firmy wraz z rekomendacjami i w zakresie podstawowych wymagań z obszaru cyberbezpieczeństwa, które firma musi wdrożyć; deklaracji zgodności produktów dostarczanych przez firmę z wymaganiami CRA oraz rekomendacji i planu działania w zakresie dostosowania do wymagań dyrektywy NIS2.</p> |

| Lp. | Nazwa systemu | Gestor systemu | Opis systemu | Status | Krótki opis ewentualnej zmiany |
|-----|---------------|------------------------------------|--|------------|--------------------------------|
| | | | sobie radzić w biznesie, i umożliwia realizację spraw administracyjnych drogą elektroniczną. | | |
| 2 | CEIDG | Ministerstwo Rozwoju i Technologii | System, w którym prowadzona jest centralna ewidencja działalności gospodarczej (CEIDG). Zadaniem systemu jest umożliwienie rejestracji działalności gospodarczej drogą elektroniczną oraz zgłaszania informacji o zmianach danych, zawieszeniu lub wznowieniu oraz zaprzestaniu wykonywania działalności. System CEIDG umożliwia składanie wniosku o wpis do CEIDG oraz do innych urzędów (Urzędy Skarbowe, ZUS/KRUS, GUS). CEIDG udostępnia również informacje o przedsiębiorcach oraz uzyskanych przez nich licencjach, koncesjach lub zezwoleniach. | Istniejący | |
| 3 | e-Doręczenia | Ministerstwo Cyfryzacji | e-Doręczenia – zapewnia działanie usługi rejestrowanego doręczenia elektronicznego. Celem systemu jest zapewnienie narzędzia umożliwiającego podmiotom sektora publicznego, obywatelom i przedsiębiorcom bezpieczne doręczenie elektroniczne, równoważne prawnie z tradycyjną przesyłką poleconą za potwierdzeniem odbioru, zachowujące jednocześnie zgodność z obowiązkami nałożonymi na państwa członkowskie UE, wskazanymi w obowiązujących przepisach i dyrektywach unijnych, w szczególności zgodnego z | Istniejący | |

| Lp. | Nazwa systemu | Gestor systemu | Opis systemu | Status | Krótki opis ewentualnej zmiany |
|-----|------------------------|------------------------------------|---|------------|--------------------------------|
| | | | ustaleniami Tallinn Declaration on eGovernment i wymogami kwalifikowanych usług rejestrowanego doręczenia elektronicznego z Rozporządzenia Parlamentu Europejskiego i Rady (UE) NR 910/2014 z dnia 23 lipca 2014 r. w sprawie identyfikacji elektronicznej i usług zaufania w odniesieniu do transakcji elektronicznych na rynku wewnętrznym nazywanego Rozporządzeniem eIDAS . | | |
| 4 | ePUAP | Ministerstwo Cyfryzacji | ePUAP (elektroniczna Platforma Usług Administracji Publicznej) – ogólnopolska platforma teleinformatyczna służąca do komunikacji obywateli i przedsiębiorców z jednostkami administracji publicznej w ujednolicony, standardowy sposób. Platforma służy również do komunikacji pomiędzy jednostkami administracji publicznej. Usługodawcami są podmioty administracji publicznej oraz inne podmioty wykonujące zadania publiczne zlecone lub powierzone im do realizacji. | Istniejący | |
| 5 | e-Płatności (KIR) | Krajowa Izba Rozliczeniowa | Platforma do realizacji transakcji płatności elektronicznych obsługiwana przez KIR | Istniejący | |
| 6 | Hurtownia danych CEIDG | Ministerstwo Rozwoju i Technologii | Hurtownia danych CEIDG i Biznes.gov.pl to zbiór informacji o przedsiębiorcach zarejestrowanych w Centralnej Ewidencji i Informacji o Działalności Gospodarczej (CEIDG). Informacje o przedsiębiorcach | Istniejący | |

| Lp. | Nazwa systemu | Gestor systemu | Opis systemu | Status | Krótki opis ewentualnej zmiany |
|-----|----------------------------------|-------------------------|---|------------|--------------------------------|
| | | | <p>udostępniane są bezpłatnie dla użytkowników, którzy przejdą procedurę rejestracji. Hurtownia danych CEIDG i Biznes.gov.pl, dostępna jest pod adresem dane.biznes.gov.pl. W skład Hurtowania danych CEIDG i Biznes.gov.pl wchodzi:</p> <ol style="list-style-type: none"> 1. Aplikacja Raportowa, która umożliwia użytkownikom dostęp do predefiniowanych raportów. 2. Repozytorium Raportów umożliwiające dostęp do wcześniej wygenerowanych i gotowych do pobrania predefiniowanych raportów. 3. Moduł do zarządzania API. Moduł umożliwia zarządzanie interfejsami API można m.in.: tworzyć interfejsy API, zarządzać dostępem do interfejsów API, monitorować logi dostępowe do interfejsów API. | | |
| 7 | Katalog Administracji Publicznej | Ministerstwo Cyfryzacji | <p>System teleinformatyczny zawierający referencyjne rejestry na potrzeby świadczenia usług publicznych. System zawiera i udostępnia informacje o obiektach takich jak: podmioty świadczące usługi publiczne, rejestry publiczne, usługi publiczne i wzory dokumentów wykorzystywane w świadczeniu usług publicznych. Katalog Administracji Publicznej to system teleinformatyczny, w którym utrzymywane jest centralne, referencyjne repozytorium rejestrów, które będą udostępniały przez API</p> | Istniejący | |

| Lp. | Nazwa systemu | Gestor systemu | Opis systemu | Status | Krótki opis ewentualnej zmiany |
|-----|---------------|------------------------------|---|--------------|---------------------------------------|
| | | | ustandaryzowaną, spójną, wiarygodną i kompletną informację na potrzeby świadczenia e-usług publicznych przez polskie podmioty. KAP jest istotnym komponentem przewidzianym w Wizji Architektury Informacyjnej Państwa, elementem zmodernizowanej elektronicznej platformy usług administracji (ePUAP) określonej w Ustawie o Informatyzacji Podmiotów Publicznych. | | |
| 8 | KRS | Ministerstwo Sprawiedliwości | Krajowy Rejestr Sądowy jest systemem, który służy do prowadzenia rejestru KRS - jednego z najważniejszych rejestrów państwa, w którym rejestrowani są przedsiębiorcy będący osobami prawnymi (inni niż jednoosobowa działalność gospodarcza), stowarzyszenia oraz inne wybrane podmioty. System umożliwia zawieranie oraz podejmowanie innych czynności w odniesieniu do spółek, których umowa jest zawierana przy wykorzystaniu wzorca umowy udostępnionego w tym systemie, oraz podejmowanie czynności w postępowaniu rejestrowym w odniesieniu do podmiotów podlegających wpisowi do Rejestru, udzielanie informacji z Rejestru i udostępnianie akt rejestrowych. System KRS udostępnia dane referencyjne z rejestru KRS w postaci odpisów aktualnych i pełnych. Odpis z | Modyfikowany | System modyfikowany w innym projekcie |

| Lp. | Nazwa systemu | Gestor systemu | Opis systemu | Status | Krótki opis ewentualnej zmiany |
|-----|----------------|-------------------------|--|--------------|--|
| | | | KRS to zestawienie informacji w określonej strukturze zawartych w rejestrze KRS, w przypadku odpisu pełnego prezentowane są wszystkie wpisy sądu rejestrowego dotyczące podmiotu począwszy od jego rejestracji, czyli zmieniane adresy siedziby, zmiany członków zarządów i rad nadzorczych itd. Odpis aktualny z KRS prezentuje dane aktualne na chwilę pobrania odpisu (aktualna siedziba, aktualny skład organów reprezentacji i nadzoru itd.). | | |
| 9 | Profil Zaufany | Ministerstwo Cyfryzacji | <p>Profil Zaufany to system, który:</p> <ol style="list-style-type: none"> 1) zapewnia obsługę publicznego systemu identyfikacji elektronicznej, w którym wydawany jest profil zaufany, 2) umożliwia podmiotom publicznym: <ol style="list-style-type: none"> a) uwierzytelnienie osoby fizycznej przy użyciu środka identyfikacji elektronicznej - profilu zaufanego b) zapewnienie osobie fizycznej możliwości opatrzenia dokumentu elektronicznego podpisem zaufanym. <p>W systemie przetwarza się następujące dane:</p> <ol style="list-style-type: none"> 1) osoby, której wydano środek identyfikacji elektronicznej, obejmujące : <ol style="list-style-type: none"> a) imię (imiona), b) nazwisko, c) numer PESEL, d) datę urodzenia osoby, e) adres poczty elektronicznej, f) numer telefonu | Modyfikowany | System modyfikowany w innym projekcie realizowanym przez COI |

| Lp. | Nazwa systemu | Gestor systemu | Opis systemu | Status | Krótki opis ewentualnej zmiany |
|-----|---------------|----------------|--|--------|--------------------------------|
| | | | <p>komórkowego;</p> <p>2)dotyczące środka identyfikacji elektronicznej obejmujące:</p> <p>a)identyfikator,</p> <p>b)czas wydania,</p> <p>c)termin ważności;</p> <p>3)o których mowa w art. 20ab pkt 2.(informacje związane z zapewnieniem rozliczalności i niezaprzeczalności działań użytkownika korzystającego ze środka identyfikacji elektronicznej wydanego w publicznym systemie identyfikacji elektronicznej)</p> <p>3. Dane przetwarzane są w celu zapewnienia uwierzytelnienia osób fizycznych przy użyciu środków identyfikacji elektronicznej wydawanych w tym systemie oraz możliwości opatrzenia dokumentu elektronicznego podpisem zaufanym.</p> <p>4. W systemie przetwarza się również dane osób uczestniczących w procesie potwierdzania profilu zaufanego obejmujące:</p> <p>1)imię (imiona);2)nazwisko;3)numer PESEL.</p> <p>Dane 2. 1) a-b są weryfikowane na zgodność z rejestrem PESEL. Dane e-f mogą być inne niż dane w RDK (e-mail służy do kontaktu z użytkownikiem (unieważnienie PZ), telefon jest wykorzystywany do autoryzacji - może być inny niż telefon do kontaktów z administracją publiczną). Profil zaufany jest publicznym środkiem identyfikacji elektronicznej. Jest to potwierdzony zestaw</p> | | |

| Lp. | Nazwa systemu | Gestor systemu | Opis systemu | Status | Krótki opis ewentualnej zmiany |
|-----|---------------|-------------------------|--|--------------|---|
| | | | danych, które jednoznacznie identyfikują jego posiadacza w usługach podmiotów publicznych w internecie. Profil zaufany i podpis zaufany jest to ten sam zestaw danych, potwierdzony jednym certyfikatem ministra wł. ds cyfryzacji | | |
| 10 | S46 | Ministerstwo Cyfryzacji | <p>Zintegrowany system zarządzania cyberbezpieczeństwem, System realizujący założenia systemu teleinformatycznego z art. 46 ust. 1 Ustawy Zgodnie z art. 46 ust. 1 ustawy z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa (Dz. U. z 2018 r., poz. 1560t.j. Dz. U. z 2020 r. poz. 1369) minister właściwy do spraw informatyzacji zapewnia rozwój lub utrzymanie systemu teleinformatycznego wspierającego:</p> <ol style="list-style-type: none"> 1) współpracę podmiotów wchodzących w skład krajowego systemu cyberbezpieczeństwa; 2) generowanie i przekazywanie rekomendacji dotyczących działań podnoszących poziom cyberbezpieczeństwa; 3) zgłaszanie i obsługę incydentów; 4) szacowanie ryzyka na poziomie krajowym; 5) ostrzeganie o zagrożeniach cyberbezpieczeństwa. <p>Zgodnie z art. 89 ustawy minister właściwy do spraw informatyzacji uruchomi system teleinformatyczny, o</p> | Modyfikowany | System modyfikowany w innym projekcie realizowanym przez NASK |

| Lp. | Nazwa systemu | Gestor systemu | Opis systemu | Status | Krótki opis ewentualnej zmiany |
|-----|------------------|---------------------------|---|--------------|--|
| | | | <p>którym mowa w art. 46 ust. 1 ww. ustawy, do dnia 1 stycznia 2021 r. System ten będzie określany mianem „System 46” lub „S46”. Za podstawę do wytwarzania w projekcie produktów systemu S46 będą służyć rozwiązania własne NASK PIB oraz dostępne technologie.</p> <p>Docelowo zostanie wytworzony system Platformy Analitycznej S46, który będzie realizować zadania wskazane w ustawie o krajowym systemie cyberbezpieczeństwa.</p> <p>Docelowo system, zapewni pracę trzech CSIRT tj.: CSIRT GOV, CSIRT MON i CSIRT NASK na Platformie Analitycznej S46. Celem zadania jest wytworzenie i uruchomienie pierwszego wydania Systemu S46.</p> | | |
| 11 | TERYT | Główny Urząd Statystyczny | System teleinformatyczny służący do prowadzenia rejestru TERYT | Istniejący | |
| 12 | System mObywatel | Ministerstwo Cyfryzacji | <p>System mObywatel to system teleinformatyczny zapewniający funkcjonalności niezbędne do działania aplikacji mObywatel oraz usług udostępnianych w tej aplikacji.</p> <p>System pozwala, przy użyciu publicznej aplikacji mobilnej, na pobranie i prezentację dokumentów elektronicznych i usług. Dane prezentowane w dokumentach i usługach pochodzą m.in. z rejestrów państwowych oraz innych systemów teleinformatycznych podmiotów</p> | Modyfikowany | System modyfikowany w innym projekcie realizowanym przez COI |

| Lp. | Nazwa systemu | Gestor systemu | Opis systemu | Status | Krótki opis ewentualnej zmiany |
|-----|---------------|--------------------------------|--|------------|--------------------------------|
| | | | <p>współpracujących z systemem mObywatel. System mObywatel składa się z front-endu (Publicznej Aplikacji Mobilnej, mWeryfikatora, Portalu dla Szkół i Uczelni oraz Portalu Administracyjnego) oraz back-endu.</p> <p>System mObywatel to system teleinformatyczny, który pozwala, przy użyciu publicznej aplikacji mobilnej, na pobranie dokumentu elektronicznego:</p> <p>1) zawierającego dane osobowe użytkownika publicznej aplikacji mobilnej pobrane z rejestrów publicznych;</p> <p>2) zawierającego dane dotyczące sytuacji prawnej użytkownika publicznej aplikacji mobilnej lub praw mu przysługujących;</p> <p>3) zawierającego dane umożliwiające identyfikację rzeczy związanej z użytkownikiem publicznej aplikacji mobilnej;</p> <p>4) stanowiącego kopię dokumentu urzędowego, który wydawany jest w postaci innej niż postać elektroniczna.</p> | | |
| 13 | PUE ZUS | Zakład Ubezpieczeń Społecznych | <p>Platforma Usług Elektronicznych (PUE). PUE udostępnia on-line dane zapisane na kontach w ZUS, daje możliwość łatwego generowania i przesyłania drogą elektroniczną dokumentów zgłoszeniowych i rozliczeniowych oraz różnego typu pism i wniosków. Tą drogą można również umówić się na wizytę w ZUS.</p> | Istniejący | |

| Lp. | Nazwa systemu | Gestor systemu | Opis systemu | Status | Krótki opis ewentualnej zmiany |
|-----|---------------|------------------------------------|---|------------|--------------------------------|
| 14 | TRACKER 2.0 | Ministerstwo Rozwoju i Technologii | System wydawania pozwoleń na obrót towarami wrażliwymi, w ramach którego obsługiwana będzie nowa e-usługa typu A2B - złożenie wniosku o zezwolenie na obrót z zagranicą towarami wrażliwymi oraz otrzymanie decyzji urzędu. | Istniejący | |
| 15 | Węzeł Krajowy | Ministerstwo Cyfryzacji | <p>Węzeł Krajowy jest rozwiązaniem organizacyjno-technicznym umożliwiającym uwierzytelnianie użytkownika systemu teleinformatycznego, korzystającego z usługi online, z wykorzystaniem środka identyfikacji elektronicznej wydanego w systemie identyfikacji elektronicznej przyłączonym do tego węzła bezpośrednio albo za pośrednictwem Węzła Transgranicznego. Zapewnia osobie chcącej skorzystać z publicznych usług online wybór, najwygodniejszego dla niej, sposobu potwierdzenia jej tożsamości</p> <p>Do Węzła Krajowego przyłączane są:</p> <ul style="list-style-type: none"> * systemy identyfikacji elektronicznej (za które odpowiada podmiot posiadający siedzibę na terenie jednego z państw członkowskich Unii Europejskiej po spełnieniu warunków określonych w Ustawie o środkach zaufania). * systemy udostępniające usługi online (usługa określa, jaki środek identyfikacji jest dla niej odpowiedni) | Istniejący | |

| Lp. | Nazwa systemu | Gestor systemu | Opis systemu | Status | Krótki opis ewentualnej zmiany |
|-----|---------------|----------------|--|--------|--------------------------------|
| | | | <p>Węzeł Krajowy pełni główną rolę zarządczą w sfederowanym modelu tożsamości w Polsce, w szczególności skupia wszystkie akredytowane systemy identyfikacji w Polsce, a także jest pośrednikiem między węzłami komercyjnymi, węzłem transgranicznym i dostawcami usługi.</p> <p>Węzeł Krajowy umożliwia:</p> <ul style="list-style-type: none"> ☒ Wybór Dostawcy środka identyfikacji elektronicznej ☒ Przekierowanie do zagranicznych i notyfikowanych Dostawców środków identyfikacji elektronicznej ☒ Mechanizm pobierania dodatkowych atrybutów do Dostawcy Atrybutów i ich agregacji ☒ Potwierdzenie uwierzytelnienia u Dostawcy środka identyfikacji elektronicznej ☒ Zarządzanie połączeniami do Węzła <p>System nie przechowuje danych uwierzytelniających się osób fizycznych wykorzystujących środki identyfikacji elektronicznej, jest jedynie pośrednikiem między systemami identyfikacji elektronicznej a systemami udostępniającymi usługi online. Przechowuje jedynie w logi.</p> <p>System przetwarza jedynie dane obowiązkowe z całkowitego zakresu określonego w ustawie o identyfikacji (zgodnego z eIDAS)</p> | | |

Lista przepływów

| Lp. | System źródłowy | System docelowy | Zakres wymienianych danych | Sposób wymiany danych | Typ modyfikacji | Typ interfejsu |
|-----|-----------------------------------|-----------------|--|----------------------------|-----------------|----------------|
| 1 | e-Płatności (KIR) | Biznes.gov.pl | Dane transakcyjne e-płatności | tryb odwołań bezpośrednich | Użytkowany | API |
| 2 | CEIDG | Biznes.gov.pl | Dane firm z CEIDG, status spraw CEIDG, lista firm z CEIDG i KRS spełniająca kryteria wyszukiwania | Tryb odwołań bezpośrednich | Użytkowany | API |
| 3 | Hurtownia danych CEIDG | Biznes.gov.pl | Dane firm z CEIDG i KRS | tryb odwołań bezpośrednich | Użytkowany | API |
| 4 | e-Doręczenia | Biznes.gov.pl | Korespondencja, Informacja o statusie wniosku BAE. | tryb odwołań bezpośrednich | Użytkowany | API |
| 5 | S46 | Biznes.gov.pl | Dane dot. włączenia firmy w skład podmiotów krajowego systemu cyberbezpieczeństwa | tryb odwołań bezpośrednich | Planowany | API |
| 6 | Katalogi Administracji Publicznej | Biznes.gov.pl | Dane podmiotów publicznych | tryb odwołań bezpośrednich | Użytkowany | API |
| 7 | TERYT | Biznes.gov.pl | Adres | tryb odwołań bezpośrednich | Użytkowany | API |
| 8 | Węzeł Krajowy | Biznes.gov.pl | Obsługa żądania identyfikacji i uwierzytelnienia osoby fizycznej, która się loguje do systemu biznes.gov.pl za pośrednictwem węzła | tryb odwołań bezpośrednich | Użytkowany | API |

| Lp. | System źródłowy | System docelowy | Zakres wymienianych danych | Sposób wymiany danych | Typ modyfikacji | Typ interfejsu |
|-----|-----------------|------------------|--|----------------------------|-----------------|----------------|
| | | | krajowego - dane osoby fizycznej, zawarte w środku identyfikacji elektronicznej. Dane mogą być wykorzystane biznesowo - np. w usługach online realizowanych na platformie biznes.gov.pl - np. do uzupełniania wniosku. | | | |
| 9 | Tracker 2.0 | Biznes.gov.pl | Status postępowań, status zezwoleń (aktywne/ historyczne/ modyfikowane) , parametry zezwoleń | tryb odwołań bezpośrednich | Użytkowany | API |
| 10 | Biznes.gov.pl | Profil Zaufany | Dokument do podpisania lub dokument do weryfikacji poprawności podpisu na dokumencie | tryb odwołań bezpośrednich | Użytkowany | API |
| 11 | Biznes.gov.pl | Tracker 2.0 | Formularze wniosków, dane identyfikacyjne oraz dotyczące przedmiotu zezwoleń | tryb odwołań bezpośrednich | Użytkowany | API |
| 12 | Biznes.gov.pl | System mObywatel | Obsługa żądania identyfikacji i uwierzytelnieni | tryb odwołań bezpośrednich | Planowany | API |

| Lp. | System źródłowy | System docelowy | Zakres wymienianych danych | Sposób wymiany danych | Typ modyfikacji | Typ interfejsu |
|-----|-----------------|-----------------|--|----------------------------|-----------------|----------------|
| | | | a osoby fizycznej, która się loguje do systemu biznes.gov.pl za pośrednictwem węzła krajowego - dane osoby fizycznej, zawarte w środku identyfikacji elektronicznej. Dane mogą być wykorzystane biznesowo - np. w usługach online realizowanych na platformie biznes.gov.pl - np. do uzupełniania wniosku. | | | |
| 13 | Biznes.gov.pl | PUE ZUS | Obsługa żądania identyfikacji i uwierzytelnienia osoby fizycznej, która się loguje do systemu biznes.gov.pl za pośrednictwem węzła krajowego wraz z identyfikacją | tryb odwołań bezpośrednich | Użytkowany | API |
| 14 | Profil Zaufany | Biznes.gov.pl | Podpisany dokument lub weryfikacja poprawności podpisu na dokumencie | tryb odwołań bezpośrednich | Użytkowany | API |

| Lp. | System źródłowy | System docelowy | Zakres wymienianych danych | Sposób wymiany danych | Typ modyfikacji | Typ interfejsu |
|-----|------------------|------------------------|---|----------------------------|-----------------|----------------|
| 15 | System mObywatel | Biznes.gov.pl | Obsługa żądania identyfikacji i uwierzytelnienia osoby fizycznej, która się loguje do systemu biznes.gov.pl za pośrednictwem węzła krajowego - dane osoby fizycznej, zawarte w środku identyfikacji elektronicznej. Dane mogą być wykorzystane biznesowo - np. w usługach online realizowanych na platformie biznes.gov.pl - np. do uzupełniania wniosku. | tryb odwołań bezpośrednich | Planowany | API |
| 16 | Biznes.gov.pl | Hurtownia danych CEIDG | Obsługa żądania identyfikacji i uwierzytelnienia osoby fizycznej, która się loguje do systemu biznes.gov.pl za pośrednictwem węzła krajowego wraz z identyfikacją przekazywane są parametry | tryb odwołań bezpośrednich | Użytkowany | API |

| Lp. | System źródłowy | System docelowy | Zakres wymienianych danych | Sposób wymiany danych | Typ modyfikacji | Typ interfejsu |
|-----|-----------------|------------------------|---|----------------------------|-----------------|----------------|
| | | | konta związane z uprawnieniami w systemie. | | | |
| 17 | Biznes.gov.pl | CEIDG | Wnioski do CEIDG, dane statystyczne dotyczące działań użytkowników na Biznes.gov.pl | tryb odwołań bezpośrednich | Użytkowany | API |
| 18 | PUE ZUS | Biznes.gov.pl | Informacja dotyczące obsługi wniosku o niezalegani w składkach ZUS, zaświadczenie o niezaleganiu. | tryb odwołań bezpośrednich | Użytkowany | API |
| 19 | ePUAP | Biznes.gov.pl | Dokumenty odpowiedzi na wnioski eusług | tryb odwołań bezpośrednich | Użytkowany | API |
| 20 | Biznes.gov.pl | ePUAP | Dokumenty wniosków eusług | tryb odwołań bezpośrednich | Użytkowany | API |
| 21 | Biznes.gov.pl | e-Doręczenia | Korespondencja, Webhook dla aktywacji dokumentów BAE | tryb odwołań bezpośrednich | Użytkowany | API |
| 22 | Biznes.gov.pl | S46 | Dane dot. firmy w obszarze podlegania pod NIS2 | tryb odwołań bezpośrednich | Planowany | API |
| 23 | KRS | Hurtownia danych CEIDG | Dane rejestrowe spółek z rejestru KRS. | tryb odwołań bezpośrednich | Użytkowany | API |

7.2. Kluczowe komponenty architektury rozwiązania



7.3. Przyjęte założenia technologiczne

| Lp. | Obszar | Założenie technologiczne |
|-----|------------------------------|--------------------------|
| 1. | Infrastruktura | |
| 2. | Sieć i bezpieczeństwo | |
| 3. | Standardy wymiany danych | |
| 4. | Systemy operacyjne serwerowe | |
| 5. | Bazy danych | |
| 6. | Serwery aplikacji | |
| 7. | Portale | |
| 8. | Inne | |

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?

| Lp. | Rejestr publiczny | Opis | Zakres przetwarzania |
|-----|--|--|----------------------|
| 1 | Centralna Ewidencja i Informacja o Działalności Publicznej | <p>Zgodnie z obowiązującymi przepisami, minister właściwy do spraw gospodarki przy użyciu systemu teleinformatycznego prowadzi: Centralną Ewidencję i Informację o Działalności Gospodarczej (art. 2 ust. 1 ustawy z dnia 6 marca 2018 r. o Centralnej Ewidencji i Informacji o Działalności Gospodarczej i Punkcie Informacji dla Przedsiębiorcy).</p> <p>Rejestr CEIDG</p> <p>Przeznaczenie: Elektroniczny rejestr działający w ramach Systemu Teleinformatycznego Centralnej Ewidencji i Informacji o Działalności Gospodarczej, którego przeznaczeniem jest:</p> <ul style="list-style-type: none"> ewidencjonowanie przedsiębiorców będących osobami fizycznymi; udostępnianie informacji o przedsiębiorcach i innych podmiotach w zakresie wskazanym w ustawie; umożliwienie wglądu do danych bezpłatnie udostępnianych przez Centralną Informację Krajowego Rejestru Sądowego: umożliwienia ustalenia terminu i zakresu zmian wpisów w CEIDG oraz wprowadzającego je organu. | Użycie danych. |
| 2 | Krajowy Rejestr Sądowy (e-KRS) | <p>Krajowy Rejestr Sądowy jest scentralizowaną, informatyczną bazą danych składającą się z trzech osobnych rejestrów:</p> <ul style="list-style-type: none"> -rejestru przedsiębiorców, -rejestru stowarzyszeń, innych organizacji społecznych i zawodowych, fundacji oraz publicznych zakładów opieki zdrowotnej, | Użycie danych. |

| Lp. | Rejestr publiczny | Opis | Zakres przetwarzania |
|-----|-------------------|---|----------------------|
| | | -rejestru dłużników niewypłacalnych. Krajowy Rejestr Sądowy został utworzony w oparciu o ustawę z dnia 20 sierpnia 1997 r. o Krajowym Rejestrze Sądowym i działa od dnia 1 stycznia 2001 r. Zadaniem Krajowego Rejestru Sądowego jest powszechne udostępnienie szybkiej i niezawodnej informacji o statusie prawnym zarejestrowanego podmiotu (Centralna Informacja KRS), najważniejszych elementach jego sytuacji finansowej oraz sposobie jego reprezentowania. | |
| 3 | TERYT | TERYT, Krajowy Rejestr Urzędowy Podziału Terytorialnego Kraju – rejestr urzędowy podziału terytorialnego Polski, prowadzony przez Główny Urząd Statystyczny. | Użycie danych. |

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~~

Potwierdzam zgodność wydruku z dokumentem wydanym w postaci elektronicznej:

| | |
|-------------------------|---|
| Identyfikator dokumentu | 3002153.12651513.9468433 |
| Nazwa dokumentu | 19092024 OZPI_Zwiększenie dojrzałości cyfrowej i cyberbezpieczeństwa MŚP.pdf |
| Tytuł dokumentu | 19092024 OZPI_Zwiększenie dojrzałości cyfrowej i cyberbezpieczeństwa MŚP |
| Data dokumentu | 19.09.2024 00:00:00 |
| Skrót dokumentu | 0E055882178FA3ABFFECAB0ABF4B754F3F96BB41 |
| Wersja dokumentu | 1.0 |
| Akceptacja | Niemczycki Ignacy, 19.09.2024 10:00:03, wersja 1.0 (Podsekretarz Stanu, Minister Ignacy Niemczycki (MIN), Minister Ignacy Niemczycki (MIN)) Ministerstwo Rozwoju i Technologii |
| Akceptacja | Sidoroff Marianna, 19.09.2024 09:44:34, wersja 1.0 (dyrektor departamentu, Departament Gospodarki Cyfrowej (DGC), Departament Gospodarki Cyfrowej (DGC)) Ministerstwo Rozwoju i Technologii |
| | EZD 3.124.8.8. |
| Data wydruku: | 19.09.2024 10:18:00 |
| Autor wydruku: | Macnar Marta |