

Słownik AI dla organizacji regulowanych

361 publicznych haseł • aktualizacja 20.10.2026

allclouds.pl | Definicje, regulacje i powiązane pojęcia

A-BCP-01

AI Service Continuity & DR Plan

Artefakt CDF (fazy F1.5/F6) mechanizmu CBC – plan ciągłości działania systemu AI wymagany przez art. 21 ust. 2 lit. c NIS2/uKSC. Zasila AIMS Evidence Package oraz pakiet dowodowy uKSC (artefakty K4/K8). Wprowadzony w CDF 1.5.0.

Metodyka CDF

Zobacz: AIMS Evidence Package, NIS2/uKSC, AIMS

[Hasło online](#)

A-F2-16

Service Fallback Specification

Artefakt CDF (fazy F2 i F4) kontroli PAG-2 – specyfikacja zastępczej ścieżki kontaktu z pracownikiem dla procesów styku AI z obywatelem. Obejmuje funkcję przełączenia do człowieka, kanał niezależny od systemu AI oraz ścieżkę zgłoszenia zastrzeżeń. Utrzymywana jako sekcja SA-XAI Documentation. Wprowadzony w 1.6.0.

Metodyka CDF

Zobacz: SA-XAI, PAG-2

[Hasło online](#)

A-GOV-01

Karta zasadności zastosowania AI

Artefakt CDF (faza F0) kontroli PAG-1 – udokumentowana odpowiedź na cztery pytania Etapu 0 Przewodnika MC po AI wraz z rozstrzygnięciem GO / NO-GO / REDESIGN i zatwierdzeniem Business Ownera. Wchodzi do Evidence Book jako dowód należytej staranności przy wyborze technologii. Wprowadzony w 1.6.0.

Metodyka CDF

Zobacz: Evidence Book, PAG-1

[Hasło online](#)

A-GOV-02

Polityka korzystania z AI w jednostce

Artefakt CDF (faza F2) kontroli PAG-3 – zasady korzystania z narzędzi AI przez pracowników, katalog danych zakazanych (dane osobowe i identyfikatory, dane szczególnych kategorii, informacje niejawne, wewnętrzne dokumenty urzędowe nieprzeznaczone do upublicznienia), tryb zatwierdzania nowych narzędzi, obowiązki informacyjne. Wprowadzony w 1.6.0.

Metodyka CDF

Zobacz: PAG-3

[Hasło online](#)

A-GOV-03

Rejestr zatwierdzonych narzędzi AI

Artefakt CDF (fazy F2 i F6) kontroli PAG-3 – wykaz narzędzi AI dopuszczonych do użytku służbowego z podstawą dopuszczenia, zakresem dozwolonych danych, informacją o wykorzystywaniu danych do trenowania modeli na rzecz innych klientów, właścicielem biznesowym i datą przeglądu. Wprowadzony w 1.6.0.

Metodyka CDF

Zobacz: PAG-3

[Hasło online](#)

A-HDP-01

Health Data Protection & EHDS Assessment

Artefakt CDF (faza F1.5) mechanizmu HDC (kontrola HDC-1) – ocena ochrony danych zdrowotnych oraz zgodności z EHDS i RODO art. 9. Wymagany dla wdrożeń z aktywnym tagiem HEALTH. Wprowadzony w CDF 1.5.0.

Metodyka CDF

Zobacz: HEALTH (tag ACE), HDC-1, EHDS (rozp. 2025/327), RODO

[Hasło online](#)

A-MDR-01

Medical Device AI Conformity Dossier

Artefakt CDF (faza F1.5) mechanizmu HDC (kontrola HDC-2) – dossier zgodności wyrobu medycznego AI (MDR 2017/745 / IVDR 2017/746), generowany gdy system AI kwalifikuje się jako oprogramowanie wyrobu medycznego. Wprowadzony w CDF 1.5.0.

Metodyka CDF

Zobacz: HDC-2, IVDR (rozp. 2017/746)

[Hasło online](#)

A-MON-01

Post-Deployment Monitoring Checklist

Artefakt CDF generowany w F5 i utrzymywany w F6, oparty na taksonomii NIST AI 800-4 (CAISI, marzec 2026). Definiuje 6 kategorii monitorowania zgodnych z NIST: (1) Functionality – czy system działa zgodnie z przeznaczeniem, (2) Operational – czy infrastruktura utrzymuje spójny poziom usługi, (3) Human Factors – jakość interakcji człowiek–AI (wg NIST: intencja i percepcja użytkownika, ciemne wzorce, pętle sprzężenia zwrotnego; w CDF dodatkowo automation bias, skill degradation, overtrust), (4) Security – zabezpieczenie przed atakami (OWASP ASI, prompt injection), (5) Compliance – zgodność regulacyjna (AI Act, NIS2, DORA), (6) Large-Scale Impacts – pozytywne efekty społeczne i środowiskowe. Wymagany dla LOA $\geq$ L2. Dla każdej kategorii określa metryki, częstotliwość pomiaru, progi eskalacji i właściciela. Wprowadzony w CDF 1.5.0.

Metodyka CDF

Zobacz: NIST AI 800-4, AI Act, OWASP, DORA, NIST

[Hasło online](#)

A-PLD-01

Product Liability Evidence Dossier

Artefakt CDF (fazy F1.5/F2/F6) mechanizmu LER – dossier gotowości dowodowej zawierające mapę ról (producent / importer / dystrybutor / znaczący modyfikujący), rejestr znaczących modyfikacji (LER-2), indeks dowodów podlegających ujawnieniu (art. 9 dyrektywy PLD 2024/2853) z klauzulą ochrony tajemnicy przedsiębiorstwa oraz dokumentację adekwatności bezpieczeństwa produktu (art. 7 ust. 2 lit. f). Zasila Evidence Book (EB-4). Wprowadzony w CDF 1.5.0.

Metodyka CDF

Zobacz: Evidence Book, LER-2

[Hasło online](#)

A-SSI-01

Mapa organów nadzoru AI

Identyfikacja właściwego organu nadzoru (Komisja, KNF, regulator sektorowy) dla danego wdrożenia AI na terytorium RP. Obejmuje mapowanie art. 5–47 ustawy o systemach AI (organ nadzoru i rozdział 2) na strukturę organizacyjną klienta oraz wskazanie obowiązków informacyjnych i rejestrowych wobec właściwych organów. Obowiązkowy artefakt fazy F0/F1 w wariantcie GOV.PL.

Metodyka CDF

[Hasło online](#)

A-SSI-02

Procedura zgłaszania incydentów 24h (Katalog artefaktów) – procedura zgłaszania poważnych incydentów

Workflow zgłaszania poważnych incydentów do Komisji zgodnie z AI Act art. 73 (co do zasady 15 dni; 10 dni w razie śmierci osoby; 2 dni przy naruszeniu powszechnym lub incydencie infrastruktury krytycznej); odrębnie obejmuje wczesne ostrzeżenie ≤ 24 h do właściwego CSIRT, gdy zdarzenie jest incydem NIS2/uKSC. Ustawa o systemach AI nie ustanawia odrębnego polskiego kanału zgłoszenia 24h; oznaczenie „24h” w nazwie katalogowej odnosi się do rygoru NIS2/uKSC i wewnętrznego standardu CDF (przygotowanie zgłoszenia do Komisji w ≤ 24 h). Definiuje kryteria kwalifikacji, szablon zgłoszenia, eskalację wewnętrzną i zewnętrzną (Komisja, CSIRT GOV/MON/NASK) oraz rejestr statusów z dashboardem monitoringowym. Fazy F3/F5, tag GEO:PL. Wprowadzony w CDF 1.5.0.

Metodyka CDF

Zobacz: NIS2/uKSC, AI Act, NASK

[Hasło online](#)

A-SSI-03

Checklist gotowości do kontroli

Lista kontrolna gotowości organizacji na kontrolę Komisji (rozdział 3, art. 48–57), z zawiadomieniem 7 dni przed kontrolą. Obejmuje kompletność dokumentacji technicznej w języku polskim, dostęp do dokumentów, systemów i chmury obliczeniowej (art. 52), wyznaczenie osoby kontaktowej, dostępność logów systemowych i Agent Registry. Uwzględnia rygor natychmiastowej wykonalności decyzji (art. 108). Faza F4.

Metodyka CDF

Zobacz: Agent Registry

[Hasło online](#)

A-SSI-04

Szablon opinii indywidualnej

Wniosek do Komisji o wydanie opinii indywidualnej dotyczącej stosowania AI Act do konkretnego wdrożenia AI (art. 8–18). Opłata 150 zł wynika z art. 11; termin wynosi 30 dni albo 60 dni w sprawie szczególnie skomplikowanej (art. 12), a brak opinii oznacza opinię zgodną ze stanowiskiem wnioskodawcy. Opinia jest wiążąca w zakresie sprawy (art. 13) i po anonimizacji publikowana w BIP (art. 17). Faza F1/F6.

Metodyka CDF

Zobacz: AI Act

[Hasło online](#)

A-SSI-05

Procedura obsługi kontroli

Pełny workflow obsługi kontroli Komisji (art. 48–57): zawiadomienie 7 dni → udostępnienie dokumentacji i infrastruktury → protokół kontroli → prawo do zastrzeżeń → zalecenia pokontrolne → plan realizacji zaleceń → raport wykonania. Zalecenia wyznaczają co do zasady terminy nie krótsze niż 30 dni (art. 57); w razie bezpośredniego ryzyka Komisja może nakazać zaprzestanie stosowania lub wycofanie systemu (art. 63) i nadać decyzji rygor natychmiastowej wykonalności (art. 108). Faza F5.

Metodyka CDF

[Hasło online](#)

A-SSI-06

Szablon zgłoszenia do piaskownicy

Wniosek o dopuszczenie do piaskownicy regulacyjnej AI prowadzonej przez Komisję (rozdział 7, art. 91–103). Udział trwa 6–12 miesięcy i następuje w drodze konkursu; dla MŚP jest nieodpłatny. Uczestnik składa raport roczny (art. 98), a w terminie 90 dni od potwierdzenia uczestnictwa może wnioskować o opinię indywidualną (art. 101). Faza F0/F2.

Metodyka CDF

[Hasło online](#)

A-SSI-07

Matryca kar i sankcji SSI

Matryca ryzyka kar administracyjnych i sankcji karnych według ustawy o systemach AI (art. 104–114). Kwoty kar wynikają z art. 99 AI Act, a ich równowartość w złotych oblicza się według kursu NBP z 28 stycznia (art. 104 ust. 4). Obejmuje układ 20–70% / 30–90% (art. 70 i 84), obniżkę 10–50% (art. 107) oraz przepisy karne art. 112–113. Faza F1.

Metodyka CDF

Zobacz: AI Act

[Hasło online](#)

Acceptance Criteria Checklist (F0-AC-01)

Acceptance Criteria Checklist

Artefakt Fazy F0 definiujący kryteria formalne, które muszą być spełnione, aby Klient zaakceptował wynik wdrożenia. Zawiera 6 kryteriów minimalnych rekomendowanych przez CDF (sekcja G.9 Evidence Book): komplet artefaktów obowiązkowych z profilu ACE, AI Act Readiness Score na poziomie docelowym (rekomendacja $\geq 90\%$), zatwierdzone ASIA Report i SoA, ukończony Human Competence Gate, uzgodnione i podpisane Cognitive SLA oraz plan przejścia do F6 CogOps, a także kryteria własne Klienta. Stanowi załącznik do umowy wdrożeniowej. Identyfikator: F0-AC-01.

Metodyka CDF

Zobacz: AIMS Evidence Package, Agent Coordination, Cognitive SLA, AIMS

[Hasło online](#)

Accountability Matrix

Matryca odpowiedzialności per LOA

Tabela przypisująca odpowiedzialność za decyzje systemu AI do konkretnych ról organizacyjnych w zależności od poziomu autonomii agenta (LOA L0–L4). Dla L0–L1 pełna odpowiedzialność leży po stronie operatora / deployera; dla L2 odpowiedzialność jest dzielona (deployer + provider); dla L3–L4 odpowiedzialność przesuwa się na organizację (zarząd) z obowiązkowym audytem i pełnym pakietem Evidence Book. W procesach rozstrzygających profilu GOV maksymalny poziom to L2 (CV-12). Patrz: Załącznik B, Tabela 62 w Metodyce.

Metodyka CDF

[Hasło online](#)

ACE (Adaptive Configuration Engine)

Adaptive Configuration Engine

Dynamiczny mechanizm konfiguracyjny wbudowany w CDF, który aktywuje odpowiedni podzbiór faz, kontroli, artefaktów i załączników na podstawie profilu organizacji i wybranych wymogów zgodności. Działa w trybie Self-Service (Kwestionariusz Konfiguracyjny) lub Guided (F0). Wprowadzony w CDF 1.4.4; opisany w sekcji „Adaptive Configuration Engine (ACE)” Metodyki.

Metodyka CDF

Zobacz: Kwestionariusz Konfiguracyjny

[Hasło online](#)

ACE Configuration Profile

Profil konfiguracyjny ACE

Dokument wynikowy ACE określający aktywne tagi, wybrany profil referencyjny, aktywne tiers mechanizmów CDF (Cognitive SLA, HCG, F6) oraz spersonalizowaną Matrycę Zgodności. Generowany w F0, wersjonowany jako ACE-[PROFIL]-v[N].[M].

Metodyka CDF

Zobacz: Cognitive SLA

[Hasło online](#)

ACE Profile Matrix

Matryca profili ACE

Załącznik E-ACE: matryca 77 wymogów zgodności × 11 profili referencyjnych z przypisaniem WYMAGANE / REKOMENDOWANE / DOSTĘPNE per wymóg i profil.

Metodyka CDF

[Hasło online](#)

ACE Profile Version Record

Rekord wersji profilu ACE

Formalny, niezmienny (immutable) rekord każdej wersji profilu konfiguracyjnego organizacji. Zawiera wersję, datę, autora, uzasadnienie zmiany i flagę REDUCTION (jeśli Scope Reduction). Schemat: ACE-[PROFIL]-v[N].[M].

Metodyka CDF

Zobacz: Scope Reduction, REDUCTION (flag)

[Hasło online](#)

ACE Reconfiguration Log

Rejestr rekonfiguracji ACE

Artefakt CDF (F0–F6) dokumentujący każdą zmianę profilu konfiguracyjnego organizacji: wersja przed/po, data, uzasadnienie, autor, flaga REDUCTION.

Metodyka CDF

Zobacz: REDUCTION (flag)

[Hasło online](#)

Agent (AI)

Autonomiczny agent AI

Program AI zdolny do samodzielnego podejmowania decyzji i wykonywania działań w środowisku cyfrowym lub fizycznym w celu realizacji konkretnego zadania biznesowego lub operacyjnego.

Podstawy AI

[Hasło online](#)

AGENT (tag ACE)

Tag konfiguracyjny ACE

Tag ACE aktywowany, gdy wdrożenie obejmuje agenty AI (pojedyncze lub wieloagentowe). Włącza sekcje Agent Governance, tożsamości agentów, bezpieczeństwa i cyklu życia agentów.

Metodyka CDF

[Hasło online](#)

Agent Coordination

Agent Coordination

Metryka mierząca skuteczność współpracy agentów AI w środowisku multi-agent. Definiowana jako procent zadań multi-agent ukończonych bez eskalacji do człowieka. Target bazowy CDF: $\geq 85\%$. Metryka należy do Cognitive SLA Tier 2 (6 metryk). Mierzona w Fazie F4 (Cognitive Sprint) i monitorowana w Fazie F6 (CogOps). Patrz: Tabela 14 w Metodyce.

Metodyka CDF

Zobacz: Cognitive SLA Tier, Cognitive Sprint, Cognitive SLA, CogOps

[Hasło online](#)

Agent Identity Schema

Agent Identity Schema (CDF, na bazie NIST NCCoE)

Schemat tożsamości agenta AI. Konstrukcja własna CDF rozwijająca filary identyfikacji i uwierzytelniania z concept paper NIST NCCoE „Accelerating the Adoption of Software and AI Agent Identity and Authorization” (5.02.2026). Nie jest cytatem z publikacji NIST. Kontrola T-011, faza F2, artefakt A-F2-05 Agent Registry.

Metodyka CDF

Zobacz: Agent Registry, NIST

[Hasło online](#)

Agent Kill-Switch

Procedura awaryjnego wyłączenia agenta

Mechanizm natychmiastowego, sprzętowego lub programowego zatrzymania pojedynczego agenta albo całego roju agentów, z kaskadowym powiadomieniem zależnych węzłów i automatycznym przełączeniem na weryfikację manualną. Obowiązkowy element Agent Governance od Fazy 2.

Podstawy AI

[Hasło online](#)

Agent Lifecycle Management (ALM)

Zarządzanie cyklem życia agenta

Sześciostopniowy model zarządzania agentem w CDF: Design → Build → Test → Deploy → Monitor → Optimize/Retire. Obejmuje także Agent Retirement Protocol zapewniający bezpieczne wycofanie agenta, sprawdzenie zależności oraz transfer wiedzy operacyjnej i biznesowej. Realizowane w Fazie 6 CDF. Zob. także ALM (Agent Lifecycle Management).

Metodyka CDF

Zobacz: ALM (Agent Lifecycle Management), Agent Retirement Protocol

[Hasło online](#)

Agent Readiness Audit

Audyt gotowości na agenty AI

Ocena dojrzałości organizacji do wdrożenia autonomicznych agentów AI, obejmująca dane, procesy, kompetencje, governance, gotowość psychologiczną i zdolność do bezpiecznego nadzorowania agentów w środowisku pracy. Realizowany w Fazie 0 CDF.

Metodyka CDF

[Hasło online](#)

Agent Registry

Rejestr agentów AI

Obowiązkowy od Fazy 2 centralny rejestr wszystkich agentów systemu, zawierający ich rolę, uprawnienia, poziom autonomii, właściciela, zależności, budżety tokenowe, pole Delegated By, Kill-Switch Authority i historię audytów. Fundament Agent Governance Model oraz audytowalności systemu wieloagentowego.

Metodyka CDF

[Hasło online](#)

Agent Retirement Protocol

Agent Retirement Protocol

Formalna procedura Fazy 6 CDF definiująca bezpieczne wycofanie agenta AI z eksploatacji. Obejmuje: (1) archiwizację pamięci i historii decyzji agenta, (2) cofnięcie uprawnień w Agent Registry, (3) sprawdzenie zależności – czy inne agenty lub procesy polegają na wycofywanym agencie, (4) transfer wiedzy operacyjnej do następcy lub zespołu ludzkiego, (5) weryfikację braku aktywnych subskrybentów MCP, (6) raport końcowy z powodami i analizą wpływu.

Metodyka CDF

Zobacz: Agent Registry

[Hasło online](#)

Agent Threat Model

Agent Threat Model

Spersonalizowany model zagrożeń agentowych oparty na CoSAI, OWASP ASI i CSA ATF. Filtrowany przez profil ACE. Patrz: Załącznik B.

Metodyka CDF

Zobacz: OWASP

[Hasło online](#)

Agentic RAG

agentowe wyszukiwanie z dopytywaniem

Tryb wyszukiwania w dokumentach, w którym agent AI sam ocenia, czy zebrany materiał wystarcza do odpowiedzi. Gdy czegoś brakuje, tworzy zapytania uzupełniające i przeszukuje dokumenty w kolejnej rundzie, a na końcu łączy fragmenty ze wszystkich rund i usuwa powtórzenia. Diagnostyka pokazuje każdą rundę, zapytanie i źródło, więc odpowiedź da się sprawdzić

Podstawy AI

AI Act · ISO/IEC 42001

Zobacz: RAG, Agent (AI), Multi-agent, LLM

[Hasło online](#)

Gdzie o tym piszemy: SAIE Pantera

AI

Artificial Intelligence

Sztuczna inteligencja – systemy komputerowe zdolne do wykonywania zadań wymagających ludzkiej inteligencji, takich jak rozumowanie, uczenie się, klasyfikacja, generowanie treści, podejmowanie decyzji czy analiza kontekstu.

Podstawy AI

AI Act

Zobacz: AI Act

[Hasło online](#)

AI Act

AI Act (Rozp. 2024/1689)

Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2024/1689 ustanawiające zharmonizowane przepisy dotyczące sztucznej inteligencji, zmienione rozporządzeniem (UE) 2026/1744 (Digital Omnibus on AI). Klasyfikuje systemy według poziomu ryzyka i nakłada obowiązki na dostawców oraz wdrażających, w tym obowiązki dotyczące zarządzania ryzykiem, logowania, przejrzystości, nadzoru ludzkiego i dokumentacji technicznej. Stosowanie etapowe: zakazane praktyki i kompetencje w zakresie AI od 02.02.2025; modele GPAI, governance i kary od 02.08.2025; obowiązki przejrzystości (art. 50) od 02.08.2026; nowe zakazy z art. 5 po okresie przejściowym do 02.12.2026; samodzielne systemy wysokiego ryzyka z zał. III od 02.12.2027; systemy wbudowane w produkt z zał. I od 02.08.2028.

Regulacje i normy

rozp. 2026/1744

Zobacz: Digital Omnibus (EU)

[Hasło online](#)

Gdzie o tym piszemy: Ustawa o systemach SI

Gdzie o tym piszemy: Polityka korzystania z AI — wzór

Gdzie o tym piszemy: ChatGPT Enterprise, Copilot czy własne

AI Act Readiness Score (ARS)

AI Act Readiness Score

Ilościowy wskaźnik (0–100%) gotowości organizacji do zgodności z AI Act. Formuła: $ARS = \sum (waga \times wynik)$ dla 5 wymiarów: Risk Classification, Technical Documentation, Human Oversight, Transparency, FRIA Readiness. Progi decyzyjne: $\geq 90\%$ – pełna zgodność (full compliance), 70–89% – zgodność warunkowa (conditional), $< 70\%$ – blokada wdrożenia (blocked). Generowany w F0 i aktualizowany w F1.5. Sformalizowany w CDF 1.4.4 (Z-003).

Metodyka CDF

Zobacz: AI Act, FRIA

[Hasło online](#)

AI Champions Program

Program liderów AI

Program budowy wewnętrznych liderów transformacji AI w organizacji, realizowany w Fазie 3 CDF. Jego celem jest tworzenie lokalnych ambasadorów zmiany zdolnych do wspierania adopcji AI, eskalowania problemów i promowania prawidłowych praktyk użycia systemów kognitywnych.

Wdrożenie i zarządzanie

[Hasło online](#)

AI Concerns Feedback Channel

Kanał zgłaszania obaw AI

Formalny mechanizm umożliwiający pracownikom, użytkownikom końcowym, partnerom i osobom trzecim, których dotyczy działanie systemu AI, zgłaszanie obaw, skarg i wniosków związanych z decyzjami podejmowanymi przez systemy AI. Wymagany przez ISO/IEC 42001 Annex A – A.3.3 (kanał zgłaszania obaw AI), z ochroną zgłaszających zgodnie z dyrektywą (UE) 2019/1937; wspiera wymogi art. 14 AI Act (nadzór ludzki i możliwość interwencji). W CDF realizowany w Fazie F6 (CogOps) przez artefakt A-F6-07 Rejestr zgłoszeń kanału obaw AI (w sekcji F6 Metodyki oznaczany także jako F6-AFC-01). Odrębny od ścieżki zgłoszenia zastrzeżeń obywatela z kontroli PAG-2.

Wdrożenie i zarządzanie

AI Act · ISO/IEC 42001

Zobacz: ISO/IEC 42001, AI Act

[Hasło online](#)

AI Fatigue Index

Indeks zmęczenia AI

Wskaźnik wprowadzony w Fazie 5, systematycznie mierzący poziom zmęczenia organizacji wynikającego z tempa wdrożeń AI, przeciążenia zmianą, nadmiaru inicjatyw lub spadku zaangażowania użytkowników. Służy do zapobiegania stagnacji wdrożeniowej i odpowiedniego dozowania skali transformacji.

Wdrożenie i zarządzanie

[Hasło online](#)

AI Model & Vendor Risk Assessment

AI Model & Vendor Risk Assessment

Kompleksowy proces oceny ryzyka modeli AI i ich dostawców realizowany w Fazie 1.5 CDF przed zatwierdzeniem docelowego modelu. Obejmuje 6 kryteriów: (1) jurysdykcja dostawcy, (2) jurysdykcja danych treningowych, (3) compliance disclosure, (4) vendor lock-in i migracja (powiązanie z VDP-1), (5) historia regulacyjna dostawcy, (6) ciągłość dostępu. Artefakt A-F15-07 (Katalog artefaktów). Wynik dokumentowany w Tabeli 12 Metodyki.

Metodyka CDF

[Hasło online](#)

AI Vendor Diversification Strategy

AI Vendor Diversification Strategy

Strategia minimalizacji ryzyka uzależnienia od pojedynczego dostawcy AI (VDP-1).

Metodyka CDF

[Hasło online](#)

AIMS

AI Management System (ISO/IEC 42001)

System zarządzania sztuczną inteligencją zdefiniowany w normie ISO/IEC 42001:2023. W CDF stanowi jeden z kluczowych punktów odniesienia dla governance AI, obok AI Act i NIS2/uKSC. Metodyka CDF jest zaprojektowana tak, aby wspierać organizacje w budowie AIMS i przygotowaniu do certyfikacji.

Regulacje i normy

ISO/IEC 42001

Zobacz: ISO/IEC 42001

[Hasło online](#)

AIMS Evidence Package

AIMS Evidence Package

Zbiór dowodów zgodności z ISO/IEC 42001:2023 generowany i utrzymywany w ramach CDF (artefakt A-F15-03). Obejmuje: Politykę AI, Rejestr ryzyk AI, Statement of Applicability (SoA), plan zarządzania AI, raport z przeglądu kierownictwa, zapisy z audytów wewnętrznych, dziennik incydentów AI oraz dowody kompetencji. Tworzony w F1.5 (baseline), wzbogacany w F2–F4, przeglądany w F5 i F6 (kwartalnie). Cykl życia poszczególnych artefaktów pakietu definiuje Tabela 9 Metodyki.

Metodyka CDF

Zobacz: Compliance Readiness Report, Agent Registry, ASIA

[Hasło online](#)

AIMS Lifecycle

Cykl życia artefaktów AIMS

Tabela definiująca cykl życia 12 kluczowych artefaktów pakietu AIMS Evidence Package w fazach CDF F0–F6: moment utworzenia (Created), aktualizacji (Updated), przeglądu (Reviewed) i właściciela (Owner). Źródło: Metodyka, sekcja AIMS Evidence Package. Wprowadzone w v1.4.4.

Metodyka CDF

Zobacz: AIMS Evidence Package, AIMS

[Hasło online](#)

AIP

Agent Interaction Protocols

Zestaw protokołów zarządzających współpracą agentów AI w CDF. Obejmuje trzy wzorce: Hierarchical (Supervisor–Worker, domyślny i najbezpieczniejszy dla procesów krytycznych, L0–L1), Collaborative (współdzielona przestrzeń robocza, dozwolony wyłącznie dla procesów pomocniczych, L1–L2) i Pipeline (sekwencyjne przekazywanie wyników, procesy deterministyczne i liniowe). Każda interakcja maszyna-maszyna jest logowana w Immutable Audit Trail ze znacznikiem czasu, inicjatorem, kosztem w tokenach i wynikiem. Patrz: Załącznik B.

Metodyka CDF

Zobacz: Immutable Audit Trail

[Hasło online](#)

Air-gap

Izolacja sieciowa

Fizyczne odcięcie systemu IT od zewnętrznych sieci, w tym internetu. Jest to najwyższy poziom bezpieczeństwa dla suwerennych systemów AI i typowy wymóg dla środowisk obronnych, niejawnych lub szczególnie krytycznych.

Suwerenność i architektura

[Hasło online](#)

Gdzie o tym piszemy: Bielik i PLLuM

Gdzie o tym piszemy: ChatGPT Enterprise, Copilot czy własne

Air-Gapped Defense

Izolowana architektura obronna

Najwyższy poziom docelowego wzorca wdrożeniowego w CDF, zakładający pełną fizyczną izolację środowiska AI, brak połączeń z internetem oraz brak operacyjnych zależności od zewnętrznych usług. Stosowany dla obronności, informacji niejawnych i wybranych systemów infrastruktury krytycznej państwa.

Suwerenność i architektura

[Hasło online](#)

ALM (Agent Lifecycle Management)

Agent Lifecycle Management

Zarządzanie pełnym cyklem życia agenta AI: od rejestracji w Agent Registry (F2), przez monitoring operacyjny (F4–F6), do wycofania (Agent Retirement Protocol). Zob. Agent Lifecycle Management (ALM).

Metodyka CDF

Zobacz: Agent Lifecycle Management (ALM), Agent Retirement Protocol, Agent Registry

[Hasło online](#)

API

Application Programming Interface

Interfejs programowania aplikacji – zestaw reguł i metod umożliwiających komunikację między różnymi systemami lub komponentami oprogramowania. W kontekście CDF wymaga oceny w wymiarze zależności łańcucha dostaw i bezpieczeństwa integracji.

Podstawy AI

[Hasło online](#)

ARS (AI Act Readiness Score)

AI Act Readiness Score

Wskaźnik gotowości organizacji do spełnienia wymogów AI Act. Skala 0–100%. Target CDF: $\geq 90\%$. Zob. AI Act Readiness Score (ARS). Patrz: Tabela 19 w Metodyce.

Metodyka CDF

Zobacz: AI Act Readiness Score (ARS), AI Act

[Hasło online](#)

ASIA

AI System Impact Assessment

Ocena wpływu systemu AI realizowana przed wdrożeniem, obejmująca analizę ryzyk dla praw podstawowych, bezpieczeństwa, środowiska i społeczeństwa. W CDF inicjowana w Fazie F1.5 (dla profili z tagiem REGULATED) lub aktywowana przez profil ACE (REKOMENDOWANE dla pozostałych). Aktualizowana w kolejnych fazach (F2, F5, F6). Mapuje się na obowiązki art. 9 i art. 27 AI Act oraz na wymagania FRIA. Dla wdrożeń CSE-GOV i CSE-COM z danymi regulowanymi raport zawiera rozszerzony moduł suwerenności.

Metodyka CDF

Zobacz: REGULATED (tag ACE), AI Act, FRIA

[Hasło online](#)

ATF (Agentic Trust Framework)

Agentic Trust Framework (otwarta specyfikacja MassiveScale.AI, opublikowana na blogu CSA)

Framework dojrzałości agentowej opublikowany 2.02.2026 na blogu Cloud Security Alliance jako otwarta specyfikacja (licencja Creative Commons, kanoniczna wersja w repozytorium GitHub massivescale-ai); autor: Josh Woodruff, MassiveScale.AI. Jest to wpis gościnny, nie formalna publikacja badawcza CSA. 4 poziomy dojrzałości: Level 1 (Intern – obserwacja, zatwierdza każdą akcję), Level 2 (Junior – rekomenduje i wykonuje po zatwierdzeniu), Level 3 (Senior – działa samodzielnie z powiadomieniem ex-post), Level 4 (Principal – pełna autonomia w granicach mandatu). Mapowanie na CDF LOA: L0–L1 (Intern), L2 (Junior), L3 (Senior), L4 (Principal). Patrz: Tabela 61 (ATF ↔ LOA Cross-Reference) w Załączniku B Metodyki.

Metodyka CDF

[Hasło online](#)

Autonomous Swarm

Autonomiczny rój agentów

Sieć wielu współpracujących agentów AI działających bez stałego nadzoru człowieka w ramach zdefiniowanych granic autonomii. W CDF stosowana wyłącznie dla procesów niekrytycznych lub zaplecza operacyjnego, z obowiązkowym Token Budget Governance i Agent Kill-Switch.

Podstawy AI

[Hasło online](#)

Backup 3-2-1

Strategia backupu 3-2-1

Strategia tworzenia kopii zapasowych zakładająca utrzymanie co najmniej 3 kopii danych, na 2 różnych nośnikach, z których 1 przechowywana jest poza główną lokalizacją. W CDF stosowana w Fazie 1.5 jako element wymagań NIS2/uKSC.

Suwerenność i architektura

[Hasło online](#)

Badanie NASK 2026

AI w e-administracji publicznej – perspektywa urzędników i instytucji

Raport NASK – PIB z 17 marca 2026 r. Źródło klasy D w kanonie CDF: nie tworzy wymagań, lecz dostarcza baseline adopcji dla wariantu CSE-GOV (sekcja D.5) oraz warunków brzegowych czterech konceptów rozwiązań. Badanie ilościowe jest przez autorów określone jako eksploracyjne i pilotażowe, a próba jako niereprezentatywna; wartości wolno stosować jako materiał porównawczy wewnątrz próby, nie jako parametry populacyjne ani podstawę zobowiązań kontraktowych (warunek brzegowy EB-4).

Regulacje i normy

Zobacz: NASK

[Hasło online](#)

Biblioteka wzorców wdrożeniowych

Biblioteka wzorców wdrożeniowych

Skatalogowany zbiór reużywalnych, sprawdzonych wzorców wdrożeń AI, umożliwiających szybkie i bezpieczne powielanie sukcesów w kolejnych działach lub jednostkach organizacyjnych. Budowana w Fazie 5 CDF.

Wdrożenie i zarządzanie

[Hasło online](#)

Bielik

Bielik (polski model językowy)

Polski otwarty model językowy Fundacji SpeakLeash, trenowany na superkomputerach ACK Cyfronet AGH. Rodzina od 1,5 do 11 mld parametrów na licencji Apache 2.0 (użycie komercyjne bez opłat); mniejsze wersje działają na laptopie, 11B na jednej karcie 24 GB. W SAIE dostępny przez PROXY:AI na tych samych zasadach co modele globalne

Podstawy AI

Zobacz: PLLuM, LLM, Kwantyzacja, On-premises / On-prem, RAG

[Hasło online](#)

Gdzie o tym piszemy: Bielik i PLLuM

Gdzie o tym piszemy: ChatGPT Enterprise, Copilot czy własne

Biuro Komisji

Obsługa Komisji Rozwoju i Bezpieczeństwa SI

Ustawa nie tworzy odrębnego biura ani państwowej osoby prawnej: obsługę administracyjną i biurową Komisji oraz jej Przewodniczącego zapewnia urząd obsługujący ministra właściwego do spraw informatyzacji (art. 43). Maksymalny limit wydatków z budżetu państwa (art. 126) określono na lata 2026–2035: 2026 = 9,30 mln zł; 2027 = 23,74 mln zł; 2028 = 24,17 mln zł; 2029 = 24,89 mln zł; 2030 = 25,63 mln zł; dalej rosnąco do 29,68 mln zł w 2035 r. Środki z administracyjnych kar pieniężnych są dochodem budżetu państwa (art. 106).

Regulacje i normy

Zobacz: Ustawa o systemach sztucznej inteligencji (SSI)

[Hasło online](#)

Bounded Autonomy

Ograniczona autonomia agenta

Zasada projektowa CDF zakładająca, że każdy agent AI działa w ściśle zdefiniowanych granicach uprawnień, budżetu tokenowego i zakresu decyzyjnego. Granice autonomii są przypisywane na podstawie Skali Autonomii (L0–L4) i podlegają ciągłemu monitorowaniu w ramach Agent SLA.

Podstawy AI

[Hasło online](#)

Business Continuity

Ciągłość działania

Zdolność organizacji do utrzymania kluczowych funkcji biznesowych podczas i po incydencie lub zakłóceniu. W CDF adresowana mechanizmem CBC (Cognitive Business Continuity, kontrole CBC-1..3, artefakt A-BCP-01) wymaganym przez art. 21 ust. 2 lit. c NIS2/uKSC, a w warstwie agentowej przez Agent Kill-Switch i Vendor Disruption Protocol (Załącznik B).

Suwerenność i architektura

[Hasło online](#)

C-Suite

Zarząd / najwyższe kierownictwo

Zbiorcze określenie najwyższego kierownictwa organizacji (CEO, CTO, CIO, CFO, CISO). W CDF uczestniczy w Executive Alignment Workshop (Faza 0) oraz w walidacji North Star (Faza 1).

Wdrożenie i zarządzanie

[Hasło online](#)

CapEx

Capital Expenditure / Wydatki inwestycyjne

Wydatki kapitałowe na zakup lub budowę aktywów trwałych, w tym infrastruktury AI (serwery, GPU, chłodzenie, okablowanie). W CDF uwzględniane w TCO Model 3–5 lat projektowanym w Fazie 1.

Wdrożenie i zarządzanie

Zobacz: OpEx

[Hasło online](#)

CBC

Cognitive Business Continuity

Mechanizm ciągłości działania systemu AI wprowadzający reżim ciągłości i przywracania po awarii wymagany przez art. 21 ust. 2 lit. c NIS2/uKSC: plan ciągłości i DR (BCP/DRP), RTO/RPO per system, kopie zapasowe 3-2-1, tryby kontrolowanej degradacji, fallback na model suwerenny. Odrębny od CBP (Cyfrowego Bliźniaka Poznawczego). Obejmuje kontrole CBC-1, CBC-2, CBC-3. Fazy F1/F1.5/F6. Artefakt: A-BCP-01. Wprowadzony w CDF 1.5.0.

Metodyka CDF

[Hasło online](#)

CBC-1

Continuity & DR Plan

Kontrola CDF mechanizmu CBC: plan ciągłości działania i przywracania (BCP/DRP) dla usług AI – RTO/RPO per system, kopie zapasowe 3-2-1, tryby kontrolowanej degradacji, fallback na model suwerenny (spięcie z VDP-2). Obszary wiedzy KD5/KD11. Fazy F1/F1.5/F6. Wprowadzona w CDF 1.5.0.

Metodyka CDF

[Hasło online](#)

CBC-2

Crisis Management & Comms

Kontrola CDF mechanizmu CBC: procedury zarządzania kryzysowego i komunikacji, eskalacja oraz powiązanie z obsługą incydentów (24h/72h wg NIS2/uKSC). Obszary wiedzy KD5/KD2. Fazy F1.5/F6. Wprowadzona w CDF 1.5.0.

Metodyka CDF

Zobacz: NIS2/uKSC

[Hasło online](#)

CBC-3

Continuity Testing

Kontrola CDF mechanizmu CBC: cykliczne testy odtworzeniowe oraz utrzymanie aktualności planu ciągłości działania. Obszary wiedzy KD5/KD12. Faza F6. Wprowadzona w CDF 1.5.0.

Metodyka CDF

[Hasło online](#)

CBP

Cyfrowy Bliźniak Poznawczy / Cognitive Worker Twin

Wierny model poznawczy pracownika organizacji, obejmujący wiedzę jawną, wiedzę ukrytą (tacit knowledge), interpretacje, preferencje decyzyjne i wzorce zachowań. Służy jako warstwa ciągłości poznawczej i dopełnienie wdrożenia AI do pełnego potencjału. Element K12 ontologii CDF.

Podstawy AI

[Hasło online](#)

CBP Fidelity Test

CBP Fidelity Test

Test wierności poznawczej (artefakt A-CBP-05, F5/F6) weryfikujący, w jakim stopniu CBP w produkcji wiernie odwzorowuje sposób myślenia, interpretacji i podejmowania decyzji pracownika. Wynikiem jest Cognitive Fidelity Score (CFS), który determinuje poziom CFL. Wykonywany w F5 i cyklicznie w F6.

Metodyka CDF

[Hasło online](#)

CBP Monitoring Dashboard

CBP Monitoring Dashboard

Dashboard F5/F6 wizualizujący metryki CBP i wskaźniki Human Factors Monitoring (częstotliwość override'ów decyzji AI, czas walidacji outputów, wskaźnik eskalacji do człowieka). Oparty na taksonomii NIST AI 800-4. Wskazany w sekcji „Zasady architektoniczne NIST AI 800-4” Metodyki; nie ma odrębnej pozycji w Katalogu artefaktów CDF.

Metodyka CDF

Zobacz: NIST AI 800-4, NIST

[Hasło online](#)

CBP Readiness Assessment

CBP Readiness Assessment

Artefakt F1 (A-CBP-01, tag SCALE) oceniający, ile wiedzy organizacji jest jawnej, a ile ukrytej, oraz gdzie znajdują się luki poznawcze; punkt wyjścia do CBP Capture Strategy (F2).

Metodyka CDF

[Hasło online](#)

CBP Sync Protocol

Protokół Synchronizacji CBP

Mechanizm ciągłej aktualizacji Cyfrowego Bliźniaka Poznawczego z nowych danych pracownika. Artefakt Fazy F6 (Operate) zapewniający, że CBP pozostaje aktualny w miarę ewolucji wiedzy i zachowań pracownika.

Metodyka CDF

[Hasło online](#)

CDF

Cognitive Deployment Framework

Uniwersalny, agnostyczny wobec systemów i infrastruktury IT framework metodyczny allclouds.pl do wdrożeń Enterprise Cognitive Systems (ECS). W edycji Client Success dostosowany do sektora publicznego i regulowanego. Obejmuje pełny cykl od rekonesansu kognitywnego i compliance po wdrożenie, skalowanie, governance i ciągłą optymalizację. Wersjonowanie w formacie [N].[M].[P] (sekcja „Wersjonowanie metodyki CDF”).

Wdrożenie i zarządzanie

[Hasło online](#)

Gdzie o tym piszemy: ChatGPT Enterprise, Copilot czy własne

CDF Academy

Akademia CDF

Program szkoleniowy CDF (Faza 3) dostarczający 40-godzinne certyfikujące szkolenie z modulem projektowania interakcji minimalizujących obciążenie poznawcze operatorów. Fundament budowy wewnętrznych kompetencji AI i programu AI Champions.

Metodyka CDF

[Hasło online](#)

CDF North Star

Dokument North Star CDF

Artefakt Fazy 1 łączący cele strategiczne, KPI i kamienie milowe programu AI.

Metodyka CDF

[Hasło online](#)

CDF Platform

CDF Platform

Aplikacja webowa wspomagająca wdrożenie metodyki CDF. Realizuje ACE (Adaptive Configuration Engine) jako interaktywny konfigurator profili, wyświetla tagi, matrycę zgodności i artefakty. ACE jest modulem logicznym opisanym w sekcji „Adaptive Configuration Engine (ACE)” Metodyki; CDF Platform jest jego implementacją technologiczną i trzecim elementem triady wydania.

Wdrożenie i zarządzanie

[Hasło online](#)

CDF Risk Engine

Silnik zarządzania ryzykiem

Rozwiązanie technologiczne wdrażane jako fundament bezpieczeństwa systemu, realizujące ciągłe procedury zarządzania ryzykiem zgodne z ISO/IEC 23894 i wymaganiami governance AI.

Metodyka CDF

Zobacz: ISO/IEC 23894

[Hasło online](#)

Center of Excellence

Centrum Doskonałości

Wewnętrzna jednostka organizacyjna odpowiedzialna za standaryzację, skalowanie i zarządzanie wiedzą w obszarze AI. W CDF element modelu organizacyjnego Fazy 5 (Skalowanie i Industrializacja).

Wdrożenie i zarządzanie

[Hasło online](#)

CETS 225 (Konwencja Rady Europy o AI)

Council of Europe Framework Convention on AI (CETS 225)

Konwencja ramowa Rady Europy o sztucznej inteligencji, prawach człowieka, demokracji i praworządności. Otwarta do podpisu 5 września 2024 r. w Wilnie. Podstawą podpisania przez Unię Europejską była decyzja Rady (UE) 2024/2218 z 28.08.2024; dokument zatwierdzenia Unia złożyła 15 maja 2026 r. Na 12 września 2026 r. konwencja nie weszła w życie, ponieważ nie osiągnięto progu z art. 30 ust. 3 (pięć zgód na związanie, w tym trzy państwa członkowskie Rady Europy). Depozyt Unii nie zalicza się do progu trzech państw. Relację z AI Act opisuje sekcja E.6 Załącznika E.

Regulacje i normy

[Hasło online](#)

CFL

Cognitive Fidelity Levels

Pięciostopniowa skala dojrzałości CBP, niezależna od skali LOA. Mierzy wierność odwzorowania poznawczego: CFL-1 Profil Deklaratywny, CFL-2 Profil Obserwacyjny, CFL-3 Profil Interpretacyjny (CFS $\geq 60\%$), CFL-4 Profil Predykcyjny (CFS $\geq 80\%$), CFL-5 Profil Autonomiczny (CFS $\geq 90\%$).

Metodyka CDF

[Hasło online](#)

CFS

Cognitive Fidelity Score

Miara jakości odwzorowania poznawczego w skali 0–100%. Określa, w jakim stopniu Cyfrowy Bliźniak Poznawczy (CBP) wiernie reprezentuje sposób myślenia, interpretacji i podejmowania decyzji przez pracownika. Progi: CFL-3 $\geq 60\%$, CFL-4 $\geq 80\%$, CFL-5 $\geq 90\%$.

Metodyka CDF

[Hasło online](#)

Chain of Custody

Chain of Custody

Pełna ścieżka odpowiedzialności od danych wejściowych do decyzji wyjściowej systemu AI, obejmująca każdy etap transformacji, wzbogacenia i wykorzystania. W CDF realizowany poprzez: Immutable Audit Trail (F6), Data Provenance Tracking (K3), Agent Identity Schema oraz Cognitive Observability. Różni się od data lineage zakresem – obejmuje nie tylko pochodzenie danych, ale również decyzje ludzkie (kto zatwierdził, na jakiej podstawie) i agentowe (który agent, z jakim promptem, w jakiej roli).

Suwerenność i architektura

[Hasło online](#)

Champion (AI Champion)

Lider AI / Ambasador AI

Wewnętrzny pracownik organizacji przeszkolony jako ekspert i promotor wdrożeń AI. Pomaga zespołom w praktycznym użyciu narzędzi AI i pełni rolę pomostu między biznesem, użytkownikami a zespołem transformacyjnym.

Wdrożenie i zarządzanie

[Hasło online](#)

Change Management

Zarządzanie zmianą

Proces systematycznego zarządzania przejściem organizacji przez transformację – od planowania, komunikacji i szkolenia po monitoring adopcji i przeciwdziałanie oporowi. W CDF realizowane w Fazie 3 z obowiązkowym zaangażowaniem liderów organizacji.

Wdrożenie i zarządzanie

[Hasło online](#)

Chatbot

program do rozmowy tekstowej

Program prowadzący rozmowę tekstową w oknie czatu, na stronie albo w aplikacji. Nowoczesne chatboty korzystają z dużych modeli językowych, dlatego piszą płynnie i potrafią udawać człowieka. Dostawca musi zaprojektować chatbota tak, żeby użytkownik wiedział, że rozmawia z AI

Podstawy AI

AI Act (art. 50 ust. 1)

Zobacz: LLM, Voicebot, Agent (AI)

[Hasło online](#)

Gdzie o tym piszemy: Gra TURING:AI

CLASSIFIED (tag ACE)

Tag ACE dla wdrożeń niejawnych

Tag ACE stosowany w profilach obejmujących systemy przetwarzające informacje niejawne. Aktywuje wymagania związane z akredytacją bezpieczeństwa (np. ABW), fizyczną separacją infrastruktury, kryteriami personalnymi oraz zgodnością z przepisami o ochronie informacji niejawnych. Dotyczy profili DEFENSE i SOV (Sovereign) na najwyższym poziomie restrykcyjności.

Metodyka CDF

Zobacz: DEFENSE (tag ACE)

[Hasło online](#)

Cognitive Circuit Breaker

Kognitywny wyłącznik automatyczny

Mechanizm automatycznego odcięcia agenta od systemów zewnętrznych po przekroczeniu 3 kolejnych obłanych testów weryfikacji jakości kognitywnej. Zapobiega propagacji błędnych decyzji i stanowi zabezpieczenie dla środowisk wieloagentowych.

Metodyka CDF

[Hasło online](#)

Cognitive Degradation Monitoring

Monitoring degradacji kognitywnej

Trójstopniowa skala monitorowania jakości rozumowania agentów AI: Normal (działanie w normie), Degraded (obniżona jakość – wymagana interwencja), Critical (krytyczne odchylenie – procedury naprawcze). Wdrożona w Fazie 2, generuje alerty i uruchamia procedury naprawcze, a wyniki prezentowane są na dashboardzie CogOps. Uwaga: skala opisuje stany operacyjne agenta, niezależna od skali pomiaru metryk (Cognitive SLA Tiers).

Metodyka CDF

Zobacz: Cognitive SLA, CogOps

[Hasło online](#)

Cognitive Observability

Obserwowalność kognitywna

Zdolność do szczegółowego monitorowania i logowania ścieżek rozumowania AI, działań agentów, zależności między nimi oraz wykorzystania źródeł wiedzy – umożliwiającą odtworzenie procesu decyzyjnego post-factum. W CDF stanowi element Fazy 6 (CogOps) i wspiera zgodność, audyt, troubleshooting oraz optymalizację jakości decyzji AI.

Podstawy AI

[Hasło online](#)

Cognitive Quality Reports

Raporty jakości kognitywnej

Comiesięczne raporty generowane w Fazie 4 i kolejnych, prezentujące wyniki metryk Cognitive SLA, trendy jakości rozumowania, incydenty kognitywne i rekomendacje optymalizacyjne.

Metodyka CDF

Zobacz: Cognitive SLA

[Hasło online](#)

Cognitive SLA

Umowa o poziomie usług kognitywnych

Wielowarstwowy system metryk jakości rozumowania systemów AI stosowany w CDF, wykraczający poza tradycyjne wskaźniki IT (uptime, latency). Mierzy gotowość, spójność, poziom halucynacji, świeżość wiedzy, skuteczność koordynacji agentów i zdolność do szybkiej mitygacji błędów. Breach procedura: Yellow (24h) → Orange (72h) → Red (7 dni lub halucynacje >5% w procesie krytycznym → Kill-Switch).

Podstawy AI

[Hasło online](#)

Cognitive SLA Tier

Poziom Cognitive SLA

Trójpoziomowy podział mechanizmu Cognitive SLA (blok Skale i taksonomie CDF): Tier 1 (CORE – 4 metryki bazowe: System Availability, Reasoning Accuracy Rate, Hallucination Rate, Mitigation Response Time), Tier 2 (AGENT + PRODUCTION – +2 metryki koordynacji: Agent Coordination, Confidence Calibration; łącznie 6 metryk), Tier 3 (SCALE lub SOVEREIGN – +Knowledge Freshness Index; łącznie 7 metryk + dashboardy CogOps). Każdy tier jest w pełni operacyjny na swoim poziomie; kolejne tiery dodają metryki, nie zastępują poprzednich.

Metodyka CDF

Zobacz: Knowledge Freshness Index, Mitigation Response Time, Reasoning Accuracy Rate, Confidence Calibration, System Availability

[Hasło online](#)

Cognitive Sprint

Kognitywny sprint

Iteracyjny cykl wdrożeniowy w metodyce CDF, analogiczny do Agile Sprint, ale skupiony na szybkim i kontrolowanym dostarczeniu wartości AI w warunkach compliance, audytowalności i pomiaru jakości rozumowania. Realizowany w Fazie 4 CDF.

Wdrożenie i zarządzanie

[Hasło online](#)

CogOps

Cognitive Operations

Operacyjna faza utrzymania systemów AI, obejmująca monitoring, optymalizację modeli, compliance, retraining, zarządzanie driftem, świeżością wiedzy i degradacją jakości działania. Jest to odpowiednik dojrzałego modelu operacyjnego dla systemów kognitywnych. W CDF realizowane w Fazie 6.

Podstawy AI

[Hasło online](#)

Compliance Gap Analysis

Analiza luk zgodności

Realizowany w Fazie 0 proces diagnozujący braki organizacji względem wymogów AI Act, norm ISO, regulacji sektorowych oraz wzorca umownego Ministerstwa Cyfryzacji. Stanowi podstawę planu naprawczego i dalszych decyzji architektonicznych.

Metodyka CDF

Zobacz: AI Act

[Hasło online](#)

Compliance Readiness Report

Compliance Readiness Report

Kluczowy artefakt F1.5 dokumentujący stan gotowości regulacyjnej organizacji.

Metodyka CDF

[Hasło online](#)

Compliance Timeline Tracker

Compliance Timeline Tracker

Interaktywny widok deadline'ów regulacyjnych (AI Act, CRA, NIS2/uKSC, CEN/CENELEC) zintegrowany z CDF Platform. Umożliwia śledzenie terminów zgodności i automatyczne powiadomienia.

Metodyka CDF

Zobacz: CDF Platform, NIS2/uKSC, AI Act

[Hasło online](#)

Compliance-First

Zgodność regulacyjna jako priorytet

Podejście, w którym wymagania prawne, regulacyjne i audytowe są traktowane jako warunek wstępny wdrożenia AI, a nie jako etap następczy. W CDF zgodność jest projektowana od początku i domykana przed odbiorem rozwiązania.

Wdrożenie i zarządzanie

[Hasło online](#)

Confidence Calibration

Confidence Calibration

Metryka Cognitive SLA (Tabela 14 Metodyki) mierząca korelację między deklarowaną pewnością odpowiedzi AI a jej poprawnością. Target: $r \geq 0,85$. Metryka Tier 2.

Podstawy AI

[Hasło online](#)

Conformity Assessment (Ocena zgodności)

Ocena zgodności systemu AI

Proces formalnej weryfikacji, czy system AI wysokiego ryzyka spełnia wymagania AI Act przed wprowadzeniem do obrotu (art. 43). CDF realizuje go w fazach F1.5 (Compliance-First Delivery, self-assessment) i F5 (Compliance Audit Report) – pozycja 10 matrycy E.1. Systemy z Załącznika III podlegają procedurze wewnętrznej oceny zgodności lub ocenie przez jednostkę notyfikowaną; obowiązki rozdz. III sekcji 1–3 stosuje się do nich od 02.12.2027, a do systemów z Załącznika I od 02.08.2028 (rozp. (UE) 2026/1744).

Regulacje i normy

AI Act

Zobacz: AI Act

[Hasło online](#)

Coordination Effectiveness

Skuteczność koordynacji

Metryka warstwy Agent SLA (Tabela 56 Metodyki, Załącznik A) mierząca jakość współpracy między agentami w realizacji złożonych zadań end-to-end.

Metodyka CDF

[Hasło online](#)

CORE (tag ACE)

Tag konfiguracyjny ACE

Tag ACE zawsze aktywny – rdzeń CDF obowiązkowy dla każdego wdrożenia AI niezależnie od profilu organizacji. Obejmuje podstawowe fazy, kontrole i artefakty.

Metodyka CDF

[Hasło online](#)

CRA (Cyber Resilience Act)

Cyber Resilience Act – Regulation 2024/2847

Rozporządzenie (UE) 2024/2847 ustanawiające obowiązkowe wymagania cyberbezpieczeństwa dla produktów z elementami cyfrowymi. Obejmuje: wymagania zasadnicze bezpieczeństwa (Security by Design – załącznik I), obowiązki producentów (art. 13), zgłaszanie aktywnie wykorzystywanych podatności i poważnych incydentów 24h/72h/14d (art. 14), SBOM (Software Bill of Materials), klasyfikację produktów ważnych i krytycznych (art. 7–8, załączniki III–IV), oznakowanie CE. Raportowanie podatności od 11.09.2026, pełna zgodność od 11.12.2027. Kary: do 15 mln EUR lub 2,5% obrotu. W CDF mapowane w sekcji D.2b i matrycy E.1.

Regulacje i normy

Zobacz: Vulnerability Disclosure (Zgłaszanie podatności), SBOM (Software Bill of Materials)

[Hasło online](#)

Critical ICT Provider (Krytyczny dostawca ICT)

Krytyczny dostawca usług ICT

Zewnętrzny dostawca usług ICT wyznaczony wspólnie przez Europejskie Urzędy Nadzoru (EBA, ESMA, EIOPA) jako krytyczny dla sektora finansowego (DORA, art. 31–44). Podlega bezpośredniemu nadzorowi wiodącego organu nadzorczego i wymogom testowania odporności. W CDF mapowany na F1.5 i F6 – Critical Provider Oversight.

Regulacje i normy

DORA

Zobacz: DORA

[Hasło online](#)

CRM

Customer Relationship Management

System do zarządzania relacjami z klientami, na przykład Salesforce lub Microsoft Dynamics. W CDF występuje jako jeden z typowych systemów integracyjnych w Fazie 1.

Wdrożenie i zarządzanie

[Hasło online](#)

Cross-Validation Guardrail

Reguła walidacji krzyżowej ACE

Automatyczna reguła sprawdzająca spójność konfiguracji ACE (Tabela 26 Metodyki). W 1.6.0 obowiązuje 13 reguł CV-00 do CV-12 w układzie warstwowym: Warstwa 0 – BLOCKING (CV-00: próba wyłączenia REGULATED przy FINANCE/GOV; CV-12: LOA > L2 w procesie rozstrzygającym GOV); Warstwa 1 – AUTO-CORRECT (CV-01 FINANCE→REGULATED, CV-02 GOV→REGULATED, CV-03 SOVEREIGN→REGULATED+GOV+CLASSIFIED, CV-04 multi-agent→AGENT, CV-10 HEALTH→REGULATED); Warstwa 1b – ADVISORY (CV-05 HCG-Full przy REGULATED, CV-06 Tier 3 przy SCALE/SOVEREIGN, CV-07 F6-Lite przy PRODUCTION, CV-08 F6-Full przy DEFENSE, CV-09 ekspozycja PLD przy fine-tuning, CV-11 dane szczególnej kategorii przy HEALTH); Warstwa 2 – ostrzeżenia merytoryczne MV-01 do MV-07 (Reguły spójności ACE, Tabela 27). Typy reguł zdefiniowane w bloku Skale i taksonomie CDF.

Metodyka CDF

Zobacz: REGULATED (tag ACE), HCG-Full, FINANCE (tag ACE), SCALE (tag ACE)

[Hasło online](#)

CV-12

Cross-Validation Rule 12 – ograniczenie LOA w procesach rozstrzygających

Reguła walidacji krzyżowej ACE typu BLOCKING, wprowadzona w 1.6.0. Deklaracja procesu rozstrzygającego w podpytaniu 3a Kwestionariusza Konfiguracyjnego wraz z tagiem GOV blokuje przypisanie poziomu autonomii powyżej L2. Warstwa 0 walidacji obejmuje od tego wydania dwie reguły: CV-00 i CV-12.

Metodyka CDF

Zobacz: Cross-Validation Guardrail

[Hasło online](#)

Data Act (rozp. 2023/2854)

Data Act – akt w sprawie danych

Rozporządzenie (UE) 2023/2854 w sprawie zharmonizowanych przepisów dotyczących sprawiedliwego dostępu do danych i ich wykorzystywania. Reguluje dostęp do danych generowanych przez produkty i usługi oraz przełączanie dostawców (interoperacyjność, unikanie vendor lock-in). W CDF adresowane w Załączniku E (kontrola VDP – przełączanie dostawców). Obowiązuje – stosowanie od 12 września 2025.

Regulacje i normy

[Hasło online](#)

Data Gravity

Grawitacja danych

Tendencja danych do przyciągania aplikacji i usług – im więcej danych znajduje się w jednym miejscu, tym trudniej je przenieść i tym większy wpływ mają na architekturę docelową. To kluczowe pojęcie przy projektowaniu środowisk AI.

Suwerenność i architektura

[Hasło online](#)

Data Gravity Assessment

Analiza grawitacji danych

Proces Fazy 0 badający cechy i położenie danych pod kątem ich wpływu na architekturę wdrożenia AI. Ocenia wolumen, tempo zmian, wymagania integracyjne, opóźnienia, regulacje, koszty zmiany i cykl życia danych.

Metodyka CDF

[Hasło online](#)

Data Gravity Index (DGI)

Indeks grawitacji danych

Siedmiowymiarowa miara grawitacji danych obliczana w Fazie 0 na podstawie wymiarów: Volume, Velocity, Latency, Integration, Regulation, Switching Cost i Lifecycle. Wynik pomaga określić, czy najlepsza będzie architektura sovereign on-premises, hybrid sovereign-cloud czy air-gapped defense. Zob. DGI.

Metodyka CDF

Zobacz: Latency

[Hasło online](#)

Data Provenance Tracking

Śledzenie pochodzenia danych

Mechanizm rejestrowania pełnej ścieżki danych – od źródła, przez transformacje, po wykorzystanie w decyzji agenta AI. Wprowadzony w CDF 1.4.4 jako element Fazy 6 (F6 Operate), oparty na rekomendacjach NIST dotyczących agentów AI. Zapewnia audytowalność, zgodność z AI Act i zdolność do odtworzenia podstaw każdej decyzji systemu kognitywnego.

Suwerenność i architektura

AI Act

Zobacz: AI Act

[Hasło online](#)

Deepfake

treść syntetyczna (deep fake)

Głos, obraz albo nagranie wygenerowane lub przerobione przez AI tak, by wydawały się prawdziwymi wypowiedziami albo zdarzeniami. AI Act wymaga, żeby taka treść była oznaczona jako wygenerowana albo zmanipulowana sztucznie. W rozmowie telefonicznej deepfake to najczęściej sklonowany głos bliskiej osoby albo „pracownika banku”

Podstawy AI

AI Act (art. 3 pkt 60, art. 50 ust. 4)

Zobacz: Klonowanie głosu, Transparency Notice (Powiadomienie o przejrzystości), Voicebot

[Hasło online](#)

Gdzie o tym piszemy: Gra TURING:AI

DEFENSE (tag ACE)

DEFENSE

Tag ACE aktywowany dla sektora obronnego (MON, Siły Zbrojne, infrastruktura krytyczna państwa). Włącza sekcje NATO PRU, K12 CBP, F6-Full, retraining pipeline. Zawsze aktywowany razem z tagami SOVEREIGN i GOV.

Metodyka CDF

Zobacz: SOVEREIGN (tag ACE), NATO PRU, F6-Full

[Hasło online](#)

Degradacja (modelu)

Model Degradation

Spadek skuteczności i poprawności działania modelu AI w środowisku produkcyjnym. W CDF degradacja podlega systematycznemu monitorowaniu w ramach CogOps i jest traktowana na równi z driftem jako ryzyko operacyjne.

Podstawy AI

[Hasło online](#)

Delegation Chain Protocol

Delegation Chain Protocol (CDF, na bazie NIST NCCoE)

Protokół łańcucha delegacji między agentami AI. Konstrukcja własna CDF rozwijająca filar autoryzacji z concept paper NIST NCCoE (5.02.2026). Nie jest cytatem z publikacji NIST. Obejmuje scenariusz „On Behalf Of” (token delegacji: tożsamość delegującego, scope, czas ważności, polityka eskalacji), łańcuch Agent → Sub-Agent z zasadą Scope Narrowing, Human Identity Binding i kaskadowe cofnięcie delegacji. Kontrola T-012 ext., faza F2; pełny łańcuch delegacji zapisywany w Immutable Audit Trail (A-F6-05); w matrycy E.4 artefakt oznaczony jako Delegation Chain Log.

Metodyka CDF

Zobacz: NIST

[Hasło online](#)

Deployer (Podmiot wdrażający)

Podmiot stosujący system AI (deployer)

Osoba fizyczna lub prawna, organ publiczny, agencja lub inny podmiot stosujący system AI pod swoją kontrolą (art. 3 pkt 4 AI Act; w polskim tekście rozporządzenia „podmiot stosujący”). Deployer ma obowiązki określone w art. 26: stosowanie zgodnie z instrukcją, nadzór ludzki, monitorowanie, informowanie, przechowywanie logów; dla podmiotów publicznych i wybranych sektorów dodatkowo FRIA (art. 27). W CDF rola Deployera jest mapowana na fazy F2 i F6.

Regulacje i normy

AI Act

Zobacz: AI Act

[Hasło online](#)

Gdzie o tym piszemy: Ustawa o systemach SI — co muszą Państwo wykazać

Gdzie o tym piszemy: ChatGPT Enterprise, Copilot czy własne

DevSecOps

Development, Security & Operations

Podejście integrujące praktyki bezpieczeństwa z procesami wytwarzania i utrzymania oprogramowania. W kontekście CDF stosowane do zarządzania cyklem życia komponentów AI z wbudowanym bezpieczeństwem na każdym etapie.

Suwerenność i architektura

[Hasło online](#)

DGA

Data Governance Act (Rozp. 2022/868)

Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2022/868 w sprawie europejskiego zarządzania danymi. Ustanawia ramy ponownego wykorzystywania danych sektora publicznego, usług pośrednictwa danych oraz altruizmu danych. W kontekście CDF istotne dla Fazy 1 (architektura danych) i obszaru K11 (suwerenność AI, lokalizacja danych), szczególnie przy wdrożeniach w sektorze publicznym wykorzystujących dane administracji.

Regulacje i normy

[Hasło online](#)

DGI

Data Gravity Index

Skrót od Data Gravity Index. Zob. Data Gravity Index (DGI).

Metodyka CDF

Zobacz: Data Gravity Index (DGI), Data Gravity

[Hasło online](#)

Diaryzacja

speaker diarization

Rozpoznanie w nagraniu, kto i kiedy mówi: transkrypcja zostaje podzielona na wypowiedzi przypisane do osób, z czasem każdej z nich. Dzięki temu z nagrania spotkania, przesłuchania albo wywiadu powstaje tekst, który można cytować i z którego da się wyprowadzić ustalenia i zadania. Nagrania często zawierają dane osobowe, więc ważne jest, gdzie są przetwarzane

Podstawy AI

RODO

Zobacz: LLM, Token, On-premises / On-prem

[Hasło online](#)

Gdzie o tym piszemy: SAIE Pantera

Digital Omnibus (EU)

EU Digital Package Omnibus Regulation

Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2026/1744 z dnia 8 lipca 2026 r. zmieniające rozporządzenia (UE) 2024/1689, (UE) 2018/1139 i (UE) 2023/1230 w zakresie uproszczenia wdrażania zharmonizowanych przepisów dotyczących sztucznej inteligencji. Ogłoszone w Dz.Urz. UE 24.07.2026, w mocy od 27.07.2026. Kluczowe zmiany: rozdz. III sekcje 1–3 dla zał. III (samodzielne systemy wysokiego ryzyka) – stosowanie od 02.12.2027 zamiast 02.08.2026; dla zał. I (systemy wbudowane w produkt) – od 02.08.2028 zamiast 02.08.2027; znakowanie maszynowo odczytywalne treści syntetycznych (art. 50 ust. 2) dla systemów wprowadzonych przed 02.08.2026 – do 02.12.2026; operacyjne piaskownice krajowe (art. 57) – do 02.08.2027; nowe zakazy w art. 5 (materiały przedstawiające seksualne wykorzystywanie dzieci, intymne wizerunki bez zgody) z okresem przejściowym do 02.12.2026; złagodzenie obowiązku kompetencji AI (art. 4); doprecyzowanie pojęcia elementu bezpieczeństwa (art. 6). Status: obowiązujące.

Regulacje i normy

AI Act · rozp. 2026/1744

Zobacz: AI Act

[Hasło online](#)

Digital Resilience Testing (TLPT)

Testowanie odporności cyfrowej

Program testowania odporności operacyjnej podmiotów finansowych wymagany przez DORA (art. 24–27). Obejmuje testy penetracyjne kierowane zagrożeniami (TLPT) co najmniej raz na 3 lata. W CDF mapowany na F4 i F6 – Digital Resilience Testing Programme (pozycja 35 matrycy E.1).

Regulacje i normy

DORA

Zobacz: DORA

[Hasło online](#)

DoD (Definition of Done)

Definicja ukończenia

Zbiór formalnych kryteriów, które muszą być spełnione, aby faza CDF mogła zostać uznana za zakończoną i nastąpiło przejście do kolejnej fazy. DoD jest specyficzny dla każdej fazy F0–F6 i obejmuje zarówno artefakty jak i warunki jakościowe. Źródło: Metodyka, sekcja Kryteria wejścia i wyjścia faz CDF. Wprowadzone w v1.4.4.

Wdrożenie i zarządzanie

[Hasło online](#)

DORA

Digital Operational Resilience Act (Rozp. 2022/2554)

Rozporządzenie Unii Europejskiej (2022/2554) dotyczące cyfrowej odporności operacyjnej sektora finansowego. W CDF adresowane przez DORA ICT Risk Mapping (F1.5), DORA Compliance Addendum (A-F15-08, tag FINANCE), wymagania dla dostawców ICT oraz strategię wyjścia i zarządzania ryzykiem stron trzecich (matryca E.1, art. 5–44).

Regulacje i normy

[Hasło online](#)

DPIA (Data Protection Impact Assessment)

Ocena Skutków dla Ochrony Danych

Formalna ocena wpływu operacji przetwarzania danych osobowych na prawa i wolności osób fizycznych, wymagana przez art. 35 RODO. W CDF obligatoryjna dla CBP (Cyfrowy Bliźniak Poznawczy), ponieważ obejmuje systematyczne profilowanie pracowników z wykorzystaniem AI. Realizowana w Fazie F1.5 (Compliance-First Delivery). Patrz: sekcja „Ochrona danych osobowych w CBP (RODO/DPIA)” w Metodyce.

Regulacje i normy

RODO

Zobacz: RODO

[Hasło online](#)

Gdzie o tym piszemy: ChatGPT Enterprise, Copilot czy własne — quiz z halucynacji

DPO / IOD (Inspektor Ochrony Danych)

Data Protection Officer / Inspektor Ochrony Danych

Osoba wyznaczona na mocy art. 37 RODO, odpowiedzialna za monitorowanie zgodności przetwarzania danych osobowych, współpracę z organem nadzorczym i doradzanie w zakresie DPIA. W CDF rola IOD jest mapowana na RACI Matrix (F1.5) z obowiązkowym przypisaniem w profilu compliance.

Regulacje i normy

RODO

Zobacz: RODO

[Hasło online](#)

Drift (Model Drift)

Dryfowanie modelu

Stopniowe pogarszanie się jakości przewidywań modelu AI w czasie, spowodowane zmianami danych wejściowych, środowiska operacyjnego lub zachowań użytkowników. Wymaga monitorowania, re-evaluacji i czasem retrainingu.

Podstawy AI

[Hasło online](#)

Dual-Orbit Sovereignty Matrix

Dual-Orbit Sovereignty Matrix

Narzędzie oceny ryzyka geopolitycznego stacku AI. Identyfikuje trzy orbity dostawców: US-orbit, CN-orbit, EU-sovereign. Ocenia: dostępność modeli, ryzyko sankcji, data residency, supply chain resilience, IP protection. Patrz: Załącznik F, sekcja 2.9.

Metodyka CDF

[Hasło online](#)

ECS

Enterprise Cognitive Systems

Systemy kognitywne klasy korporacyjnej – zaawansowane platformy AI zintegrowane z procesami przedsiębiorstwa, wspierające decyzje, automatyzację, analizę wiedzy i pracę agentową.

Podstawy AI

[Hasło online](#)

EHDS (rozp. 2025/327)

European Health Data Space

Rozporządzenie (UE) 2025/327 ustanawiające europejską przestrzeń danych zdrowotnych, regulujące pierwotne i wtórne wykorzystanie danych zdrowotnych oraz ich interoperacyjność. W CDF adresowane mechanizmem HDC (kontrola HDC-1, artefakt A-HDP-01), aktywowane tagiem HEALTH. Stosowanie fazowe: organy nadzoru od 26 marca 2027, pełne funkcjonalności 2029/2031.

Regulacje i normy

[Hasło online](#)

EN 18286:2026

EN 18286:2026 – Artificial intelligence: Quality management system for AI Act regulatory purposes

Pierwsza europejska norma wspierająca wdrożenie AI Act, opublikowana przez CEN/CENELEC 22.07.2026. Dotyczy systemu zarządzania jakością AI wymaganego art. 17 AI Act. Norma nie została przywołana w Dzienniku Urzędowym UE, więc jej stosowanie nie daje domniemania zgodności. Pozycja QMS-1 matrycy E.1, status pokrycia PARTIAL. Klasa źródła: N.

Regulacje i normy

AI Act

Zobacz: AI Act

[Hasło online](#)

Enterprise AI Catalog

Katalog rozwiązań AI

Wewnętrzna biblioteka gotowych i zwalidowanych przypadków użycia AI, dostępnych do ponownego wdrożenia w różnych częściach organizacji. Wspiera skalowanie w Fazie 5.

Wdrożenie i zarządzanie

[Hasło online](#)

ERP

Enterprise Resource Planning

System planowania zasobów przedsiębiorstwa, na przykład SAP lub Oracle. W CDF jest typowym systemem integracyjnym w architekturze enterprise AI.

Wdrożenie i zarządzanie

[Hasło online](#)

EU

European Union

Unia Europejska – organizacja ponadnarodowa będąca regulatorem m.in. AI Act, DORA, NIS2 i innych ram wpływających na wdrożenia AI w sektorach regulowanych.

Regulacje i normy

[Hasło online](#)

EU Database (Unijna baza danych systemów AI)

Unijna baza danych systemów AI wysokiego ryzyka

Baza danych prowadzona przez Komisję Europejską (art. 71 AI Act), w której rejestrowane są systemy AI wysokiego ryzyka przed wprowadzeniem do obrotu lub oddaniem do użytku (obowiązek rejestracji – art. 49). Większość wpisów jest publicznie dostępna; wpisy dotyczące organów ścigania i migracji znajdują się w części niepublicznej. W CDF realizowane w fazie F5 – EU Database Registration Process.

Regulacje i normy

AI Act

Zobacz: AI Act

[Hasło online](#)

Gdzie o tym piszemy: [Ustawa o systemach SI — klasyfikator AI Act](#)

Evidence Book

Warstwa dowodowa CDF

Załącznik G Metodyki CDF – artefakt wspierający warstwę dowodową metodyki. Obejmuje: EB-1 Mapowanie regulacyjne, EB-2 Case studies, EB-3 Przykładowe deliverables, EB-4 Warunki brzegowe claimów, EB-5 Benchmarki i metryki (w tym EB-5.2 baseline NASK 2026) oraz G.9 Kryteria Odbioru. Wprowadzony w v1.4.4, opracowany w v1.4.4-r4, rozszerzony w 1.6.0.

Wdrożenie i zarządzanie

[Hasło online](#)

Executive Alignment Workshop

Warsztat uzgodnienia kierowniczego

Warsztat dla C-Suite realizowany w Fazie 0, którego celem jest uzgodnienie priorytetów biznesowych, oczekiwanych rezultatów i horyzontów czasowych dla programu transformacji AI.

Wdrożenie i zarządzanie

[Hasło online](#)

Exit Strategy

Strategia wyjścia

Plan awaryjnego lub planowego zakończenia współpracy z dostawcą AI, obejmujący transfer danych, kodu źródłowego, dokumentacji i wiedzy operacyjnej. W CDF wymagana w Fazie 1.5 jako element compliance NIS2/uKSC i DORA.

Wdrożenie i zarządzanie

DORA

Zobacz: DORA

[Hasło online](#)

F6-AFC-01

Rejestr zgłoszeń kanału obaw AI (oznaczenie katalogowe A-F6-07)

Oznaczenie używane w sekcji F6 Metodyki dla artefaktu AI Concerns Feedback Channel Register; w Katalogu artefaktów CDF pozycja ta ma identyfikator A-F6-07 (Rejestr zgłoszeń kanału obaw AI, F6, CORE, właściciel CDF Lead, wprowadzony w 1.5.0). Dokumentuje konfigurację kanału (formularz, e-mail, portal), procedurę obsługi, SLA odpowiedzi, ścieżkę eskalacji, historię zgłoszeń i podjęte działania. Realizuje wymóg ISO/IEC 42001 Annex A – A.3.3; wyniki analizy zgłoszeń zasilają Evidence Book i cykliczne przeglądy ASIA.

Metodyka CDF

Zobacz: AI Concerns Feedback Channel, AI Act

[Hasło online](#)

F6-Full

Pełny tryb Fazy 6

Rozszerzony tryb Fazy 6 (CogOps) aktywowany tagiem SCALE lub DEFENSE (Tabela 38 Metodyki): F6-Lite + Knowledge Graph Governance, retraining pipeline, industrializacja CogOps i Biblioteka wzorców wdrożeniowych. Profile: DEFENSE, MULTI-JURIS.

Metodyka CDF

Zobacz: Cognitive Degradation Monitoring, Knowledge Freshness Index, CogOps, SCALE (tag ACE)

[Hasło online](#)

F6-Lite

Uproszczony tryb Fazy 6

Podstawowy tryb Fazy 6 (CogOps) aktywowany tagiem PRODUCTION (Tabela 38 Metodyki): monitoring operacyjny, alerty, compliance audit, periodic performance review. Wystarczający dla każdego wdrożenia produkcyjnego bez pełnej skali. Profile: STANDARD, STANDARD+AGENT, FINANCE, GOV, SOVEREIGN, ENTERPRISE, HEALTH.

Metodyka CDF

Zobacz: Cognitive SLA Tier, Cognitive SLA, PRODUCTION (tag ACE), CogOps

[Hasło online](#)

FINANCE (tag ACE)

Tag konfiguracyjny ACE

Tag ACE aktywowany dla sektora finansowego. Włącza sekcje DORA, ICT third-party risk, specyfikę KNF. Automatycznie wymusza REGULATED (guardrail CV-01, AUTO-CORRECT); brak DORA w pytaniu 7 generuje ostrzeżenie MV-01.

Metodyka CDF

Zobacz: REGULATED (tag ACE), DORA

[Hasło online](#)

Fine-tuning

Dostrajanie modelu

Proces dalszego trenowania wstępnie nauczonego modelu AI na specyficznym zbiorze danych w celu dostosowania go do konkretnej domeny, stylu lub typu zadań.

Podstawy AI

[Hasło online](#)

FRIA

Fundamental Rights Impact Assessment

Ocena wpływu na prawa podstawowe wymagana przez AI Act (art. 27) dla systemów AI wysokiego ryzyka wdrażanych przez podmioty prawa publicznego lub operatorów usług publicznych. W CDF realizowana jako element ASIA w Fazie F1.5.

Regulacje i normy

AI Act

Zobacz: AI Act

[Hasło online](#)

[Gdzie o tym piszemy: Ustawa o systemach SI — klasyfikator AI Act](#)

Fully On-Premises

Pełne wdrożenie lokalne

Wzorzec wdrożeniowy, w którym cała główna warstwa AI, dane, logi, orkiestracja agentów i integracje pozostają w infrastrukturze lokalnej klienta. Stosowany tam, gdzie kluczowe są suwerenność danych, kontrola operacyjna i ograniczenie ryzyka dostawcy.

Suwerenność i architektura

[Hasło online](#)

GDPR

General Data Protection Regulation (Rozp. 2016/679)

Ogólne rozporządzenie o ochronie danych osobowych Unii Europejskiej, stosowane bezpośrednio we wszystkich państwach członkowskich od 25 maja 2018 r. W Polsce funkcjonuje pod nazwą RODO; krajowa ustawa z dnia 10 maja 2018 r. o ochronie danych osobowych jedynie je uzupełnia. W CDF stanowi fundament wymagań dotyczących przetwarzania danych osobowych przez systemy AI. Zob. RODO.

Regulacje i normy

RODO

Zobacz: RODO

[Hasło online](#)

GEO (tag ACE)

Tag lokalizacyjny ACE

Warstwa jurysdykcyjna ACE działająca niezależnie od tagów sektorowych. Warianty: GEO:PL (Polska), GEO:EU (inny kraj UE/EOG), GEO:MULTI (wielojurysdykcyjne), GEO:NON-EU (poza UE).

Metodyka CDF

[Hasło online](#)

Global Rollout

Globalne wdrożenie / skalowanie

Proces realizowany w Fazie 5, polegający na replikacji ustandaryzowanych agentów, wzorców i komponentów AI na kolejne działy, jednostki lub obszary działalności.

Metodyka CDF

[Hasło online](#)

Gotowość dowodowa

Evidence Readiness

Zdolność organizacji do przedstawienia – na wypadek roszczenia z tytułu odpowiedzialności za produkt (dyrektywa PLD 2024/2853) – kompletnego, wiarygodnego materiału dowodowego (Agent Registry, logi decyzji, dokumentacja modelu, Evidence Book), pełniącego funkcję dowodu należytej staranności obalającego domniemania wadliwości i związku przyczynowego (art. 10 PLD). Realizowana kontrolą LER-1. Wprowadzona w CDF 1.5.0.

Wdrożenie i zarządzanie

PLD 2024/2853

Zobacz: PLD (dyrektywa 2024/2853)

[Hasło online](#)

GOV (tag ACE)

Tag konfiguracyjny ACE

Tag ACE aktywowany dla sektora publicznego lub obronnego. Włącza sekcje specyficzne dla administracji, NATO PRU, wzorzec MC, informacje niejawne. Automatycznie wymusza REGULATED.

Metodyka CDF

Zobacz: REGULATED (tag ACE), NATO PRU

[Hasło online](#)

Governance Divergence Matrix

Matryca rozbieżności governance US-EU

Narzędzie analityczne CDF (Załącznik F, sekcja 2.11, Tabela 84) porównujące podejścia regulacyjne UE i USA w obszarze AI governance. Obejmuje 8 obszarów: Safety Guardrails, Transparency / Disclosure, Data Ownership, Incident Reporting, Liability Model, Risk Classification, Bias / Fairness, Supply Chain Compliance. Dla każdego obszaru zestawia wymogi AI Act z klauzulą GSAR 552.239-7001 („American AI”, GSA 03/2026) i NIST AI RMF oraz wskazuje kontrolę i fazę CDF. Zasada ogólna: „strictest applicable” – dla wdrożeń obejmujących obie jurysdykcje stosuje się wymogi bardziej restrykcyjne (EU) z adnotacją o rozbieżności w SoA. Zob. US-EU AI Governance Divergence.

Metodyka CDF

Zobacz: Conformity Assessment (Ocena zgodności), AI Act, NIST

[Hasło online](#)

Groq 3 LPU

Groq 3 LPU / NVIDIA Groq 3 LPX

Akcelerator inferencyjny oparty na technologii Groq (LPU, używanej przez NVIDIA na licencji Groq, Inc.), oferowany przez NVIDIA jako Groq 3 LPX – rozszerzenie platformy Vera Rubin dla interaktywnego wnioskowania agentowego; pełna produkcja ogłoszona przez NVIDIA 24.08.2026 (wg NVIDIA 4-krotnie szybsza responsywność w zadaniach agentowych niż najbliższa platforma alternatywna). W CDF uwzględniany w benchmarkach infrastruktury obliczeniowej (Tabela 15 w Metodyce, gdzie figuruje jeszcze jako produkt Groq) jako referencja dla scenariuszy ultra-low-latency i agentowych workloadów K8.

Suwerenność i architektura

[Hasło online](#)

Ground Truth

Prawda referencyjna

Zweryfikowany, poprawny stan wiedzy lub odpowiedź służący jako punkt odniesienia do pomiaru trafności rozumowania AI. Używany w definicji metryki Reasoning Accuracy Rate w Cognitive SLA (Tabela 14 Metodyki).

Podstawy AI

[Hasło online](#)

Hallucination

Halucynacja modelu

Zjawisko generowania przez AI informacji nieprawdziwych, niepotwierdzonych lub nieopartych na wiarygodnych źródłach. W CDF zakłada się bardzo niską tolerancję dla tego zjawiska, a w procesach krytycznych jego aktywną mitygację i ciągły pomiar.

Podstawy AI

[Hasło online](#)

Gdzie o tym piszemy: [ChatGPT Enterprise, Copilot czy własne — quiz z halucynacji](#)

Gdzie o tym piszemy: [Baza wiedzy](#)

Hallucination Rate

Hallucination Rate

Metryka Cognitive SLA (Tabela 14 Metodyki) określająca procent odpowiedzi zawierających informacje niepotwierdzone w źródłach lub sprzeczne z bazą wiedzy. Targety CDF: $\leq 2\%$ dla zastosowań krytycznych, $\leq 5\%$ dla standardowych; przekroczenie 5% w procesie krytycznym uruchamia eskalację Red (Agent Kill-Switch). Metryka Tier 1 (bazowa, wymagana dla wszystkich profili).

Podstawy AI

[Hasło online](#)

HCG

Human Competence Gate

Skrót od Human Competence Gate. Zob. Human Competence Gate (HCG).

Wdrożenie i zarządzanie

Zobacz: [Human Competence Gate \(HCG\)](#)

[Hasło online](#)

HCG Audit Log Specification

HCG Audit Log Specification

Artefakt F2 definiujący format logowania interakcji człowiek-AI w ramach Human Competence Gate.

Metodyka CDF

Zobacz: [Human Competence Gate \(HCG\)](#)

[Hasło online](#)

HCG Control Policy

HCG Control Policy

Artefakt F2 definiujący zasady nadzoru ludzkiego nad systemem AI: kto zatwierdza jakie decyzje, przy jakim progu pewności.

Metodyka CDF

[Hasło online](#)

HCG-Full

Pełny tryb Human Competence Gate

Rozszerzony tryb HCG aktywowany tagami AGENT + REGULATED: pełna matryca HCG, checkpoint per use case, audit log decyzji, rejestr pytań kontrolnych, eskalacja, periodic review.

Metodyka CDF

Zobacz: REGULATED (tag ACE)

[Hasło online](#)

HCG-Lite

Uproszczony tryb Human Competence Gate

Podstawowy tryb HCG aktywowany tagiem CORE: minimum jeden checkpoint ludzki per wdrożenie AI, decyzja go/no-go przed uruchomieniem produkcyjnym, jasna definicja kto odpowiada za nadzór.

Metodyka CDF

Zobacz: CORE (tag ACE)

[Hasło online](#)

HDC

Health-AI Compliance

Mechanizm zgodności AI w sektorze zdrowia, osadzający w metodyce reżim aktywowany wejściem na rynek medyczny: EHDS (dostęp i wtórne wykorzystanie danych zdrowotnych), MDR/IVDR (kwalifikacja systemu AI jako oprogramowania wyrobu medycznego, sprzężona ze ścieżką wysokiego ryzyka zał. I AI Act) oraz RODO art. 9 (dane szczególnej kategorii). Bramkowany tagiem HEALTH. Obejmuje kontrole HDC-1 i HDC-2. Fazy F1.5/F2. Artefakty: A-HDP-01, A-MDR-01. Wprowadzony w CDF 1.5.0.

Metodyka CDF

Zobacz: A-HDP-01, A-MDR-01, AI Act, HEALTH (tag ACE), HDC-1

[Hasło online](#)

HDC-1

Health Data Governance

Kontrola CDF mechanizmu HDC: przetwarzanie danych szczególnej kategorii (RODO art. 9), wtórne wykorzystanie i interoperacyjność zgodnie z EHDS. Rozszerzenie mechanizmu K3 Data Governance (cegła istnieje – nie nowy mechanizm). Obszar wiedzy KD3. Fazy F1.5/F2. Artefakt A-HDP-01. Wprowadzona w CDF 1.5.0.

Metodyka CDF

Zobacz: A-HDP-01, EHDS (rozp. 2025/327), RODO

[Hasło online](#)

HDC-2

Medical Device AI Conformity

Kontrola CDF mechanizmu HDC: ocena kwalifikacji systemu AI jako oprogramowania wyrobu medycznego (MDR 2017/745 / IVDR 2017/746) i sprzężenie ze ścieżką wysokiego ryzyka zał. I AI Act. Nowa kontrola – CDF nie posiadał dotąd zgodności wyrobu medycznego. Obszar wiedzy KD8. Faza F1.5. Artefakt A-MDR-01. Wprowadzona w CDF 1.5.0.

Metodyka CDF

Zobacz: A-MDR-01, AI Act, IVDR (rozp. 2017/746)

[Hasło online](#)

HEALTH (tag ACE)

HEALTH – tag konfiguracyjny ACE

Tag konfiguracyjny ACE aktywowany, gdy wdrożenie dotyczy sektora zdrowia (dane zdrowotne, wyrób medyczny AI, EHDS). Włącza mechanizm HDC (kontrolę HDC-1/HDC-2) oraz reguły walidacji krzyżowej CV-10 (auto-aktywacja tagu REGULATED) i CV-11. Powiązany z profilem referencyjnym HEALTH. Wprowadzony w CDF 1.5.0.

Metodyka CDF

Zobacz: AGENT (tag ACE), CORE (tag ACE), FINANCE (tag ACE), GOV (tag ACE), PRODUCTION (tag ACE)

[Hasło online](#)

HITL

Human-in-the-Loop

Model nadzoru AI, w którym człowiek uczestniczy w procesie decyzyjnym lub może go zablokować, odwrócić albo skorygować. W CDF jest jednym z podstawowych mechanizmów governance i bezpieczeństwa.

Podstawy AI

AI Act

Zobacz: AI Act

[Hasło online](#)

HR

Human Resources

Obszar zarządzania zasobami ludzkimi. W CDF występuje zarówno jako potencjalny use case dla AI, jak i jako przykład domeny, w której poziom suwerenności może być niższy niż w systemach mission-critical.

Wdrożenie i zarządzanie

[Hasło online](#)

Human Competence Gate (HCG)

Kontrola kompetencji decydenta przed akceptacją decyzji AI

Mechanizm, w którym system AI przed dopuszczeniem użytkownika do zatwierdzenia decyzji generuje kontekstowo zależny zestaw pytań sprawdzających zrozumienie istotnych faktów, kluczowych konsekwencji oraz ograniczeń i wyjątków związanych z daną sprawą. Brak spełnienia zdefiniowanego progu poprawności blokuje zatwierdzenie decyzji i może skutkować eskalacją lub skierowaniem użytkownika do dodatkowego materiału szkoleniowego. Wdrażany od Fazy 2 CDF. System generuje 5–15 pytań kontekstowych typu Tak/Nie. Zob. HCG.

Wdrożenie i zarządzanie

[Hasło online](#)

Human Factors Monitoring

Human Factors Monitoring

Kategoria monitorowania post-deployment wg NIST AI 800-4 (pytanie kluczowe: czy system jest transparentny dla ludzi i wysokiej jakości). NIST wskazuje w niej: ograniczone rozumienie intencji i percepcji użytkownika, ciemne wzorce interakcji (sycophancy, antropomorfizacja), pętle sprzężenia zwrotnego człowiek–system oraz koszt zbierania i oceny opinii użytkowników. CDF rozszerza tę kategorię o wskaźniki własne: automation bias, skill degradation i overtrust (częstotliwość override'ów, czas walidacji outputów, wskaźnik eskalacji do człowieka). Element F5/F6 CogOps.

Wdrożenie i zarządzanie

Zobacz: NIST AI 800-4, NIST

[Hasło online](#)

Human Override

Nadpisanie przez człowieka

Mechanizm umożliwiający człowiekowi zatrzymanie, zablokowanie, cofnięcie albo skorygowanie decyzji podjętej przez system AI. W sektorach regulowanych stanowi podstawowy element realnego nadzoru człowieka.

Podstawy AI

[Hasło online](#)

Hybrid Sovereign-Cloud

Hybrydowa architektura suwerenna

Wzorzec wdrożeniowy, w którym dane krytyczne, pamięć organizacyjna, kontrola dostępu i kluczowe komponenty governance pozostają pod kontrolą organizacji, podczas gdy część mocy obliczeniowej lub modeli może działać w zaufanym środowisku chmurowym.

Suwerenność i architektura

[Hasło online](#)

ICT Security Addendum

Aneks bezpieczeństwa ICT

Uzupełnienie kontraktowe stosowane zwłaszcza w kontekście NIS2/uKSC, obejmujące klauzule bezpieczeństwa, prawo audytu, zarządzanie incydentami, backup, strategię wyjścia i ocenę dostawców ICT oraz AI. Wdrażany w Fazie 1.5 CDF.

Metodyka CDF

Zobacz: NIS2/uKSC

[Hasło online](#)

Immutable Audit Trail

Niemodyfikowalny dziennik zdarzeń

Log systemowy, którego wpisów nie można usunąć ani zmienić bez pozostawienia śladu. W CDF stanowi fundament automatycznego logowania, audytowalności i dowodowości działań AI oraz agentów.

Suwerenność i architektura

AI Act

Zobacz: AI Act

[Hasło online](#)

Inference / Inferencja

Wnioskowanie modelu

Faza działania modelu AI, w której wykonuje on predykcje, generuje odpowiedzi lub rekomendacje na podstawie nowych danych wejściowych.

Podstawy AI

[Hasło online](#)

Innovation Plateau Diagnostic

Diagnostyka plateau innowacji

Narzędzie Fazy 0 CDF (artefakt A-F0-07) diagnozujące Innovation Plateau – stan organizacyjny, w którym inwestycje w AI nie przekładają się na wartość biznesową. Identyfikuje 5 typów plateau: (1) Pilot Purgatory, (2) Scale Paralysis, (3) Governance Gridlock, (4) Cultural Resistance, (5) Data Readiness. Każdy typ ma indywidualny plan naprawczy w CDF.

Wdrożenie i zarządzanie

[Hasło online](#)

ISO/IEC 23894

ISO/IEC 23894:2023

Norma dotycząca zarządzania ryzykiem w systemach AI. Dostarcza wytycznych do identyfikacji, oceny i mitygacji ryzyk związanych z projektowaniem, wdrażaniem i użytkowaniem AI.

Regulacje i normy

ISO/IEC 42001

Zobacz: ISO/IEC 42001

[Hasło online](#)

ISO/IEC 42001

ISO/IEC 42001:2023

Norma definiująca system zarządzania sztuczną inteligencją (AIMS) – certyfikowalny system zarządzania dla organizacji rozwijających lub wdrażających AI, z katalogiem kontroli w załączniku A.

Regulacje i normy

Zobacz: AIMS

[Hasło online](#)

Gdzie o tym piszemy: [Polityka korzystania z AI — wzór](#)

Gdzie o tym piszemy: [ChatGPT Enterprise, Copilot czy własne — quiz z halucynacji](#)

IVDR (rozp. 2017/746)

In Vitro Diagnostic Regulation

Rozporządzenie (UE) 2017/746 w sprawie wyrobów medycznych do diagnostyki in vitro. Obejmuje oprogramowanie diagnostyczne, w tym systemy AI. W CDF adresowane kontrolą HDC-2 (artefakt A-MDR-01), łącznie z MDR.

Regulacje i normy

AI Act · MDR/IVDR

Zobacz: AI Act

[Hasło online](#)

J-curve of Productivity

Krzywa J produktywności

Zjawisko przejściowego spadku efektywności pracowników na początku wdrożenia AI. Parametryzacja CDF: dip –10% do –30% przez 3–9 miesięcy (F0– F3), inflection point (F4), acceleration +40–300% (F5–F6).

Mechanizmy przyczynowe ECS: osiągnięcie masy krytycznej KG, zakończenie Cognitive Succession, dojrzałość Skill Partnership. W CDF zjawisko to jest planowane i zarządzane jako element ROI Baseline i Scale Path Definition.

Wdrożenie i zarządzanie

[Hasło online](#)

Jednostka notyfikowana (SSI)

Notified Body

Jednostka oceniająca zgodność notyfikowana wg rozdz. III sekcji 4 AI Act; w Polsce organem notyfikującym jest minister właściwy ds. informatyzacji (art. 86–90 ustawy o systemach AI), przy wsparciu Polskiego Centrum Akredytacji. Faza F1 (ocena zgodności systemów wysokiego ryzyka).

Regulacje i normy

AI Act · ustawa o systemach SI

Zobacz: AI Act

[Hasło online](#)

Jurisdiction Compliance Card

Karta jurysdykcyjna

Artefakt ACE generowany w F0: dokument opisujący prawo bazowe, prawo krajowe, instytucje nadzorcze, timeline wymogów i artefakty specyficzne dla lokalizacji wdrożenia.

Metodyka CDF

[Hasło online](#)

Katalog artefaktów CDF

CDF Artifact Catalogue

Jedyne źródło wykazu artefaktów CDF (Tabela 6 Metodyki), wprowadzone w 1.6.0. Scala wykazy dotąd rozproszone w listach fazowych, artefaktach ACE, artefaktach CBP, rejestrze artefaktów SSI i opisach mechanizmów dziedzicznych. 94 pozycje z przypisaniem fazy, tagu aktywacji, właściciela z macierzy RACI, typu nośnika i wersji wprowadzenia. Liczba artefaktów aktywnych dla wdrożenia wynika z profilu ACE, nie z liczby pozycji katalogu.

Metodyka CDF

Zobacz: RACI

[Hasło online](#)

Katalog kontroli CDF

CDF Control Catalogue

Jedyne źródło wykazu kontroli CDF (Tabela 5 Metodyki), wprowadzone w 1.6.0. 34 kontrole w ośmiu rodzinach: T (kontrole metodyczne), MCP (bezpieczeństwo warstwy narzędziowej agentów), VDP (ciągłość dostawcy), SAG (bezpieczeństwo agentów), LER (gotowość dowodowa), CBC (ciągłość działania), HDC (sektor zdrowia), PAG (administracja publiczna). Każda kontrola ma przypisany obszar wiedzy, fazy, tag aktywacji, typ i powiązany artefakt.

Metodyka CDF

[Hasło online](#)

KG-RAG Integration Governance

Zarządzanie integracją KG-RAG

Zestaw zasad (Faza 6 CDF) zapewniających, że agenty generatywne korzystają wyłącznie z aktualnych, zwalidowanych źródeł w grafie wiedzy. Obejmuje mechanizmy Knowledge Freshness Monitoring i Knowledge Audit Trail.

Metodyka CDF

Zobacz: Knowledge Freshness Monitoring, Knowledge Audit Trail

[Hasło online](#)

Kill/Pivot Criteria

Kryteria przerwania lub zmiany kierunku

Z góry ustalone warunki, przy których pilotaż AI powinien zostać zakończony lub przekierowany. Element Scale Path Definition. Uwaga: odróżnić od Scale-or-Kill Gate – obowiązkowego binarnego punktu decyzyjnego (Scale / Kill) celowo eliminującego opcję „extend pilot”, gdzie „Kill” = pozytywny wynik (uniknięcie kosztownej inwestycji produkcyjnej).

Wdrożenie i zarządzanie

[Hasło online](#)

Klonowanie głosu

voice cloning

Odtworzenie głosu konkretnej osoby przez model AI na podstawie krótkiego nagrania, na przykład z filmu w mediach społecznościowych. Do sklonowania głosu wystarczy kilkanaście sekund nagrania. Oszuści używają tej techniki w metodzie „na wnuczka” i „na pracownika banku”, dlatego Policja radzi ustalić z bliskimi hasło rodzinne

Podstawy AI

AI Act (art. 50 ust. 4), RODO

Zobacz: Deepfake, Voicebot

[Hasło online](#)

Gdzie o tym piszemy: Gra TURING:AI

Knowledge Audit Trail

Ścieżka audytowa bazy wiedzy

Pełna, niezmienna (immutable) ścieżka audytowa rejestrująca wszystkie zmiany w bazie wiedzy organizacji. Spełnia wymogi regulatorów w zakresie transparentności i możliwości kontroli systemu AI (Faza 6 CDF).

Metodyka CDF

[Hasło online](#)

Knowledge Curator

Kurator wiedzy

Dedykowana rola organizacyjna odpowiedzialna za jakość, aktualność, bezpieczeństwo i wersjonowanie grafu wiedzy. Zarządza Ontology Change Control i wskaźnikami świeżości wiedzy. Rola wdrażana w Fazie 6 CDF.

Metodyka CDF

Zobacz: Ontology Change Control

[Hasło online](#)

Knowledge Debt Management

Zarządzanie długiem wiedzy

Systematyczna identyfikacja i eliminacja długu informacyjnego organizacji, obejmującego braki dokumentacyjne, silosy danych, nieaktualne procedury i rozproszenie wiedzy, które ograniczają skuteczność systemów AI. Realizowane w Fazie 6 CDF.

Podstawy AI

[Hasło online](#)

Knowledge Freshness Index

Indeks świeżości wiedzy

Miara wykorzystywana w Cognitive SLA, określająca jaki odsetek bazy wiedzy został zaktualizowany w zdefiniowanym oknie czasowym. Metryka Cognitive SLA Tier 3 (aktywna od profilu SOVEREIGN/SCALE). Target CDF: $\geq 95\%$ w 7-dniowym oknie czasowym.

Metodyka CDF

Zobacz: Cognitive SLA Tier, Cognitive SLA, SOVEREIGN (tag ACE), SCALE (tag ACE)

[Hasło online](#)

Knowledge Freshness Monitoring

Knowledge Freshness Monitoring

Automatyczny system alertów F6 wyzwalany przy przekroczeniu progu przedawnienia wiedzy w Knowledge Graph lub RAG.

Metodyka CDF

Zobacz: Knowledge Graph

[Hasło online](#)

Knowledge Graph

Graf wiedzy

Strukturalna reprezentacja wiedzy organizacyjnej w postaci grafu encji i relacji, stanowiąca fundament systemów RAG w CDF. Podlega ścisłemu Knowledge Graph Governance w Fazie 6 (Knowledge Curator, Ontology Change Control, KG-RAG Integration Governance).

Podstawy AI

[Hasło online](#)

Komisja Rozwoju i Bezpieczeństwa Sztucznej Inteligencji

Komisja Rozwoju i Bezpieczeństwa Sztucznej Inteligencji (KRiBSI)

Komisja Rozwoju i Bezpieczeństwa Sztucznej Inteligencji, zwana dalej Komisją, jest centralnym organem nadzoru rynku AI i pojedynczym punktem kontaktowym (art. 5). W jej skład wchodzi: Przewodniczący, 2 Zastępców oraz 4 członków wskazanych przez UOKiK, KNF, KRRiT i UKE – łącznie 7 osób (art. 19). Przewodniczącego powołuje na 5-letnią kadencję Sejm za zgodą Senatu (art. 28). Podstawa prawna: ustawa z dnia 3 lipca 2026 r. o systemach sztucznej inteligencji (Dz. U. z 2026 r. poz. 1003), obowiązująca od 11.08.2026; przepisy o kontroli, postępowaniu, układzie i karach oraz o opiniach indywidualnych – od 28.10.2026.

Regulacje i normy

AI Act

Zobacz: AI Act

[Hasło online](#)

[Gdzie o tym piszemy: Ustawa o systemach SI](#)

[Gdzie o tym piszemy: Baza wiedzy](#)

KPI

Key Performance Indicator

Kluczowy wskaźnik efektywności – mierzalna miara realizacji celu biznesowego, operacyjnego lub wdrożeniowego.

Wdrożenie i zarządzanie

[Hasło online](#)

Kryptografia postkwantowa (Post-Quantum Cryptography)

Kryptografia odporna na ataki kwantowe

Algorytmy kryptograficzne odporne na ataki z wykorzystaniem komputerów kwantowych. Strategia Cyberbezpieczeństwa RP 2025–2029 wymaga planu migracji kryptograficznej. CDF w Security Baseline (K8, F3/F4) uwzględnia ocenę gotowości kryptograficznej systemów AI.

Suwerenność i architektura

Zobacz: NIST

[Hasło online](#)

Kwantyzacja

Kwantyzacja modelu (quantization)

Zmniejszenie precyzji liczb w wagach modelu (np. z 16 do 8 lub 4 bitów), dzięki czemu model zajmuje kilkakrotnie mniej pamięci karty graficznej i działa szybciej kosztem niewielkiej utraty jakości. Decyduje o tym, czy model 11B zmieści się na karcie 24 GB, a 70B — na serwerze z kilkoma kartami

Podstawy AI

Zobacz: LLM, Inference / Inferencja, Bielik, PLLuM, Sovereign Compute

[Hasło online](#)

Gdzie o tym piszemy: [Bielik i PLLuM](#)

Kwestionariusz Konfiguracyjny

ACE Configuration Questionnaire

Interaktywna ankieta ACE (Tabela 25 Metodyki) służąca do ustalenia profilu konfiguracyjnego organizacji w trybie Self-Service. Część I: 7 pytań o cel wdrożenia, typy AI, sektor (z podpytaniem 3a o procesy rozstrzygające dla sektora publicznego i obronnego, od 1.6.0), rodzaj danych, skalę, lokalizację i wymogi compliance; Część I-A: walidacja krzyżowa (CV-00..CV-12, MV-01..MV-07); Część II: selekcja zgodności (WYMAGANE / REKOMENDOWANE / DOSTĘPNE).

Metodyka CDF

[Hasło online](#)

Latency

Opóźnienie

Czas potrzebny systemowi na odpowiedź lub wykonanie operacji. W architekturze AI ma znaczenie zarówno infrastrukturalne, jak i użytkowe.

Podstawy AI

[Hasło online](#)

LER

Liability Evidence Readiness

Rodzina mechanizmów CDF zapewniająca gotowość dowodową pod odpowiedzialność za produkt wynikającą z dyrektywy 2024/2853 (PLD), która czyni oprogramowanie i systemy AI produktem objętym odpowiedzialnością niezależną od winy. LER spina istniejące nośniki dowodowe (Agent Registry, Immutable Audit Trail, Evidence Book) w reżim umożliwiający obalenie domniemań wadliwości i związku przyczynowego (art. 9–10 PLD) oraz realizację obowiązku ujawnienia dowodów. Obejmuje kontrole LER-1 i LER-2. Fazy F1.5/F2/F6. Artefakt: A-PLD-01. Wprowadzony w CDF 1.5.0.

Metodyka CDF

Zobacz: Immutable Audit Trail, Agent Registry, Evidence Book, A-PLD-01, LER-1

[Hasło online](#)

LER-1

Product Liability Evidence Readiness

Kontrola CDF mechanizmu LER: utrzymanie kompletu dowodowego (dokumentacja modelu i danych, logi decyzji, Agent Registry, wersjonowanie, testy bezpieczeństwa) w stanie umożliwiającym obalenie domniemań z art. 10 dyrektywy PLD 2024/2853 oraz realizację obowiązku ujawnienia z art. 9, z ochroną tajemnicy przedsiębiorstwa. Obszary wiedzy KD8/KD6/KD3. Fazy F1.5/F2/F6. Wprowadzona w CDF 1.5.0.

Metodyka CDF

Zobacz: Agent Registry

[Hasło online](#)

LER-2

Substantial Modification Register

Kontrola CDF mechanizmu LER: rejestr znaczących modyfikacji (fine-tuning, ciągłe uczenie, aktualizacje) sygnalizujący moment, w którym podmiot wdrażający przechodzi w rolę producenta (art. 8 ust. 2 dyrektywy PLD 2024/2853) i przejmuje odpowiedzialność. Obszary wiedzy KD1/KD4. Fazy F2/F6. Wprowadzona w CDF 1.5.0.

Metodyka CDF

[Hasło online](#)

Liability Framework

Ramy odpowiedzialności prawnej AI

Struktura definiująca łańcuch odpowiedzialności prawnej za decyzje i działania systemu AI w środowisku produkcyjnym. Obejmuje trzy poziomy: odpowiedzialność operatora (deployer), dostawcy (provider) i organizacji (zarząd) jako właściciela systemu. W CDF powiązany z Accountability Matrix (per LOA, Załącznik B, Tabela 62) i mechanizmem LER (odpowiedzialność za produkt wg PLD 2024/2853) oraz mapowany na wymogi art. 9, 25 i 26 AI Act.

Regulacje i normy

AI Act

Zobacz: AI Act

[Hasło online](#)

LLM

Large Language Model

Duży model językowy trenowany na bardzo dużych zbiorach tekstu, zdolny do generowania języka naturalnego, streszczania, klasyfikacji, ekstrakcji informacji i wsparcia agentów.

Podstawy AI

[Hasło online](#)

Gdzie o tym piszemy: Bielik i PLLuM

LOA

Level of Autonomy

Skrót oznaczający poziom autonomii agenta AI w pięciostopniowej Skali Autonomii CDF (L0–L4). Zob. Skala Autonomii (L0–L4).

Podstawy AI

Zobacz: Skala Autonomii (L0–L4)

[Hasło online](#)

Make-vs-Buy Decision Framework

Framework decyzji Make vs Buy

Strukturalna ocena ekonomiczno-operacyjna realizowana w Fazie 0, dostarczająca uzasadnienia wyboru między budową rozwiązania AI wewnątrznie a zakupem gotowych komponentów lub usług. Uwzględnia TCO, ryzyko, czas wdrożenia i vendor lock-in.

Wdrożenie i zarządzanie

[Hasło online](#)

Mapa Kognitywna

Cognitive Map

Artefakt Fazy 0: wizualizacja procesów, danych, kompetencji i obszarów decyzyjnych organizacji pod kątem potencjału wdrożenia AI.

Podstawy AI

[Hasło online](#)

MC

Ministerstwo Cyfryzacji

Polskie Ministerstwo Cyfryzacji – autor projektu wzorcowych klauzul umownych dla zamówień publicznych na systemy AI (sygn. DPiS.WWKS.002.20.1.2026, pismo z 16.02.2026; projekt w konsultacjach, w CDF rekomendowana baza negocjacyjna, klasa M) oraz Przewodnika po sztucznej inteligencji dla administracji publicznej (marzec 2026, klasa M, podstawa mechanizmu PAG).

Regulacje i normy

AI Act

Zobacz: AI Act

[Hasło online](#)

MCP

Model Context Protocol

Otwarty protokół (Anthropic, 2024; specyfikacja w wersji 2026-07-28) standaryzujący komunikację między agentami AI a zewnętrznymi narzędziami, źródłami danych i usługami. W CDF podlega sześciu wymogom bezpieczeństwa MCP-REQ-01 do MCP-REQ-06 (autentykacja OAuth, walidacja wejścia, izolacja sieciowa z TLS 1.3, monitoring i audyt, ochrona przed tool poisoning, minimalne uprawnienia), realizowanym kontrolami MCP-CTL-01 do MCP-CTL-06 (Katalog kontroli, tag AGENT, artefakt A-F2-08). Zob. MCP Security.

Podstawy AI

[Hasło online](#)

MCP Security

MCP Security Requirements (wykładnia własna CDF)

Sześć wymogów bezpieczeństwa warstwy Model Context Protocol, oznaczonych MCP-REQ-01 do MCP-REQ-06. Numeracja i układ są wykładnią własną CDF i nie pochodzą ze specyfikacji MCP. Źródła: specyfikacja MCP w wersji 2026-07-28 (normatywna sekcja Authorization: OAuth 2.1, RFC 6750, 8414, 8707, 9207, 9728, OIDC Discovery oraz Client ID Metadata Documents; dynamiczna rejestracja klienta wg RFC 7591 jest oznaczona jako przestarzała i utrzymana wyłącznie dla zgodności wstecznej), dokument Security Best Practices (w części docs/tutorials/security specyfikacji) oraz Cybersecurity Information Sheet NSA AI Security Center „Model Context Protocol (MCP): Security Design Considerations for AI-Driven Automation”, ver. 1.0, maj 2026 (komunikat NSA z 20.05.2026; dokument wydany samodzielnie przez NSA, bez CISA). Realizowane kontrolami MCP-CTL-01 do MCP-CTL-06.

Suwerenność i architektura

Zobacz: MCP

[Hasło online](#)

MDR (rozp. 2017/745)

Medical Device Regulation

Rozporządzenie (UE) 2017/745 w sprawie wyrobów medycznych. Obejmuje oprogramowanie kwalifikowane jako wyrób medyczny, w tym systemy AI. W CDF sprzężone ze ścieżką wysokiego ryzyka zał. I AI Act, adresowane kontrolą HDC-2 (artefakt A-MDR-01).

Regulacje i normy

AI Act · MDR/IVDR

Zobacz: AI Act

[Hasło online](#)

MEP

Mechanical, Electrical & Plumbing

Infrastruktura techniczna budynku, obejmująca instalacje mechaniczne, elektryczne i sanitarne. Ma kluczowe znaczenie przy projektowaniu lokalnej infrastruktury AI i datacenter.

Suwerenność i architektura

[Hasło online](#)

MES

Manufacturing Execution System

System realizacji produkcji – oprogramowanie do zarządzania procesami wytwórczymi i operacyjnymi na poziomie wykonawczym.

Wdrożenie i zarządzanie

[Hasło online](#)

MFA

Multi-Factor Authentication

Uwierzytelnianie wieloskładnikowe – mechanizm weryfikacji tożsamości wymagający co najmniej dwóch niezależnych czynników (np. hasło + token sprzętowy). W CDF wymagane jako element Zero Trust w dostępie do systemów AI i paneli zarządzania agentami.

Suwerenność i architektura

[Hasło online](#)

Minimalizacja danych (Data Minimisation)

Zasada minimalizacji danych

Zasada RODO (art. 5 ust. 1 lit. c) wymagająca, aby dane osobowe były adekwatne, stosowne oraz ograniczone do tego, co niezbędne do celów przetwarzania. W CDF realizowane w F2 poprzez Data Governance Package i Data Quality Certificate.

Regulacje i normy

RODO

Zobacz: RODO

[Hasło online](#)

Minimum Sufficient Sovereignty (MSS)

Minimalna Wystarczająca Suwerenność

Zasada projektowa CDF zakładająca dobór takiego poziomu izolacji, lokalizacji i kontroli nad systemem AI, który jest wystarczający do spełnienia wymogów regulacyjnych, bezpieczeństwa, ciągłości działania i ochrony IP, ale nie jest większy niż to konieczne. Chroni organizację przed over-engineeringiem i under-engineeringiem architektury AI. Zob. MSS (Minimum Sufficient Sovereignty).

Suwerenność i architektura

[Hasło online](#)

Mitigation Response Time

Mitigation Response Time

Metryka Cognitive SLA (Tabela 14 Metodyki): czas od detekcji błędu kognitywnego do korekcji. Targety: ≤ 15 min krytyczne, ≤ 4 h standardowe. Metryka Tier 1.

Metodyka CDF

Zobacz: Cognitive SLA

[Hasło online](#)

Model Selection Compliance Matrix

Matryca zgodności wyboru modeli AI

Narzędzie decyzyjne CDF (Załącznik F, sekcja 2.10, Tabela 83) wspierające wybór modeli AI. Ocenia każdy model w 6 wymiarach na skali 1–5: Data Sovereignty, AI Act Compliance, Vendor Lock-in Risk, Censorship / Alignment Risk, Supply Chain Sanction Risk, Cost / TCO Transparency. Wynik sumaryczny (6–30 pkt) klasyfikuje model: 25–30 niskie ryzyko, 18–24 dopuszczalny z mitygacją, 12–17 wymaga eskalacji do zarządu, poniżej 12 niedopuszczalny (blokada w F2); w wariantcie CSE-GOV próg akceptacji to 20 pkt. Wypełniana w F0, aktualizowana w F2. Powiązana z Dual-Orbit Sovereignty Matrix i Vendor Disruption Protocol.

Metodyka CDF

Zobacz: Dual-Orbit Sovereignty Matrix, SBOM (Software Bill of Materials)

[Hasło online](#)

MSS (Minimum Sufficient Sovereignty)

Minimum Sufficient Sovereignty

Skróć od Minimum Sufficient Sovereignty. Minimalny wymagany poziom suwerenności AI dla danego profilu, określany w F0 na podstawie SLA-S. Patrz: Załącznik F. Zob. Minimum Sufficient Sovereignty (MSS).

Metodyka CDF

Zobacz: Minimum Sufficient Sovereignty (MSS), SLA-S

[Hasło online](#)

Multi-agent

Wieloagentowy system AI

Architektura, w której wiele autonomicznych agentów współpracuje, aby wykonać bardziej złożone zadania lub procesy end-to-end.

Podstawy AI

[Hasło online](#)

Multi-Jurisdiction Compliance Map

Mapa zgodności wielojurysdykcyjnej

Artefakt ACE generowany w F0 dla profilu GEO:MULTI: wymogi per jurysdykcja, konflikty regulacyjne, Cross-Border Data Transfer Assessment.

Metodyka CDF

[Hasło online](#)

MVOrg / MVOp (dawniej MVO)

Minimum Viable Organization (MVOrg) / Minimum Viable Operation (MVOp)

MVOrg (Minimum Viable Organization) – minimalna konfiguracja kompetencji, governance i zdolności technicznych wymagana przed inicjowaniem wdrożenia ECS (m.in. Executive Sponsor, rola Knowledge Curator, inwentaryzacja danych z F0). MVOp (Minimum Viable Operation) – minimalna operacyjna wersja procesu back-office realizowanego przez rój agentów AI (Autonomous swarm, LOA L2–L3) w kontrolowany sposób przed pełnym skalowaniem; trzeci poziom wdrożenia produkcyjnego w Fazie 4. Akronim MVO wycofany z użycia z uwagi na kolizję semantyczną.

Wdrożenie i zarządzanie

[Hasło online](#)

MVP

Minimum Viable Product

Wersja produktu z minimalnym zestawem funkcji wystarczającym do walidacji pomysłu lub kierunku rozwoju.

Wdrożenie i zarządzanie

[Hasło online](#)

Named Shortcut (ACE)

Nazwany skrót ACE

Profil referencyjny ACE (np. STARTER, FINANCE, SOVEREIGN) będący nazwanym skrótem dla typowej kombinacji tagów. Punkt wyjścia konfiguracji – organizacja może modyfikować tagi niezależnie od wybranego profilu.

Metodyka CDF

Zobacz: SOVEREIGN (tag ACE), FINANCE (tag ACE)

[Hasło online](#)

NASK

Naukowa i Akademicka Sieć Komputerowa

Państwowy instytut badawczy prowadzący CSIRT NASK – jeden z trzech zespołów CSIRT poziomu krajowego (obok CSIRT GOV i CSIRT MON) – oraz operator systemu S46. W kontekście CDF i uKSC/NIS2 – podmiot, któremu podmioty kluczowe i ważne zgłaszają incydenty cyberbezpieczeństwa.

Regulacje i normy

[Hasło online](#)

NASK GOV Prerequisites

Wymagania wstępne NASK GOV

Checklist wymagań wstępnych dla wariantu CSE-GOV (artefakt A-F0-11, tag GOV+GEO:PL, wprowadzony w CDF 1.5.0), weryfikowany w F0 przed przejściem do F1. Oparty na danych badania NASK 2026 i obejmuje: istnienie wewnętrznych procedur wdrożeniowych AI, plan szkoleniowy kadry, określenie poziomu nadzoru ludzkiego (LOA) oraz dostępność suwerennej infrastruktury AI (modele lokalne, data residency PL/EU). Uzupełnia GOV Deployment Prerequisites (Załącznik D.3).

Metodyka CDF

Zobacz: NASK

[Hasło online](#)

NATO PRU

NATO Principles of Responsible Use of AI

Zasady odpowiedzialnego użycia AI przyjęte przez NATO, obejmujące: lawfulness (zgodność z prawem), responsibility (odpowiedzialność), explainability (wyjaśnialność), reliability (niezawodność), governability (sterowność) i bias mitigation (ograniczanie uprzedzeń). W CDF adresowane dla sektora obronnego artefaktem A-F15-09 NATO PRU Compliance Addendum (tag DEFENSE).

Regulacje i normy

[Hasło online](#)

NGAC

Next Generation Access Control

Model kontroli dostępu nowej generacji, standard ANSI/INCITS 499 (NGAC-FA, architektura funkcjonalna) i ANSI/INCITS 525 (NGAC-IRPAD, wymagania implementacyjne, protokoły i API); porównanie z XACML w NIST SP 800-178. Oparty na atrybutach i politykach, umożliwia dynamiczne zarządzanie uprawnieniami agentów AI w środowisku wieloagentowym. W CDF stosowany jako rekomendacja dla Fazy 2 obok SPIFFE/SPIRE i SCIM.

Suwerenność i architektura

Zobacz: NIST

[Hasło online](#)

NIS2/uKSC

NIS2 / Krajowy System Cyberbezpieczeństwa

Dyrektywa (UE) 2022/2555 (NIS2) oraz wdrażająca ją znowelizowana ustawa o Krajowym Systemie Cyberbezpieczeństwa (uKSC) – regulacje cyberbezpieczeństwa dla podmiotów kluczowych i ważnych. Dla dostawców ICT/AI (CDF): klauzule bezpieczeństwa w umowach, prawo audytu, raportowanie incydentów ≤24h, zarządzanie ryzykiem łańcucha dostaw. Wdrożone w Fazie 1.5 jako ICT Security Addendum.

Regulacje i normy

[Hasło online](#)

NIST

National Institute of Standards and Technology

Amerykański instytut normalizacyjny przy Departamencie Handlu USA. W CDF przywoływany jako źródło frameworków: NIST AI RMF (zarządzanie ryzykiem AI), NIST SP 800-178 (porównanie XACML i NGAC), NIST AI 800-4 (CAISI, monitorowanie po wdrożeniu), NIST Cybersecurity Framework oraz badań NCCoE nad bezpieczeństwem agentów AI.

Regulacje i normy

[Hasło online](#)

NIST AI 800-4

NIST AI 800-4 – Challenges to the Monitoring of Deployed AI Systems

Raport NIST opracowany przez Center for AI Standards and Innovation (CAISI), opublikowany w marcu 2026 r. (komunikat NIST z 9.03.2026), analizujący bariery monitorowania systemów AI po wdrożeniu. Definiuje sześć kategorii monitorowania: Functionality, Operational, Human Factors, Security, Compliance, Large-Scale Impacts. Dokument nie formułuje wymagań normatywnych; CDF przejmuje z niego taksonomię kategorii jako podstawę artefaktu A-MON-01. Klasa źródła: N.

Regulacje i normy

Zobacz: NIST

[Hasło online](#)

Non-repudiation

Niezaprzeczalność

Właściwość systemu gwarantująca, że żaden uczestnik (człowiek ani agent) nie może zaprzeczyć wykonaniu lub zleceniu operacji. W CDF wymagana w Fazie 6 (artefakt A-F6-05 Immutable Audit Trail Specification, tag AGENT+REGULATED), rozwinięcie filarów NIST NCCoE. Realizowana poprzez kryptograficznie podpisane wpisy w Immutable Audit Trail (klucz agenta powiązany z Agent Identity Schema), tamper-proof storage, Human Authorization Binding i weryfikowalność zewnętrzną.

Suwerenność i architektura

[Hasło online](#)

North Star

Gwiazda Polarna / cel strategiczny

Nadrzędny cel strategiczny projektu AI: jeden mierzalny wynik biznesowy + ≤ 5 KPI + 90-dniowe kamienie milowe + koperta inwestycyjna. Zapobiega fragmentacji portfela inicjatyw AI. Służy jako framework ewaluacji dla Scale-or-Kill Gate. Delta vs. North Star Metric (Ellis 2017): wymiar enterprise transformation, nie product growth.

Wdrożenie i zarządzanie

[Hasło online](#)

Nudifier (Aplikacja Nudifier)

Nudifier Application

Aplikacja AI generująca obrazy nagości bez zgody osoby przedstawionej. Objęta zakazem dodanym do art. 5 ust. 1 AI Act rozporządzeniem (UE) 2026/1744 jako lit. ba (systemy generujące lub manipulujące realistycznymi intymnymi wizerunkami możliwej do zidentyfikowania osoby fizycznej bez jej zgody) i lit. bb (materiały przedstawiające seksualne wykorzystywanie dzieci w rozumieniu dyrektywy 2011/93/UE); dla systemów, dla których nie jest to przeznaczenie, wymagane są adekwatne techniczne środki zabezpieczające przed nadużyciem. Okres przejściowy upływa 2 grudnia 2026 r. W CDF uwzględnione w matrycy kar i sankcji (SSI-7) oraz w module prohibited practices F2.

Podstawy AI

[Hasło online](#)

OC

Odpowiedzialność Cywilna

Ubezpieczenie od odpowiedzialności cywilnej. W kontekście CDF dotyczy polis pokrywających szkody związane z wdrożeniem systemu AI.

Regulacje i normy

[Hasło online](#)

Ochrona informacji niejawnych (OIN)

Klasyfikacja i ochrona informacji niejawnych

Wymogi wynikające z ustawy z dnia 5 sierpnia 2010 r. o ochronie informacji niejawnych, dotyczące klauzul tajności (zastrzeżone / poufne / tajne / ściśle tajne), poświadczeń bezpieczeństwa personelu, akredytacji systemów teleinformatycznych oraz warunków przetwarzania. W CDF mapowane na F0 – GOV Deployment Prerequisites (dokument klasyfikacji, weryfikacja ABW/SKW).

Regulacje i normy

[Hasło online](#)

Odbiór

Acceptance

Formalne potwierdzenie przez Klienta, że wdrożenie spełnia kryteria zdefiniowane w Acceptance Criteria Checklist (F0-AC-01). Odbiór następuje po Fazie F5 (Skalowanie i Industrializacja), na podstawie weryfikacji wszystkich kryteriów odbioru – zarówno 6 kryteriów minimalnych rekomendowanych przez CDF (sekcja G.9), jak i kryteriów własnych Klienta. Protokół odbioru stanowi formalne zamknięcie fazy wdrożeniowej i warunek przejścia do F6 (CogOps).

Wdrożenie i zarządzanie

[Hasło online](#)

On-premises / On-prem

Wdrożenie lokalne

Model wdrożenia, w którym infrastruktura AI działa w fizycznej lokalizacji klienta lub organizacji, bez uzależnienia od chmury publicznej jako warstwy podstawowej.

Suwerenność i architektura

[Hasło online](#)

Gdzie o tym piszemy: Bielik i PLLuM

Gdzie o tym piszemy: ChatGPT Enterprise, Copilot czy własne

Ontology Change Control

Kontrola zmian ontologii

Rygorystyczna procedura zarządzania zmianami w ontologii grafu wiedzy, obejmująca wersjonowanie i zatwierdzanie zmian. Realizowana przez Knowledge Curator w Fazie 6 CDF, zapewniająca spójność i integralność bazy wiedzy systemu AI.

Metodyka CDF

Zobacz: Knowledge Curator

[Hasło online](#)

OpEx

Operational Expenditure / Wydatki operacyjne

Bieżące wydatki operacyjne na utrzymanie i eksploatację systemu AI (energia, licencje, wsparcie, retraining). W CDF uwzględniane w TCO Model 3–5 lat projektowanym w Fazie 1.

Wdrożenie i zarządzanie

Zobacz: CapEx

[Hasło online](#)

Opinia indywidualna

Opinia indywidualna Komisji

Interpretacja Komisji dotycząca stosowania AI Act lub ustawy do konkretnego systemu AI (art. 8–18). Opłata wynosi 150 zł (art. 11); termin to 30 dni albo 60 dni w sprawie szczególnie skomplikowanej (art. 12). Niewydanie opinii oznacza opinię zgodną ze stanowiskiem wnioskodawcy; opinia jest wiążąca w zakresie sprawy (art. 13) i po anonimizacji publikowana w BIP Komisji (art. 17).

Regulacje i normy

AI Act

Zobacz: AI Act

[Hasło online](#)

Opinia milcząca (SSI)

Milcząca opinia indywidualna

Skutek z art. 12 ust. 3 ustawy o systemach AI: niewydanie opinii indywidualnej w terminie 30 albo 60 dni uznaje się za wydanie opinii zgodnej ze stanowiskiem przedstawionym we wniosku, korzystnej dla wnioskodawcy.

Regulacje i normy

[Hasło online](#)

Orchestration

Orkiestracja

Proces koordynowania i zarządzania przepływem zadań między wieloma agentami AI, systemami lub komponentami w celu realizacji złożonego procesu biznesowego. W CDF każda orkiestracja podlega logowaniu w Immutable Audit Trail.

Podstawy AI

[Hasło online](#)

Organ notyfikujący (SSI)

Notifying Authority

Minister właściwy do spraw informatyzacji – organ notyfikujący jednostki oceniające zgodność AI (art. 86 ustawy o systemach AI); PCA współtworzy program akredytacji i informuje ministra w 14 dni o istotnych decyzjach akredytacyjnych.

Regulacje i normy

AI Act

Zobacz: AI Act

[Hasło online](#)

OWASP

Open Web Application Security Project

Międzynarodowa organizacja non-profit publikująca standardy i listy zagrożeń bezpieczeństwa aplikacji. W CDF podstawowym punktem odniesienia dla bezpieczeństwa agentów jest OWASP Top 10 for Agentic Applications 2026 (ASI01–ASI10, pełne pokrycie w Załączniku B), a komplementarnie OWASP Top 10 for LLM Applications 2026 (warstwa aplikacji opartych na LLM; edycja 2025 pozostaje referencją historyczną).

Regulacje i normy

[Hasło online](#)

OWASP ASI Mapping Matrix

OWASP Agentic Security Initiative Mapping Matrix

Tabela mapowania 10 ryzyk OWASP Top 10 for Agentic Applications 2026 (ASI01 Agent Goal Hijack, ASI02 Tool Misuse, ASI03 Identity & Privilege Abuse, ASI04 Agentic Supply Chain Vulnerabilities, ASI05 Unexpected Code Execution, ASI06 Memory & Context Poisoning, ASI07 Insecure Inter-Agent Communication, ASI08 Cascading Failures, ASI09 Human-Agent Trust Exploitation, ASI10 Rogue Agents) na kontrole, artefakty i fazy CDF. Patrz: Załącznik B, Tabela 58 (w Tabeli 58 nazwa ASI10 wymaga korekty na Rogue Agents).

Metodyka CDF

Zobacz: OWASP

[Hasło online](#)

PAG

Public Administration Guardrails

Rodzina trzech kontroli CDF dla administracji publicznej, wprowadzona w 1.6.0 i bramkowana tagiem GOV; moduł krajowy aktywuje tag GEO:PL. Obejmuje PAG-1 Necessity Gate, PAG-2 Human-Contact Fallback i PAG-3 Approved Tooling Register. Wszystkie kontrole mają charakter blokujący: niespełnienie zatrzymuje przejście bramki fazowej. PAG jest rodziną kontroli, nie tagiem konfiguracyjnym.

Metodyka CDF

Zobacz: PAG-1, PAG-2, PAG-3

[Hasło online](#)

PAG-1

Necessity Gate – bramka zasadności

Kontrola CDF (KD1, KD8; faza F0) rodziny PAG. Bramka zasadności zastosowania AI oparta na Etapie 0 Przewodnika MC po AI. Wyjście trójwartościowe: GO – uzasadnienie przyjęte; NO-GO – cel osiągalny prostszymi środkami, projekt zamknięty w F0; REDESIGN – zakres wymaga przeprojektowania. Wariant NO-GO jest równoprawnym wynikiem fazy F0. Artefakt A-GOV-01. W profilach innych niż GOV kontrola jest rekomendowana, nie obligatoryjna.

Metodyka CDF

Zobacz: A-GOV-01

[Hasło online](#)

PAG-2

Human-Contact Fallback – zastępcza ścieżka kontaktu z człowiekiem

Kontrola CDF (KD9, KD7; fazy F2 i F4) rodziny PAG. Każdy proces styku AI z obywatelem musi udostępniać alternatywny kanał obsługi prowadzący do pracownika: funkcję przełączenia do człowieka w każdym punkcie interakcji, kanał niezależny od systemu AI utrzymywany w deklarowanych godzinach oraz ścieżkę zgłoszenia zastrzeżeń, odrębną od kanału zgłaszania obaw AI z F6. Brak zastępczej ścieżki blokuje bramkę wyjścia z F4. Artefakt A-F2-16.

Metodyka CDF

Zobacz: A-F2-16

[Hasło online](#)

PAG-3

Approved Tooling Register – rejestr narzędzi zatwierdzonych

Kontrola CDF (KD6, KD1; fazy F2 i F6) rodziny PAG. Rejestr narzędzi AI dopuszczonych do użytku służbowego wraz z polityką korzystania z AI. Różni się od Shadow Agent Governance: SAG-4 wykrywa nieautoryzowanych agentów w architekturze systemu, PAG-3 obejmuje narzędzia GenAI używane przez pracowników poza architekturą wdrożenia. Obie kontrole zasilają wspólny przegląd w F6. Artefakty A-GOV-02 i A-GOV-03.

Metodyka CDF

Zobacz: SAG (Shadow Agent Governance), Shadow Agent Governance, A-GOV-02, A-GOV-03

[Hasło online](#)

PageIndex

indeks struktury dokumentu

Indeks, który odwzorowuje strukturę długiego dokumentu jako drzewo: rozdziały, paragrafy i fragmenty. Wyszukiwanie idzie po tej strukturze, a nie tylko po podobieństwie fragmentów, więc model trafia do właściwego rozdziału i może wskazać, skąd pochodzi odpowiedź. Przydatny przy instrukcjach, normach, umowach i aktach prawnych

Podstawy AI

Zobacz: RAG, Agentic RAG, LLM

[Hasło online](#)

Gdzie o tym piszemy: SAIE Pantera

PCOC (Połączone Centrum Operacyjne Cyberbezpieczeństwa)

Połączone Centrum Operacyjne Cyberbezpieczeństwa

Format koordynacji i bieżącego zarządzania cyberbezpieczeństwem na poziomie krajowym, organizowany przez Ministerstwo Cyfryzacji we współpracy z RCB i przewidziany w Strategii Cyberbezpieczeństwa RP 2025–2029 jako jeden z kierunków interwencji (rozwiniecie skrótu wg Sprawozdania Pełnomocnika Rządu do Spraw Cyberbezpieczeństwa). CDF w fazie F2/F3 wymaga identyfikacji CSIRT sektorowego i procedury raportowania incydentów spójnej z modelem koordynacji PCOC.

Regulacje i normy

[Hasło online](#)

Pętla agentyczna

agentic loop

Sposób pracy agenta AI, w którym agent sam dobiera kolejne działania do zadania i dostępnych informacji: planuje, sięga po wiedzę, wywołuje narzędzia i sprawdza wynik, aż zadanie zostanie wykonane. Przeciwnieństwo przepływu z góry ustalonych kroków (DAG). W środowiskach regulowanych plan agenta zatwierdza człowiek przed uruchomieniem, a historia wykonania zapisuje każdy krok

Podstawy AI

AI Act · ISO/IEC 42001

Zobacz: Agent (AI), Multi-agent, HITL, Agent Registry

[Hasło online](#)

Gdzie o tym piszemy: SAIE Pantera

Phase Gate

Bramka fazowa

Formalny punkt kontrolny na przejściu między fazami CDF (F0→F1→F1.5→F2→F3→F4→F5→F6). Każda bramka definiuje: kryteria wejścia (Entry Criteria), wymagane artefakty, kryteria wyjścia (Definition of Done). Przejście wymaga zatwierdzenia przez osobę Accountable z macierzy RACI. Źródło: Metodyka, sekcja Kryteria wejścia i wyjścia faz CDF. Wprowadzone w v1.4.4.

Wdrożenie i zarządzanie

Zobacz: RACI

[Hasło online](#)

Phase Rollback

Nawrót fazowy

Mechanizm powrotu do poprzedniej fazy CDF w przypadku niespełnienia kryteriów wyjścia (DoD) bieżącej fazy. Phase Rollback wymaga formalnej decyzji osoby Accountable i dokumentacji przyczyn nawrotu. Źródło: Metodyka, sekcja Kryteria wejścia i wyjścia faz CDF. Wprowadzone w v1.4.4.

Metodyka CDF

[Hasło online](#)

Piaskownica regulacyjna AI

Piaskownica regulacyjna AI (Sandbox)

Kontrolowane środowisko do testowania innowacyjnych systemów AI pod nadzorem Komisji (rozdz. 7, art. 91–103; przepisy obowiązują od 11.08.2026). Piaskownicę ustanawia Komisja, a zgody udziela w drodze decyzji (art. 91 ust. 1); unijny termin na uruchomienie krajowej piaskownicy wynosi 02.08.2027 (art. 57 AI Act w brzmieniu rozp. (UE) 2026/1744). Udział trwa 6–12 miesięcy; wybór następuje w konkursie, a udział MŚP jest nieodpłatny. Uczestnik składa raport roczny (art. 98) i może w terminie 90 dni od potwierdzenia uczestnictwa wystąpić o opinię indywidualną (art. 101). Ustawa nie ustanawia odrębnego limitu liczby użytkowników.

Regulacje i normy

AI Act

Zobacz: AI Act

[Hasło online](#)

[Gdzie o tym piszemy: Ustawa o systemach SI](#)

PKG

Personal Knowledge Graph

Osobisty graf wiedzy pracownika – ustrukturyzowana reprezentacja relacji między pojęciami, dokumentami, procesami i kontekstami, którymi operuje dany pracownik. Komponent architektury Cyfrowego Bliźniaka Poznawczego (CBP) obok Personal Language Model (PLM) i Profilu Interpretacyjnego (PI).

Metodyka CDF

Zobacz: PLM, PLM (Personal Language Model)

[Hasło online](#)

Plan monitoringu Technologies-in-Practice

Plan monitorowania praktyk technologicznych

Artefakt Fazy 3 służący obserwacji tego, jak pracownicy realnie korzystają z AI w praktyce oraz czy nie utrwalają się nieoptymalne, niebezpieczne lub niezgodne wzorce użycia.

Metodyka CDF

[Hasło online](#)

PLD (dyrektywa 2024/2853)

Product Liability Directive

Dyrektywa Parlamentu Europejskiego i Rady (UE) 2024/2853 w sprawie odpowiedzialności za produkty wadliwe, uchylająca dyrektywę 85/374/EWG. Obejmuje oprogramowanie i systemy AI jako produkt, wprowadzając odpowiedzialność niezależną od winy, obowiązek ujawnienia dowodów (art. 9) oraz domniemania wadliwości i związku przyczynowego (art. 10). Transpozycja do prawa polskiego do 9 grudnia 2026 r. W CDF adresowana mechanizmem LER (artefakt A-PLD-01).

Regulacje i normy

PLD 2024/2853

[Hasło online](#)

PLLuM

PLLuM (Polish Large Language Model)

Rodzina polskich modeli językowych konsorcjum HIVE AI pod kierunkiem NASK, finansowana przez Ministerstwo Cyfryzacji; trenowana na tekstach urzędowych i prawnych (m.in. Monitor Polski, Dziennik Ustaw, stenogramy sejmowe). Rozmiary 4–70 mld parametrów, licencja zależna od wariantu (Apache 2.0, Llama 3.3 albo CC BY-NC). Od 31.12.2025 odpowiada w asystencji aplikacji mObywatel

Podstawy AI

Zobacz: Bielik, LLM, NASK, Badanie NASK 2026, Kwantyzacja

[Hasło online](#)

Gdzie o tym piszemy: Bielik i PLLuM

PLM

Personal Language Model

Skrót od Personal Language Model. Zob. PLM (Personal Language Model).

Metodyka CDF

Zobacz: PLM (Personal Language Model)

[Hasło online](#)

PLM (Personal Language Model)

Personal Language Model – Osobisty Model Językowy

Indywidualnie dostrojony model językowy będący komponentem CBP (Cyfrowego Bliźniaka Poznawczego), obok Personal Knowledge Graph (PKG) i Profilu Interpretacyjnego (PI). PLM jest kalibrowany na stylu komunikacji, terminologii i wzorcach rozumowania konkretnego pracownika. Wymaga DPIA (art. 35 RODO) ze względu na przetwarzanie danych osobowych. PLM kalibrowany jest wyłącznie na danych związanych z rolą zawodową – dane prywatne i szczególnych kategorii (art. 9 RODO) są wykluczone. Wprowadzony w CDF 1.4.4; opisany w sekcji „K12: Cyfrowy Bliźniak Poznawczy (CBP)” Metodyki. Zob. PLM.

Podstawy AI

RODO

Zobacz: DPIA (Data Protection Impact Assessment), RODO

[Hasło online](#)

Polityka korzystania z AI

Polityka korzystania z AI (regulamin korzystania z AI)

Wewnętrzny dokument organizacji, który ustala, z jakich narzędzi AI wolno korzystać, jakich danych nie wolno do nich wprowadzać, kto odpowiada za wynik i jak oznacza się treści generowane przez AI. Podstawa do wykazania obowiązków podmiotu stosującego (AI Act art. 4 i 50) i wymóg ISO/IEC 42001; nazywana też regulaminem korzystania z AI

Wdrożenie i zarządzanie

AI Act · ISO/IEC 42001 · Kodeks pracy

Zobacz: Shadow AI, Deployer (Podmiot wdrażający), AI Act, ISO/IEC 42001, A-GOV-02

[Hasło online](#)

Gdzie o tym piszemy: [Polityka korzystania z AI — wzór](#)

Gdzie o tym piszemy: [Shadow AI](#)

Gdzie o tym piszemy: [Ustawa o systemach SI — co muszą Państwo wykazać](#)

Post-Deployment Monitoring

Monitorowanie po wdrożeniu

Proces ciągłego monitorowania systemu AI po uruchomieniu produkcyjnym, obejmujący 6 kategorii wg NIST AI 800-4: funkcjonalność, wydajność operacyjną, czynnik ludzki, bezpieczeństwo, zgodność regulacyjną i wpływ na dużą skalę. W CDF realizowany w fazach F5 (Skalowanie) i F6 (CogOps) poprzez mechanizmy nadzoru kognitywnego.

Wdrożenie i zarządzanie

AI Act

Zobacz: NIST AI 800-4, AI Act, NIST

[Hasło online](#)

Prawo do usunięcia (Right to Erasure)

Prawo do usunięcia danych / prawo do bycia zapomnianym

Prawo osoby, której dane dotyczą, do żądania usunięcia jej danych osobowych (art. 17 RODO). W CDF realizowane w F2 i F6 poprzez Data Lifecycle Management – mechanizm zarządzania retencją i usuwaniem danych w systemach AI.

Regulacje i normy

RODO

Zobacz: RODO

[Hasło online](#)

PRODUCTION (tag ACE)

Tag konfiguracyjny ACE

Tag ACE aktywowany dla wdrożeń produkcyjnych lub transformacji. Włącza pełne fazy F0–F4 (lub F0–F5 przy SCALE) oraz F6-Lite. NIE aktywuje wymogów compliance – tylko pełny flow wdrożeniowy.

Metodyka CDF

Zobacz: F6-Lite, SCALE (tag ACE)

[Hasło online](#)

Production Cost Model

Model kosztów produkcyjnych

Składowa Scale Path Definition określająca pełne koszty przejścia z pilotażu do środowiska produkcyjnego. Heurystyka CDF 380%: koszty produkcji stanowią średnio 380% kosztów pilotażu, rozkładane na 5 składowych: Infrastructure 2.0×, Compliance 3.5×, CogOps Staffing 4.0×, KG Population 2.5×, Security Hardening 3.0×. Obejmuje infrastrukturę, integracje, governance, utrzymanie, wsparcie i compliance.

Wdrożenie i zarządzanie

[Hasło online](#)

Profil HEALTH

Profil referencyjny HEALTH

Profil referencyjny ACE dla podmiotów ochrony zdrowia i dostawców AI medycznego. Archetyp: dane zdrowotne, wyrób medyczny AI, EHDS. Tagi aktywne: CORE + PRODUCTION + REGULATED + HEALTH + GEO:xx (+ AGENT gdy agenty). Fazy F0→F6-Lite, Cognitive SLA Tier 2, HCG-Full. Jedenasty profil referencyjny CDF. Karta: Tabela 52 w Metodyce. Wprowadzony w CDF 1.5.0.

Metodyka CDF

Zobacz: Cognitive SLA Tier, Cognitive SLA, PRODUCTION (tag ACE), REGULATED (tag ACE), HCG-Full

[Hasło online](#)

Prompt

Instrukcja / zapytanie do AI

Tekst wejściowy przekazywany do modelu LLM lub agenta AI w celu wykonania zadania, uzyskania odpowiedzi albo uruchomienia procedury.

Podstawy AI

[Hasło online](#)

Prompt Injection

Prompt Injection

Atak manipulacji wejściem systemu AI (bezpośredni lub pośredni, przez złośliwe instrukcje w danych lub treściach z narzędzi i źródeł); w OWASP Top 10 for Agentic Applications 2026 objęty pozycją ASI01 Agent Goal Hijack. W CDF mitygacja jest wymaganiem architektonicznym Cognitive Gateway (warstwa walidacji input/output z logowaniem prób ataku, obowiązkowa dla $LOA \geq L2$), adresowanym w K8 Security Baseline, kontrolą MCP-CTL-04 (MCP Input Validation) i SAG-1 (Memory Poisoning Detection).

Podstawy AI

Zobacz: OWASP

[Hasło online](#)

Gdzie o tym piszemy: [Polityka korzystania z AI — wzór](#)

Prompt Origin

Prompt Origin

Metadane źródła promptu: direct (użytkownik), template, agent, trigger. Element Cognitive Observability w F6.

Metodyka CDF

Zobacz: Cognitive Observability

[Hasło online](#)

Proporcjonalność (Proportionality)

Zasada proporcjonalności (DORA)

Zasada stosowania wymogów DORA proporcjonalnie do wielkości, profilu ryzyka oraz charakteru, skali i złożoności działalności podmiotu finansowego (art. 4). Mikroprzedsiębiorstwa korzystają z ułatwień na podstawie art. 4; uproszczone ramy zarządzania ryzykiem ICT (art. 16) dotyczą wskazanych kategorii małych podmiotów, m.in. małych i niepowiązanych firm inwestycyjnych oraz małych instytucji płatniczych. W CDF mapowane na F1.5 – Simplified ICT Framework.

Regulacje i normy

DORA

Zobacz: DORA

[Hasło online](#)

Przewodnik MC po AI

Przewodnik po sztucznej inteligencji dla administracji publicznej

Dokument Ministerstwa Cyfryzacji z marca 2026 r. Źródło klasy M w kanonie CDF: bez mocy wiążącej, lecz wyznaczające standard postępowania, wobec którego jednostka jest oceniana przez organ nadzoru i audytora. Ośmioetapowy proces wdrożenia od Etapu 0 (ocena zasadności) do Etapu 7 (przegląd okresowy), zestawienie „co robić / czego nie robić” w sześciu obszarach (w Metodyce: matryca nakazów i zakazów) oraz sześciopunktowa checklista decyzyjna dla pracownika. Mapowanie na fazy i kontrole CDF: Załącznik D.4. Podstawa mechanizmu PAG i ograniczenia $LOA \leq L2$.

Regulacje i normy

[Hasło online](#)

Psychological Readiness

Gotowość psychologiczna

Wymiar dojrzałości organizacyjnej oceniany w Fazie 0, odnoszący się do nastawienia pracowników, poziomu akceptacji zmiany, odporności na stres poznawczy i gotowości do współpracy z AI.

Wdrożenie i zarządzanie

[Hasło online](#)

Psychological Safety Protocol

Protokół bezpieczeństwa psychologicznego

Zestaw działań wdrażanych w Fazie 3, obejmujący pomiar bezpieczeństwa psychologicznego zespołu, przeciwdziałanie stygmatyzacji użytkowników AI, interwencje zarządzania zmianą oraz monitoring utrwalania nieoptymalnych praktyk użycia AI.

Metodyka CDF

[Hasło online](#)

Quality Management System (System zarządzania jakością)

System zarządzania jakością AI

System wymagany przez art. 17 AI Act dla dostawców systemów AI wysokiego ryzyka. Obejmuje: strategię zgodności regulacyjnej, procedury projektowania i rozwoju, testowania i walidacji, zarządzanie danymi, zarządzanie ryzykiem i system monitorowania po wdrożeniu. W CDF mapowany na F5 – AIMS Evidence Package i Quality Gate (pozycja 11 matrycy E.1). Normą wspierającą jest EN 18286:2026 (pozycja QMS-1 matrycy E.1, bez domniemania zgodności).

Regulacje i normy

AI Act · ISO/IEC 42001

Zobacz: ISO/IEC 42001, AI Act

[Hasło online](#)

RACI

Macierz odpowiedzialności

Macierz definiująca role w każdej fazie CDF (Tabela 16 Metodyki): R (Responsible – wykonuje), A (Accountable – zatwierdza), C (Consulted – konsultowany), I (Informed – informowany). Obejmuje 8 ról: Sponsor / CEO, CDF Lead / AI Architect, Compliance Lead, Security Officer (K8), Data Steward (K3), Business Owner, Operations / CogOps Team, Agent Governance Lead (K8). W profilach REGULATED Compliance Lead jest Accountable w fazach F1.5, F2 i F5; Sponsor zachowuje prawo weta w F0, F1 i F5. Właściciele artefaktów w Katalogu artefaktów pochodzą z tej macierzy. Wprowadzone w v1.4.4.

Wdrożenie i zarządzanie

[Hasło online](#)

Rada przy Komisji (SSI)

Rada – organ opiniodawczo-doradczy Komisji

Organ opiniodawczo-doradczy działający przy Komisji, w ustawie określony wyłącznie jako „Rada”, liczący od 9 do 15 członków wybieranych przez Komisję na 2-letnią kadencję (art. 45). Kandydatów zgłaszają m.in. strona samorządowa Komisji Wspólnej Rządu i Samorządu Terytorialnego, RPO, RPD, Rzecznik Praw Pacjenta, Rzecznik MŚP i Główny Inspektor Pracy. Opinie i stanowiska Rady nie są wiążące dla Komisji (art. 46). Komisja powołuje i odwołuje Przewodniczącego oraz Zastępcę Przewodniczącego Rady (art. 47).

Regulacje i normy

[Hasło online](#)

RAG

Retrieval-Augmented Generation

Architektura łącząca model generatywny z zewnętrzną bazą wiedzy, dzięki czemu odpowiedzi mogą być oparte na aktualnych i kontrolowanych źródłach, co ogranicza halucynacje.

Podstawy AI

Zobacz: Agentic RAG, PageIndex

[Hasło online](#)

Gdzie o tym piszemy: Bielik i PLLuM

Gdzie o tym piszemy: ChatGPT Enterprise, Copilot czy własne

Raport bazowy bezpieczeństwa psychologicznego

Raport bazowy bezpieczeństwa psychologicznego

Artefakt Fazy 3 dokumentujący wyjściowy poziom bezpieczeństwa psychologicznego zespołów przed wdrożeniem szerokiej współpracy człowiek–AI.

Metodyka CDF

[Hasło online](#)

RBAC

Role-Based Access Control

Model kontroli dostępu oparty na rolach organizacyjnych. W CDF stosowany jako bazowy mechanizm zarządzania uprawnieniami agentów AI, uzupełniany o NGAC i polityki atrybutowe w środowiskach wieloagentowych.

Suwerenność i architektura

Zobacz: NGAC

[Hasło online](#)

Reasoning Accuracy Rate

Wskaźnik trafności rozumowania

Procent odpowiedzi lub decyzji zgodnych z ground truth albo z oczekiwanym stanem wiedzy domenowej. Jedna z podstawowych metryk Cognitive SLA.

Podstawy AI

[Hasło online](#)

Recovery Rate

Wskaźnik odzyskiwania

Metryka warstwy Agent SLA (Tabela 56 Metodyki, Załącznik A) mierząca zdolność agenta do samodzielnego przywrócenia poprawnego działania po wykryciu błędu lub incydentu kognitywnego, bez interwencji człowieka.

Metodyka CDF

[Hasło online](#)

REDUCTION (flag)

Flaga redukcji zakresu

Flaga w ACE Profile Version Record sygnalizująca, że zmiana profilu była Scope Reduction (obniżenie zakresu). Wymaga pisemnego uzasadnienia i weryfikacji regulatory floor.

Metodyka CDF

Zobacz: ACE Profile Version Record, Scope Reduction

[Hasło online](#)

REGULATED (tag ACE)

Tag konfiguracyjny ACE

Tag ACE aktywowany dla sektora regulowanego lub gdy wdrożenie przetwarza dane osobowe/operacyjne. Włącza sekcje compliance, audytu, compliance-first delivery (Faza 1.5). Aktywowane przez sektor, dane lub lokalizację.

Metodyka CDF

[Hasło online](#)

Rejestr czynności przetwarzania (ROPA)

Records of Processing Activities

Rejestr prowadzony przez administratora danych zgodnie z art. 30 RODO, dokumentujący cele przetwarzania, kategorie danych, odbiorców, transfery do państw trzecich i planowane terminy usunięcia. W CDF realizowany w F2 poprzez Data Governance Package.

Regulacje i normy

RODO

Zobacz: RODO

[Hasło online](#)

Rejestr WORM

Rejestr WORM (write once, read many — zapis bez możliwości zmiany)

Rejestr zdarzeń zapisywany w trybie „write once, read many” — raz zapisanego wpisu nie da się zmienić ani usunąć. W środowisku AI obejmuje zapytania, odpowiedzi, użyte modele i decyzje polityk dostępu; jest dowodem dla kontroli (AI Act art. 26 ust. 6 — logi systemu wysokiego ryzyka co najmniej 6 miesięcy) i audytu ISO/IEC 27001 oraz 42001

Suwerenność i architektura

AI Act · ISO/IEC 27001

Zobacz: Immutable Audit Trail, Chain of Custody, Non-repudiation, Gotowość dowodowa

[Hasło online](#)

Gdzie o tym piszemy: Ustawa o systemach SI

Gdzie o tym piszemy: Shadow AI

Gdzie o tym piszemy: Bielik i PLLuM

Gdzie o tym piszemy: ChatGPT Enterprise, Copilot czy własne

Rejestr zasobów wielokrotnego użytku

Rejestr zasobów wielokrotnego użycia

Zbiór komponentów, wzorców, agentów, szablonów i artefaktów, które mogą być bezpiecznie reużyte w kolejnych wdrożeniach AI w ramach organizacji. Element Fazy 5 CDF.

Metodyka CDF

[Hasło online](#)

Release Quality Gate

Checklista jakości wydania

11-punktowa checklista kontroli jakości, którą każda wersja CDF musi przejść przed publikacją. Obejmuje: referencje, numerację, spójność faz, artefaktów, słownika, załączników, dat, claimów, skal, formatowania i triady wydania. Owner: Delivery Lead. Zatwierdzenie: Sponsor. Źródło: Metodyka, sekcja Checklista jakości wydania CDF. Wprowadzone w v1.4.4.

Metodyka CDF

[Hasło online](#)

Retraining

Ponowne trenowanie modelu

Aktualizacja modelu AI na nowych danych w celu poprawy skuteczności, dostosowania do zmian w domenie lub ograniczenia driftu.

Podstawy AI

[Hasło online](#)

Roadmap Dojrzałości

Maturity Roadmap

Artefakt ACE generowany w F0: ścieżka rozwoju od aktualnego profilu do wyższego z timeline. Np. STARTER → STANDARD w 6 miesięcy.

Wdrożenie i zarządzanie

[Hasło online](#)

RODO

Rozporządzenie o Ochronie Danych Osobowych

Polska nazwa Ogólnego rozporządzenia o ochronie danych (GDPR, Rozp. 2016/679). W CDF stanowi kluczowy wymóg regulacyjny dotyczący przetwarzania danych osobowych przez systemy AI, w tym profilowania, automatycznego podejmowania decyzji i transferu danych. Zob. GDPR.

Regulacje i normy

Zobacz: GDPR

[Hasło online](#)

ROI

Return on Investment

Zwrot z inwestycji – wskaźnik finansowy mierzący opłacalność projektu poprzez zestawienie uzyskanych korzyści z poniesionymi kosztami.

Wdrożenie i zarządzanie

[Hasło online](#)

ROI Baseline Report

Raport bazowy ROI

Artefakt Fazy 0 określający stan wyjściowy dla pomiaru korzyści biznesowych, uwzględniający również wpływ krzywej J produktywności.

Metodyka CDF

[Hasło online](#)

Root Cause Analysis

Analiza przyczyn źródłowych

Systematyczne badanie przyczyn incydentu lub błędu kognitywnego w celu wyeliminowania źródła problemu, a nie tylko jego objawów. W CDF wymagana w procedurze eskalacji Orange (72h) w ramach Cognitive SLA.

Podstawy AI

[Hasło online](#)

Rozporządzenie (UE) 2026/1744

Digital Omnibus on AI

Rozporządzenie zmieniające AI Act (2024/1689) oraz rozporządzenia (UE) 2018/1139 i (UE) 2023/1230.

Ogłoszone w Dz.Urz. UE 24.07.2026, w mocy od 27.07.2026. Źródło obowiązujących terminów stosowania AI Act stosowanych w CDF. Patrz: Digital Omnibus (EU).

Regulacje i normy

AI Act

Zobacz: Digital Omnibus (EU), AI Act

[Hasło online](#)

Rozporządzenie maszynowe (rozp. 2023/1230)

Machinery Regulation

Rozporządzenie (UE) 2023/1230 w sprawie maszyn, zastępujące dyrektywę 2006/42/WE. Obejmuje maszyny z systemami AI pełniącymi funkcje bezpieczeństwa. Stosowanie od 20 stycznia 2027; rozporządzenie (UE) 2026/1744 zmieniło zasady kwalifikacji maszyn z elementem AI jako systemów wysokiego ryzyka i przesunęło stosowanie obowiązków zał. I AI Act na 02.08.2028. Uwzględnione w Compliance Timeline Tracker (Tabela 20 Metodyki).

Regulacje i normy

AI Act

Zobacz: AI Act

[Hasło online](#)

SA-XAI

Situation Awareness Explainable AI

Autorskie podejście CDF do wyjaśnialności AI mapujące decyzje systemu na trzy poziomy świadomości sytuacyjnej wg modelu Endsley: percepcja, rozumienie i projekcja (przewidywanie stanu przyszłego).

Stosowane w Fazie 2 jako element środków przejrzystości AI, zapewniając operatorom właściwy kontekst do nadzoru.

Wdrożenie i zarządzanie

[Hasło online](#)

SAG (Shadow Agent Governance)

Rodzina kontroli SAG – bezpieczeństwo agentów (sekcja Shadow Agent Governance)

Akronim rodziny pięciu kontroli CDF (Katalog kontroli, tag AGENT, wprowadzone w 1.5.0) adresujących zagrożenia specyficzne dla systemów wieloagentowych: SAG-1 Memory Poisoning Detection, SAG-2 Cross-Session Hijacking Prevention, SAG-3 Confused Deputy Mitigation, SAG-4 Shadow Agent Detection Protocol, SAG-5 Agent Identity Audit. Kontrole obowiązują od LOA $\geq$ L2. Zob. Shadow Agent Governance.

Metodyka CDF

Zobacz: Shadow Agent Governance

[Hasło online](#)

SAVANT

SAVANT (nazwa własna produktu)

SAVANT to nazwa własna produktu allclouds.pl – suwerenny system kognitywny klasy enterprise. Nie wymaga definicji akronimowej. Strona produktu: www.savant-ai.app.

Metodyka CDF

[Hasło online](#)

SBOM (Software Bill of Materials)

Software Bill of Materials

Formalna inwentaryzacja wszystkich komponentów oprogramowania (biblioteki, modele AI, API, frameworki) wchodzących w skład produktu cyfrowego. Wymagany przez CRA (Cyber Resilience Act) jako warunek wstępny monitorowania podatności. W CDF realizowany w artefakcie Vendor AI Registry (K2/K8), obejmującym modele LLM, embedding, vector DB i inne komponenty kognitywne. Umożliwia śledzenie łańcucha dostaw AI i szybką reakcję na CVE dotyczące komponentów.

Regulacje i normy

CRA

Zobacz: CRA (Cyber Resilience Act)

[Hasło online](#)

SCALE (tag ACE)

Tag konfiguracyjny ACE

Tag ACE aktywowany dla organizacji enterprise (5000+ pracowników), transformacji lub wdrożeń multi-agent. Włącza sekcje skalowania, industrializacji, CBP, CogOps-Full, F6-Full.

Metodyka CDF

Zobacz: F6-Full

[Hasło online](#)

Scale Path Definition

Definicja ścieżki skalowania

Obowiązkowy artefakt Fazy 0 CDF precyzujący exit criteria pilotażu, ścieżkę do wdrożenia produkcyjnego, Production Cost Model oraz kryteria kill/pivot. Ma zapobiegać utknięciu organizacji na etapie pilotaży.

Metodyka CDF

Zobacz: Production Cost Model

[Hasło online](#)

Scale-or-Kill Gate

Brama decyzyjna Scale-or-Kill

Obowiązkowy binarny punkt decyzyjny na końcu pilotażu AI, celowo eliminujący opcję „extend pilot”. Dwa wyjścia: Scale (przejsięcie do produkcji) lub Kill (zakończenie). Kill = wynik pozytywny: uniknięcie kosztownej inwestycji produkcyjnej (heurystyka 380%). Pojęcie oryginalne CDF [CDF-ORIGINAL]. Odróżnić od Kill/Pivot Criteria (element Scale Path Definition).

Wdrożenie i zarządzanie

[Hasło online](#)

SCIM

System for Cross-domain Identity Management

Otwarty standard (RFC 7643/7644) automatyzujący zarządzanie tożsamościami użytkowników i agentów AI między systemami. W CDF stosowany jako rekomendacja dla provisioningu i deprovisioningu agentów w Agent Registry, zapewniający spójność tożsamości w środowisku wieloagentowym.

Suwerenność i architektura

[Hasło online](#)

Scope Reduction

Redukcja zakresu konfiguracji

Scenariusz ACE, w którym organizacja świadomie ogranicza ambicję wdrożenia (np. rezygnuje z transformacji na rzecz pilotażu). Podlega trzem wymogom: pisemne uzasadnienie, weryfikacja regulatory floor (wymogi WYMAGANE nie mogą być wyłączone), flaga REDUCTION w rekordzie wersji.

Wdrożenie i zarządzanie

[Hasło online](#)

Scoring Gotowości AI

AI Readiness Scoring

Kluczowy artefakt Fazy 0 kwantyfikujący dojrzałość organizacji do adopcji AI w wymiarach danych, governance, kompetencji i gotowości psychologicznej.

Wdrożenie i zarządzanie

[Hasło online](#)

Security by Default

Bezpieczeństwo domyślne

Zasada projektowa, zgodnie z którą bezpieczne ustawienia, polityki i ograniczenia są aktywne domyślnie, a nie dopiero po ręcznej konfiguracji.

Suwerenność i architektura

[Hasło online](#)

Security by Design

Bezpieczeństwo przez projektowanie

Zasada wbudowywania środków bezpieczeństwa w system AI od samego początku projektu, a nie dopiero po wdrożeniu.

Suwerenność i architektura

CRA

Zobacz: CRA (Cyber Resilience Act)

[Hasło online](#)

Shadow Agent Governance

Zarządzanie agentami nieautoryzowanymi

Sekcja Załącznika B definiująca rodzinę kontroli SAG (SAG-1 do SAG-5) dla systemów wieloagentowych, obowiązującą od LOA $\geq$ L2: SAG-1 Memory Poisoning Detection (walidacja integralności pamięci agenta, hash checkpoint, rollback; F2/F6), SAG-2 Cross-Session Hijacking Prevention (izolacja kontekstów sesji per agent, token z TTL; F2/F6), SAG-3 Confused Deputy Mitigation (least privilege i explicite scope w tokenie delegacji; F2), SAG-4 Shadow Agent Detection Protocol (inwentaryzacja agentów vs Agent Registry, skanowanie endpointów, monitoring ruchu, kwartalny audyt; F4/F6), SAG-5 Agent Identity Audit (periodyczny audyt tożsamości i uprawnień agentów; F6). Różni się od PAG-3: SAG-4 wykrywa nieautoryzowanych agentów w architekturze systemu, PAG-3 obejmuje narzędzia GenAI używane przez pracowników poza architekturą wdrożenia. Patrz: Załącznik B w Metodyce.

Podstawy AI

Zobacz: Shadow AI

[Hasło online](#)

Shadow AI

Nieautoryzowane użycie AI

Zjawisko nieautoryzowanego, niezarządzanego użycia narzędzi AI przez pracowników organizacji, poza kontrolą IT i governance. W CDF adresowane jako ryzyko w Fazie 0 (diagnostyka) i mitygowane przez AI Champions Program, CDF Academy oraz polityki governance.

Podstawy AI

[Hasło online](#)

Gdzie o tym piszemy: Shadow AI

Gdzie o tym piszemy: Ustawa o systemach SI — co muszą Państwo wykazać

Gdzie o tym piszemy: Polityka korzystania z AI — wzór

SIEM

Security Information and Event Management

System zarządzania informacjami i zdarzeniami bezpieczeństwa, agregujący logi i alerty z wielu źródeł w celu wykrywania zagrożeń i incydentów. W CDF integrowany z warstwą Immutable Audit Trail i monitoringiem agentów AI.

Suwerenność i architektura

[Hasło online](#)

Single Agent

Pojedynczy agent AI

Agent AI odpowiedzialny za jedno dyskretne zadanie, na przykład klasyfikację dokumentów, ekstrakcję danych lub przygotowanie rekomendacji.

Podstawy AI

Zobacz: Agent (AI)

[Hasło online](#)

Skala Autonomii (L0–L4)

Pięciopoziomowa skala autonomii agentów AI (L0–L4)

Standardowy model CDF definiujący zakres uprawnień decyzyjnych agenta: L0 Human-only (agent wyłącznie doradza, człowiek podejmuje wszystkie decyzje i akcje), L1 Human-in-the-loop (agent wykonuje, człowiek zatwierdza każdą akcję), L2 Human-on-the-loop (agent wykonuje, człowiek nadzoruje i może przerwać), L3 Human-over-the-loop (agent autonomiczny w zdefiniowanych ramach), L4 Full autonomy (wyłącznie procesy back-office non-critical).

Podstawy AI

[Hasło online](#)

Skale i taksonomie CDF

CDF Scales and Taxonomies

Blok definicyjny wprowadzony w 1.6.0, jedyne źródło poziomów skal CDF: LOA (L0–L4), CFL (CFL-1 do CFL-5), guardrails ACE (BLOCKING, AUTO-CORRECT, ADVISORY), tiery Cognitive SLA, tiery HCG, tiery F6 CogOps, skala degradacji kognitywnej, eskalacja Cognitive SLA, poziomy suwerenności AI (Poziom 1–3) i poziomy suwerenności compute (S1–S4). Pozostałe sekcje metodyki odwołują się do poziomu i nie powtarzają definicji ani liczby elementów.

Metodyka CDF

Zobacz: Cognitive SLA, CogOps

[Hasło online](#)

Skill Partnership

Partnerstwo kompetencyjne

Model współpracy ujęty w postaci matrycy w Fazie 3, w którym człowiek i agent AI wzajemnie uzupełniają kompetencje i tworzą bardziej efektywny układ działania.

Wdrożenie i zarządzanie

[Hasło online](#)

SLA

Service Level Agreement

Umowa o poziomie usług definiująca gwarantowane parametry działania, takie jak dostępność, czas reakcji lub jakość obsługi.

Suwerenność i architektura

[Hasło online](#)

SLA-S

Sovereignty Level Assessment

Skrót używany dla oceny poziomu suwerenności realizowanej w Fazie 0, służącej do przypisania właściwego wzorca wdrożeniowego AI dla danego obszaru biznesowego.

Metodyka CDF

[Hasło online](#)

SoA

Statement of Applicability

Deklaracja stosowania – dokument określający, które kontrole i wymagania normy (w CDF: 38 kontroli ISO/IEC 42001 Annex A) są włączone lub wyłączone w kontekście konkretnego wdrożenia, wraz z uzasadnieniem, właścicielem i powiązаныmi artefaktami. W CDF artefakt Fazy F1.5 (A-F15-02, tag REGULATED), wymagany przy certyfikacji AIMS. Zob. Statement of Applicability.

Regulacje i normy

ISO/IEC 42001

Zobacz: ISO/IEC 42001

[Hasło online](#)

SOKiK (właściwość AI)

Sąd Ochrony Konkurencji i Konsumentów

Sąd Okręgowy w Warszawie – SOKiK, właściwy dla odwołań od decyzji i zażaleń na postanowienia Komisji (nowy Dział IVfa KPC „Postępowanie w sprawach z zakresu sztucznej inteligencji”, art. 115 ustawy). Opłaty sądowe: 1000 zł (odwołanie, apelacja, kasacja), 500 zł (zażalenie) – art. 120.

Regulacje i normy

[Hasło online](#)

SOVEREIGN (tag ACE)

Tag konfiguracyjny ACE

Tag ACE aktywowany dla wdrożeń z informacjami niejawnymi lub infrastrukturą krytyczną. Włącza sekcje pełnej suwerenności: air-gap, EuroHPC, Hardware Binding oraz moduł suwerenności ASIA (sekcje 11–20).

Automatycznie wymusza REGULATED + GOV + CLASSIFIED (guardrail CV-03); aktywuje Cognitive SLA Tier 3 (CV-06).

Metodyka CDF

Zobacz: REGULATED (tag ACE)

[Hasło online](#)

Sovereign AI

Suwerenna AI

Model wdrożenia i eksploatacji AI, w którym organizacja zachowuje wysoką lub pełną kontrolę nad danymi, modelem, logami, integracjami i warstwą operacyjną.

Suwerenność i architektura

[Hasło online](#)

Sovereign AI Rationale

Uzasadnienie suwerennej architektury AI

Uzasadnienie strategicznych, regulacyjnych i operacyjnych przesłanek wyboru suwerennej architektury AI, opracowywane w fazie F0 jako element Sovereignty Level Assessment (wejście do A-F0-04 SLA-S Report i A-F1-04 Sovereignty Architecture Decision Record). Obejmuje: analizę ryzyk geopolitycznych, wymogi data residency, zgodność z AI Act i NIS2/uKSC, ocenę Dual-Orbit Sovereignty Matrix oraz uzasadnienie poziomu suwerenności (MSS). Baseline NASK 2026 (75% wskazań na krajowe instytucje publiczne) stanowi wejście do uzasadnienia w profilu GOV. Wymagany dla profili GOV, SOVEREIGN i DEFENSE. Nie ma odrębnej pozycji w Katalogu artefaktów CDF.

Metodyka CDF

Zobacz: Dual-Orbit Sovereignty Matrix, NIS2/uKSC, SOVEREIGN (tag ACE), DEFENSE (tag ACE), AI Act

[Hasło online](#)

Sovereign Compute

Suwerenne zasoby obliczeniowe

Infrastruktura obliczeniowa oceniana pod kątem kontroli prawnej i operacyjnej organizacji lub państwa. CDF definiuje cztery poziomy suwerenności compute (blok Skale i taksonomie CDF; Załącznik F, sekcja 2.6, Tabela 81): S1 Sovereign (infrastruktura, zarządzanie i dane w EU, np. EuroHPC AI Factories), S2 EU-compliant (hyperscaler z regionem EU, umowa pod prawem EU), S3 Non-EU (infrastruktura poza EU, ryzyko jurysdykcyjne), S4 Self-Hosted (model open-weight on-premises bez zależności zewnętrznych). Skala jest rozłączna wobec poziomów suwerenności AI (Poziom 1–3). CSE-GOV wymaga minimum S1 lub S2; wybór S3 dla danych regulowanych wymaga uzasadnienia w Compliance Readiness Report.

Suwerenność i architektura

[Hasło online](#)

Sovereign Deployment Pattern

Wzorzec wdrożenia suwerennego

Ostateczny wybór modelu operacyjnego infrastruktury AI dokonywany w Fazie 1 CDF na podstawie Data Gravity Assessment i Sovereignty Level Assessment, spośród trzech opcji: Fully On-Premises (pełna suwerenność), Hybrid Sovereign-Cloud (dane krytyczne lokalnie, obliczenia w chmurze) i Air-Gapped Defense (fizyczna izolacja sieciowa dla sektora obronnego).

Metodyka CDF

Zobacz: SLA-S, Sovereignty Level Assessment (SLA-S), Data Gravity Assessment, Hybrid Sovereign-Cloud, Air-Gapped Defense

[Hasło online](#)

Sovereignty Dimensions

Wymiary suwerenności

Cztery kryteria oceny wymaganego poziomu suwerenności AI: klasyfikacja danych, ekspozycja regulacyjna, krytyczność operacyjna oraz zależność łańcucha dostaw.

Suwerenność i architektura

[Hasło online](#)

Sovereignty Level Assessment (SLA-S)

Ocena poziomu suwerenności

Narzędzie Fazy 0 badające dany obszar biznesowy w czterech wymiarach w celu przypisania go do odpowiedniego poziomu i wzorca wdrożeniowego AI. Chroni organizację przed przewymiarowaniem lub niedoszacowaniem poziomu izolacji i kontroli.

Metodyka CDF

[Hasło online](#)

SPIFFE/SPIRE

Secure Production Identity Framework / SPIFFE Runtime Environment

Standard CNCF (Secure Production Identity Framework for Everyone) i jego implementacja referencyjna (SPIRE) do zarządzania tożsamością obciążeń (workload identity) w środowiskach rozproszonych. W CDF stosowany jako rekomendacja dla identyfikacji agentów AI w Agent Identity Schema, zapewniający kryptograficznie weryfikowalne tożsamości bez polegania na współdzielonych sekretach.

Suwerenność i architektura

[Hasło online](#)

Statement of Applicability

Statement of Applicability (SoA)

Zob. SoA. Dokument Fazy F1.5 (artefakt A-F15-02) mapujący 38 kontroli ISO/IEC 42001 Annex A na fazy, artefakty i mechanizmy CDF, z decyzją o włączeniu lub wyłączeniu każdej kontroli, uzasadnieniem, właścicielem i statusem pokrycia (ALIGNED / PARTIAL). Generowany na podstawie profilu ACE; dokument żywy – aktualizowany przy każdej zmianie zakresu, co najmniej raz w roku w ramach przeglądu F6. Patrz: Tabela 8 w Metodyce.

Regulacje i normy

Zobacz: SoA

[Hasło online](#)

Status standardu

Standard Status

Oznaczenie stanu pozycji kanonu źródeł CDF. W Compliance Timeline Tracker (Tabela 20) i nacie do matrycy E.4 stosowane są wartości: Published (opublikowany i obowiązujący), Draft (projekt w konsultacjach), Pending (oczekuje na zatwierdzenie lub ogłoszenie), Brak / projekt. Kolumna Status matrycy E.1 wyraża natomiast status pokrycia wymogu przez CDF: ALIGNED, PARTIAL, GAP oraz RESERVED (mapowanie zarezerwowane do czasu publikacji standardu). Od 1.6.0 moc źródła określa dodatkowo kolumna Klasa (W, M, N, D – zob. Taksonomia źródeł CDF).

Metodyka CDF

[Hasło online](#)

Strategia Cyberbezpieczeństwa RP 2025–2029

Narodowa strategia cyberbezpieczeństwa

Dokument strategiczny przyjęty przez Radę Ministrów 10 marca 2026 r., wyznaczający 6 celów szczegółowych wzmacniających Krajowy System Cyberbezpieczeństwa. CDF w sekcji D.2a mapuje 7 inicjatyw Strategii na obszary wiedzy K1–K11, fazy F0–F6 i artefakty.

Regulacje i normy

[Hasło online](#)

Superteam

Superzespół człowiek–AI

Termin CDF opisujący wysoce efektywny zespół, w którym agent AI wzmacnia możliwości pracownika, a człowiek zapewnia osąd, odpowiedzialność i kontekst.

Wdrożenie i zarządzanie

[Hasło online](#)

System AI wysokiego ryzyka

System AI wysokiego ryzyka (high-risk AI system)

System AI z dziedziny wymienionej w załączniku III AI Act (m.in. rekrutacja, zdolność kredytowa, dostęp do usług publicznych, edukacja, infrastruktura krytyczna, biometria), który decyduje o ludziach lub istotnie wpływa na decyzję — chyba że wykonuje tylko wąskie zadanie pomocnicze (art. 6 ust. 3). Profilowanie osób zawsze jest wysokim ryzykiem. Obowiązki podmiotu stosującego z art. 26 i 27 obowiązują od 2.12.2027

Regulacje i normy

AI Act

Zobacz: Deployer (Podmiot wdrażający), FRIA, EU Database (Unijna baza danych systemów AI), Conformity Assessment (Ocena zgodności), AI Act

[Hasło online](#)

Gdzie o tym piszemy: Ustawa o systemach SI — klasyfikator AI Act

Gdzie o tym piszemy: ChatGPT Enterprise, Copilot czy własne

System Availability

System Availability

Metryka Cognitive SLA (Tabela 14 Metodyki): dostępność platformy bazowej systemu AI. Target: $\geq 99,9\%$. Jedyna metryka infrastrukturalna w Tier 1 (obok trzech metryk jakości rozumowania). Zob. Uptime.

Suwerenność i architektura

Zobacz: Uptime

[Hasło online](#)

System S46

System teleinformatyczny S46

System teleinformatyczny Krajowego Systemu Cyberbezpieczeństwa (art. 46 ustawy o KSC), prowadzony przez NASK, służący do zgłaszania incydentów, wymiany informacji o zagrożeniach i ostrzeżeń między podmiotami kluczowymi i ważnymi a zespołami CSIRT. CDF w artefaktach K4/K8 wymaga procedur zgłoszeń zgodnych z formatem S46 oraz integracji z CSIRT sektorowym.

Regulacje i normy

NIS2/uKSC

Zobacz: NASK

[Hasło online](#)

Taksonomia źródeł CDF

CDF Source Taxonomy – klasy W, M, N, D

Czteroklasowa klasyfikacja źródeł kanonu CDF, wprowadzona w 1.6.0. Klasa W: akty prawa powszechnie obowiązującego lub w okresie dostosowawczym; wymagania obligatoryjne i brankowane fazowo, stan stosowania w kolumnie Status matrycy E.1. Klasa M: dokumenty organów publicznych i regulatorów bez mocy wiążącej; domyślnie włączone dla objętych profili, wyłączenie wymaga uzasadnienia w Compliance Gap Analysis. Klasa N: normy i standardy techniczne; rama dojrzałości bez domniemania zgodności do czasu przywołania w Dzienniku Urzędowym UE. Klasa D: badania i dane empiryczne; zasilają Evidence Book i kalibrują wartości domyślne profili ACE.

Metodyka CDF

Zobacz: Compliance Gap Analysis, Evidence Book

[Hasło online](#)

TCO

Total Cost of Ownership

Całkowity koszt posiadania rozwiązania, obejmujący nie tylko zakup lub budowę, ale także integrację, utrzymanie, energię, personel, compliance i koszty zmiany dostawcy.

Wdrożenie i zarządzanie

[Hasło online](#)

Gdzie o tym piszemy: ChatGPT Enterprise, Copilot czy własne

Tenant (dzierżawa)

Tenant — dzierżawa w usłudze chmurowej

Wydzielona przestrzeń jednej organizacji w usłudze chmurowej dostawcy: własne konta, dane i ustawienia na współdzielonej infrastrukturze. Dane są przetwarzane w regionie i na warunkach dostawcy — organizacja administruje, ale nie wybiera lokalizacji ani nie kontroluje metadanych; przeciwieństwo środowiska on-premises

Suwerenność i architektura

RODO

Zobacz: On-premises / On-prem, Hybrid Sovereign-Cloud, Vendor Lock-in, Data Gravity, Sovereignty Dimensions

[Hasło online](#)

Gdzie o tym piszemy: ChatGPT Enterprise, Copilot czy własne

Test Turinga

gra w naśladownictwo

Próba zaproponowana przez Alana Turinga w 1950 r.: sędzia rozmawia na piśmie z człowiekiem i z maszyną i ma wskazać, kto jest kim. W badaniu Jonesa i Bergena z 2025 r. model GPT-4.5, któremu kazano udawać człowieka, został uznany za człowieka w 73% rozmów. Gra TURING:AI odwraca role: sprawdza nie maszynę, lecz człowieka, który ma ją rozpoznać

Podstawy AI

Zobacz: LLM, Chatbot

[Hasło online](#)

Gdzie o tym piszemy: [Gra TURING:AI](#)

TK Pending (flaga)

Constitutional Tribunal Pending (flaga CDF)

Oznaczenie pozycji regulacyjnej objętej zawisłym postępowaniem przed Trybunałem Konstytucyjnym. Flaga oznacza ryzyko prawne wynikające z zawisłego postępowania, nie zaś zawieszenie stosowania przepisów; przy kontroli następczej ustawa obowiązuje do czasu ewentualnego orzeczenia o niezgodności. Stan na 12.09.2026: wniosek Prezydenta RP z 19.02.2026 dotyczący nowelizacji uKSC, sygnatura sprawy nie została opublikowana. Metodyka nie podaje przewidywanej sygnatury.

Metodyka CDF

[Hasło online](#)

Token

Jednostka tekstu

Podstawowa jednostka przetwarzania tekstu przez modele LLM, odpowiadająca fragmentowi słowa, całemu słowu albo znakowi zależnie od tokenizera.

Podstawy AI

[Hasło online](#)

Token Budget Governance

Zarządzanie budżetem tokenów

Mechanizm kontroli kosztów operacyjnych agentów AI poprzez limity kosztów per agent per interakcja (w jednostkach tokenów LLM). Obowiązkowy element Agent Governance od Fazy 2, szczególnie krytyczny przy Autonomous Swarms (L2-L3).

Wdrożenie i zarządzanie

[Hasło online](#)

Transparency Notice (Powiadomienie o przejrzystości)

Powiadomienie o systemie AI

Obowiązek informowania użytkowników o interakcji z systemem AI (art. 50 AI Act). Dotyczy chatbotów, deepfake'ów, systemów rozpoznawania emocji i kategoryzacji biometrycznej. W CDF realizowane w F2 poprzez SA-XAI Framework i Transparency Notice – mechanizm jawnego powiadamiania użytkowników.

Regulacje i normy

AI Act

Zobacz: AI Act

[Hasło online](#)

Gdzie o tym piszemy: Ustawa o systemach SI

Gdzie o tym piszemy: Polityka korzystania z AI — wzór

Triada wydania CDF

CDF Release Triad

Trzy zsynchronizowane artefakty publikowane w każdym wydaniu CDF: (1) Metodyka DOCX (PL), (2) Słownik DOCX, (3) Aplikacja webowa. Wszystkie trzy są ciągle doskonalone i muszą być spójne w każdym wydaniu. Źródło: proces wydawniczy CDF. Wprowadzone w v1.4.4.

Metodyka CDF

[Hasło online](#)

Układ z Komisją

Układ z Komisją (ugoda administracyjna)

Procedura warunków nadzwyczajnego złagodzenia sankcji prowadzona przez Komisję (art. 70–85). Układ może skutkować obniżką 20–70%, a w trybie art. 84 – 30–90%, pod warunkiem współpracy, naprawienia szkody i wdrożenia działań naprawczych.

Regulacje i normy

[Hasło online](#)

Uptime

Dostępność systemu

Procent czasu, w którym system pozostaje dostępny i działa zgodnie z oczekiwanym poziomem usług. Zob. System Availability (metryka Cognitive SLA).

Suwerenność i architektura

Zobacz: System Availability

[Hasło online](#)

US-EU AI Governance Divergence

US-EU AI Governance Divergence

Analiza 8 obszarów rozbieżności regulacyjnych EU vs US (Załącznik F, sekcja 2.11). Patrz: Tabela 84 oraz hasło Governance Divergence Matrix.

Regulacje i normy

Zobacz: NIST

[Hasło online](#)

Ustawa o systemach sztucznej inteligencji (SSI)

Ustawa z dnia 3 lipca 2026 r. o systemach sztucznej inteligencji

Dz. U. z 2026 r. poz. 1003 (ogłoszona 27.07.2026). Krajowa ustawa zapewniająca stosowanie AI Act: 127 artykułów w 10 rozdziałach, zmienia 10 innych ustaw. Reguluje organizację nadzoru rynku (Komisja Rozwoju i Bezpieczeństwa Sztucznej Inteligencji), opinie indywidualne, kontrolę i postępowanie, układ w sprawie nadzwyczajnego złagodzenia sankcji, jednostki notyfikowane, piaskownicę regulacyjną oraz kary administracyjne i przepisy karne. Wejście w życie: 11.08.2026 (art. 125 ust. 4 – 28.07.2026); art. 8–18 oraz rozdziały 3–5, 8 i 9 – 28.10.2026 (art. 127). W CDF adresowana Załącznikiem H (suplement SSI), artefaktami A-SSI-01 do A-SSI-07 i pozycjami SSI-1 do SSI-7 Matrycy E.1.

Regulacje i normy

AI Act

Zobacz: AI Act

[Hasło online](#)

Gdzie o tym piszemy: [Ustawa o systemach SI](#)

Gdzie o tym piszemy: [Baza wiedzy](#)

Vendor Disruption Protocol (VDP)

Protokół zakłócenia dostawcy

Pięciostopniowy protokół postępowania na wypadek utraty dostępu do dostawcy AI (blacklisting, sankcje, bankructwo). Obejmuje: VDP-1 Multi-Vendor Fallback, VDP-2 Sovereign AI Continuity, VDP-3 Migration Runbook, VDP-4 Supply Chain Cascade Assessment, VDP-5 Prime Contractor Liability. Aktywowany w F0, egzekwowany w F2/F3.

Suwerenność i architektura

[Hasło online](#)

Vendor Lock-in

Uzależnienie od dostawcy

Sytuacja, w której organizacja ma istotnie ograniczoną możliwość zmiany dostawcy technologii z powodu formatu danych, architektury, warunków kontraktowych lub braku kontroli nad kodem i integracjami.

Suwerenność i architektura

Data Act

Zobacz: Data Act (rozp. 2023/2854)

[Hasło online](#)

Gdzie o tym piszemy: [ChatGPT Enterprise, Copilot czy własne](#)

Vendor Risk Assessment

Ocena ryzyka dostawcy

Proces oceny ryzyka związanego z dostawcami modeli AI i komponentów infrastruktury kognitywnej, sformalizowany w CDF jako AI Model & Vendor Risk Assessment (artefakt A-F15-07, Faza F1.5, tag REGULATED, wprowadzony w 1.5.0). Obejmuje kryteria z Tabeli 12 Metodyki: jurysdykcja dostawcy i danych treningowych, compliance disclosure, vendor lock-in i migracja, historia regulacyjna, ciągłość dostępu. Zasila SLA-S, SoA, Exit Strategy i Risk Register.

Suwerenność i architektura

AI Act · DORA · NIS2/uKSC

Zobacz: AI Act, DORA

[Hasło online](#)

Vera Rubin NVL72

NVIDIA Vera Rubin NVL72

Platforma obliczeniowa NVIDIA nowej generacji (zapowiedziana na GTC 2026, dostępność H2 2026), następca architektury Blackwell. Konfiguracja NVL72: 72 GPU Rubin + 36 CPU Vera. W CDF uwzględniana w benchmarkach infrastruktury obliczeniowej (Tabela 15 w Metodyce) jako referencja dla suwerennego inference na dużą skalę.

Suwerenność i architektura

[Hasło online](#)

Voicebot

asystent głosowy na infolinii

Program, który prowadzi rozmowę głosową: rozpoznaje mowę, ustala sprawę rozmówcy i odpowiada syntezowanym głosem. Firmy używają voicebotów na infoliniach, na przykład do przyjęcia zgłoszenia szkody albo skierowania rozmowy do właściwego konsultanta. Od 2 sierpnia 2026 r. rozmówca musi wiedzieć, że rozmawia z AI

Podstawy AI

AI Act (art. 50 ust. 1)

Zobacz: Chatbot, Transparency Notice (Powiadomienie o przejrzystości), Klonowanie głosu

[Hasło online](#)

Gdzie o tym piszemy: Gra TURING:AI

Vulnerability Disclosure (Zgłaszanie podatności)

Proces zgłaszania i obsługi podatności

Obowiązek producenta produktu z elementami cyfrowymi zgłaszania aktywnie wykorzystywanych podatności i poważnych incydentów (CRA art. 14: 24 h wczesne ostrzeżenie, 72 h zgłoszenie, 14 dni raport końcowy; przez platformę ENISA; obowiązuje od 11.09.2026) oraz proces koordynowanego ujawniania podatności. W CDF mapowane na F5/F6 – Incident Response Plan, CogOps Monitoring i CogOps Dashboard (Załącznik D.2b).

Regulacje i normy

CRA

Zobacz: CRA (Cyber Resilience Act)

[Hasło online](#)

Watermarking (AI)

AI Content Watermarking

Obowiązek znakowania treści generowanych przez systemy AI, wynikający z art. 50 AI Act. Obejmuje dwuwarstwowe znakowanie: podpisane cyfrowo metadane proveniencji (informacja maszynowo czytelna) i imperceptible watermark osadzany podczas inferencji lub post-processingu. Terminy: obowiązki art. 50 stosowane od 02.08.2026; dla systemów generujących treści syntetyczne wprowadzonych do obrotu przed tą datą znakowanie maszynowo odczytywalne (art. 50 ust. 2) wymagane od 02.12.2026 (rozp. (UE) 2026/1744). W CDF realizowane w F4 poprzez Art. 50 AI-Generated Content Compliance Checklist (Załącznik B, Tabela 64) i SA-XAI Framework; zasilane wytycznymi KE z 20.07.2026 i Kodeksem postępowania z 10.06.2026 (klasa M).

Podstawy AI

AI Act

Zobacz: AI Act

[Hasło online](#)

Wejście w życie ustawy o SSI

Harmonogram stosowania ustawy o systemach sztucznej inteligencji

Art. 127 ustawy: trzon ustawy obowiązuje od 11.08.2026 (14 dni od ogłoszenia), art. 125 ust. 4 od 28.07.2026 (dzień po ogłoszeniu), a art. 8–18 (opinie indywidualne) oraz rozdziały 3 (kontrola), 4 (postępowanie), 5 (układ), 8 (kary administracyjne i przepisy karne) i 9 (zmiany w przepisach) od 28.10.2026 (3 miesiące od ogłoszenia). W CDF data 28.10.2026 stanowi granicę aktywacji pełnego reżimu kontrolno-sankcyjnego w profilach z tagiem GEO:PL.

Regulacje i normy

ustawa o systemach SI

[Hasło online](#)

Wiedza Ukryta

Tacit Knowledge

Wiedza, którą pracownik posiada, ale która nie jest udokumentowana w formalnych systemach organizacji – przechowywana w głowie, na dysku lokalnym, w prywatnych notatkach i nieformalnych interpretacjach. CBP ma na celu pozyskanie i formalizację wiedzy ukrytej.

Podstawy AI

[Hasło online](#)

Workflow Redesign Mandate

Mandat przeprojektowania procesów

Zasada CDF (Faza 5) mówiąca, że każdy workflow musi zostać przeprojektowany przed integracją z agentem AI. AI nie jest nakładane na nieefektywne procesy z przeszłości. Zapobiega powielaniu i automatyzowaniu wad istniejących procesów.

Wdrożenie i zarządzanie

[Hasło online](#)

Wyrób medyczny AI (URPL)

Medical Device AI / URPL

Wyrób medyczny, którego elementem bezpieczeństwa jest system AI lub który sam jest systemem AI (MDR 2017/745, IVDR 2017/746). Podlega notyfikacji wg rozdz. III sekcji 4 AI Act; URPL współpracuje z organem notyfikującym (art. 122 ustawy). Powiązany z mechanizmem HDC i tagiem HEALTH.

Regulacje i normy

ustawa o systemach SI · MDR/IVDR

Zobacz: IVDR (rozp. 2017/746)

[Hasło online](#)

XAI

Explainable AI

Wyjaśnialna sztuczna inteligencja – techniki i metody pozwalające zrozumieć, jak model podjął decyzję, na jakiej podstawie oraz z jakim poziomem pewności.

Podstawy AI

AI Act

Zobacz: AI Act

[Hasło online](#)

Zero Trust

Architektura zerowego zaufania

Model bezpieczeństwa zakładający, że żaden użytkownik, urządzenie ani agent nie jest domyślnie zaufany, niezależnie od lokalizacji w sieci. W CDF stosowany jako zasada projektowa architektury bezpieczeństwa systemów AI, w szczególności w środowiskach wieloagentowych.

Suwerenność i architektura

[Hasło online](#)

Znacząca modyfikacja

Substantial Modification

Istotna zmiana systemu AI (fine-tuning, ciągłe uczenie, znacząca aktualizacja) po jego wprowadzeniu, mogąca przenieść podmiot wdrażający w rolę producenta w rozumieniu art. 8 ust. 2 dyrektywy PLD 2024/2853, z przejęciem odpowiedzialności. Śledzona rejestrem znaczących modyfikacji (kontrola LER-2). Wprowadzona w CDF 1.5.0.

Regulacje i normy

AI Act · PLD 2024/2853

Zobacz: AI Act

[Hasło online](#)