Kto może wyłączyć Twój biznes?

Architektura odporności: suwerenność, model operacyjny AI i ciągłość działania

Innowacja (AI)

Zaufanie

Kontrola

Piotr Beńke
CTO, Head of ATLs @ IBM NCEE
linkedin.com/in/piotrbenke

Suwerenna AI, która się opłaca

Od ryzyka i regulacji do modelu operacyjnego z mierzalnym zwrotem

1 Dlaczego teraz

Geopolityka, regulacje i presja na wartość z AI

2 Gdy suwerenności brakuje

Realne przypadki utraty kontroli 2023–2025

3 Suwerenność mierzalna

EU Cloud Sovereignty Framework, skala SEAL

4 Zgodność w praktyce

RODO, DORA, NIS2/KSC, AI Act i Data Act

5 AI Operating Model

Inteligencja, działanie, operacje i zaufanie

6 Suwerenność która się opłaca

Co wdrożyć najpierw i kiedy się zwróci inwestycja

5–6: model operacyjny AI połączony z oceną suwerenności

Dlaczego właśnie teraz?

Suwerenność stała się mierzalnym kryterium biznesowym

61%

CIO i liderów IT w Europie Zachodniej zwiększy udział lokalnych dostawców chmury z powodu geopolityki

75%

przedsiębiorstw będzie miało strategię suwerenności cyfrowej do 2030 r.

180 mln €

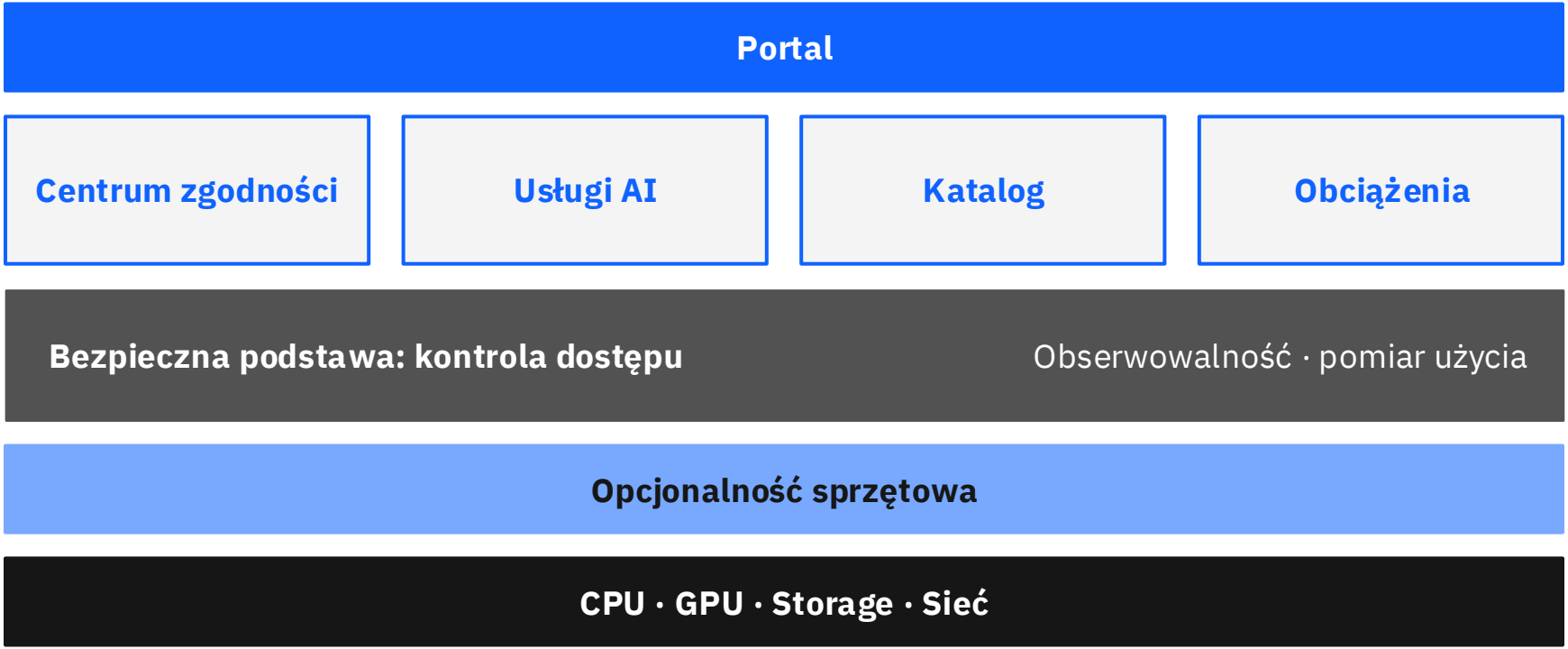
wartość pierwszego przetargu KE na suwerenną chmurę, rozstrzygniętego wg Sovereignty Score

Źródła: Gartner, 12.11.2025; Gartner, „The Future of Cloud in 2030”, 08.2025; Komisja Europejska, 17.04.2026

Suwerenność to zdolność strategiczna



Stos platformy



Pięć filarów suwerenności

Suwerenność to zdolność strategiczna



Dane

Gdzie są przechowywane i kto ma do nich dostęp



Operacje

Kto obsługuje i utrzymuje operacje, procesy, systemy



Bezpie-czeństwo

Jak chronione są obciążenia i klucze



Technologia

Na jakim stosie i sprzęcie polegasz



AI

Jakie modele działają i według jakich zasad

Gdy suwerenności brakuje

Przypadki naruszeń i utraty kontroli 2023–2025

Kto naprawdę ma władzę nad danymi?



Maj 2025

Prokurator MTK bez poczty

Po sankcjach USA wobec Międzynarodowego Trybunału Karnego Microsoft zablokował skrzynkę e-mail głównego prokuratora. Decyzję podjął obcy rząd, nie użytkownik.



Czerwiec 2025

„Nie mogę tego zagwarantować”

Dyrektor ds. prawnych Microsoft France zeznał pod przysięgą przed francuskim Senatem, że nie może zagwarantować, iż dane obywateli nie trafią do władz USA.

Lokalizacja serwera ≠ jurysdykcja: prawo spółki-matki sięga tam, gdzie jej usługi

Źródła: NL Times, 20.05.2025; PPC Land / Senat Francji, przesłuchanie 10.06.2025

Suwerenność, którą da się zmierzyć

EU Cloud Sovereignty Framework i Sovereignty Score

Jak liczy się Sovereignty Score

$$\textbf{Sovereignty Score} = \sum \text{Score}(SOV_n) / \text{Max}(SOV_n) \times \text{Waga}(SOV_n)$$

1. Próg SEAL

Zamawiający ustala minimalny poziom SEAL dla każdego z 8 celów. Oferta poniżej progu odpada.

2. Ocena 8 celów SOV

Każdy cel SOV-1…SOV-8 jest punktowany na podstawie kryteriów i dowodów.

3. Ważony ranking

Ważona suma punktów daje wynik 0–100%, który decyduje o rankingu ofert.

Źródło: Komisja Europejska, Cloud Sovereignty Framework v1.2.1, 10.2025

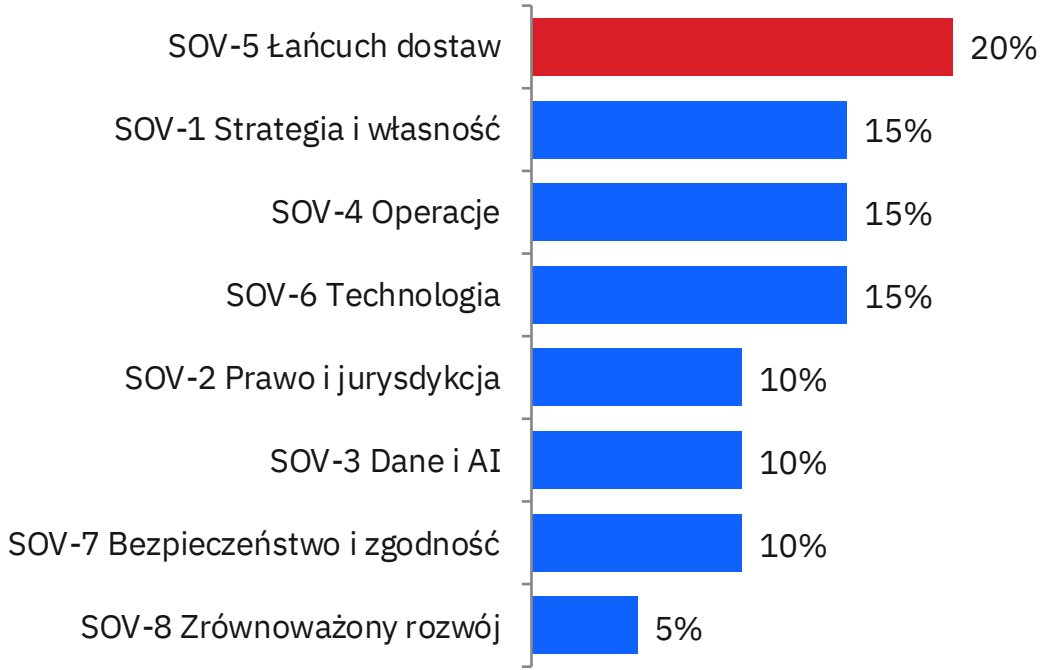
Skala SEAL *(Sovereignty Effective Assurance Level)*

Pięć poziomów — od braku do pełnej suwerenności



Źródło: Komisja Europejska, Cloud Sovereignty Framework v1.2.1 (SEAL = Sovereignty Effective Assurance Level)

Osiem celów i ich wagi



Łańcuch dostaw waży najwięcej

Pochodzenie sprzętu, firmware i oprogramowania to 20% wyniku. Razem z technologią i operacjami — połowa oceny dotyczy tego, kto i na czym naprawdę uruchamia usługę.

Źródło: Komisja Europejska, Cloud Sovereignty Framework v1.2.1; wagi SOV-1…SOV-8 sumują się do 100%

Sovereignty Score: przykład obliczenia

Dwie oferty, ten sam wzór — i próg SEAL, który rozstrzyga przed rankingiem

Cel	Waga	A: hiperskaler, region w PL	B: dostawca z UE
SOV-1 Strategia i własność	15%	3 · 4,5	9 · 13,5
SOV-2 Prawo i jurysdykcja	10%	**3 · 3,0**	9 · 9,0
SOV-3 Dane i AI	10%	8 · 8,0	9 · 9,0
SOV-4 Operacje	15%	4 · 6,0	8 · 12,0
SOV-5 Łańcuch dostaw	20%	3 · 6,0	**5 · 10,0**
SOV-6 Technologia	15%	6 · 9,0	7 · 10,5
SOV-7 Bezpieczeństwo i zgodność	10%	9 · 9,0	8 · 8,0
SOV-8 Zrównoważony rozwój	5%	9 · 4,5	6 · 3,0

Oferta A · Sovereignty Score

50%

SEAL-1 w SOV-2 (prawo USA) — odpada przed rankingiem mimo najlepszego bezpieczeństwa

Oferta B · Sovereignty Score

75%

najsłabszy cel SOV-5 osiąga SEAL-2 — przechodzi próg i wygrywa

Najpierw próg SEAL, potem ranking — najsłabsze ogniwo decyduje

Przykład ilustracyjny (punkty 0–10 · wkład w wynik); metoda wg KE, Cloud Sovereignty Framework v1.2.1; próg SEAL-2 jak w przetargu KE

Sovereign Score w praktyce

180 mln €

Przetarg Komisji Europejskiej na suwerenną chmurę dla instytucji UE, rozstrzygnięty 17.04.2026

6 lat	czas trwania
4	kontrakty
SEAL-2	próg minimalny

Post Telecom	z OVHcloud i Clever Cloud (LU/FR)
STACKIT	Grupa Schwarz (DE)
Scaleway	Grupa Iliad (FR)
Proximus	z S3NS, Clarence i Mistral (BE/FR/LU)

Większość zwycięskich ofert osiągnęła SEAL-3

Źródło: Komisja Europejska, „Commission advances cloud sovereignty through strategic procurement”, 17.04.2026; ITdaily

Sovereign Core a Sovereign Score

Platforma wzmacnia wynik, ale SEAL ocenia całą usługę i operatora



SOV-3 Dane i AI

Klucze, dane i inferencja AI pod kontrolą klienta, on-premise



SOV-4 Operacje

Obsługa przez klienta lub lokalnego partnera, także w trybie air-gap



SOV-6 Technologia

Otwarte oprogramowanie, OpenShift, opcjonalność sprzętowa



SOV-7 Zgodność

Compliance Center: ciągłe zbieranie dowodów zgodności

SOV-1, SOV-2, SOV-5: zależą od wybranego operatora, struktury własności i łańcucha dostaw sprzętu

Opracowanie na podstawie: IBM (B. Havers, „Sovereignty”; „Put AI to Work: Od zasad do działania”)

Cztery mity o suwerenności

Obiekcje, które padną na sali — i co mówią fakty

MIT „Suwerenność = on-premise”

FAKT SEAL ocenia kontrolę nad usługą, nie adres serwerowni. Chmura suwerenna i hybryda też osiągają SEAL-3 — jak większość zwycięzców przetargu KE.

MIT „Wystarczy, że dane są w Polsce”

FAKT Dane i AI to tylko 10% Sovereignty Score. Łańcuch dostaw, operacje i technologia — 50%. Lokalizacja ≠ jurysdykcja.

MIT „Suwerenność = koniec z hiperskalerami”

FAKT Chodzi o świadomy wybór dla każdego obciążenia i realną strategię wyjścia. Chmura publiczna zostaje tam, gdzie ryzyko jest niskie.

MIT „To projekt dla działu IT”

FAKT Strategia i własność (SOV-1) to 15% oceny. DORA i NIS2 czynią zarząd odpowiedzialnym za ryzyko ICT — to decyzja zarządu.

Suwerenność to zdolność do podejmowania decyzji — nie miejsce na mapie

Źródła: KE, Cloud Sovereignty Framework v1.2.1 (10.2025); KE (17.04.2026); DORA art. 5; dyrektywa NIS2 art. 20

Zgodność w praktyce

Regulacje UE i organizacje, które już działają

Regulacje wymagają dowodu kontroli

Nie wystarczy deklaracja — potrzebny jest dowód operacyjny



RODO

Kontrola nad danymi osobowymi i ich transferem poza UE



DORA

Odporność operacyjna sektora finansowego, od 17.01.2025



NIS2 / KSC

Zarządzanie ryzykiem i ciągłość działania podmiotów kluczowych



AI Act

Wymogi zależne od ryzyka systemów AI, wdrażane etapami



Data Act

Przenaszalność danych i łatwiejsza zmiana dostawcy chmury

Źródła: Rozporządzenia (UE) 2016/679, 2022/2554, 2024/1689, 2023/2854; Dyrektywa (UE) 2022/2555

Efekt MTK: Europa przechodzi do ofensywy

Po sankcjach wobec Trybunału zależność od Big Tech stała się kwestią bezpieczeństwa

Dania · 06.2025

LibreOffice zamiast Office 365

Ministerstwo Cyfryzacji rezygnuje z pakietu Microsoftu; Windows zostaje.

MTK · 10.2025

openDesk zamiast MS Office

Trybunał przechodzi na otwarty pakiet ZenDiS, rozwijany przy niemieckim MSW.

Szlezwik-Holsztyn · 10.2025

Poczta bez Exchange

Ponad 40 tys. kont przeniesionych na Open-Xchange i Thunderbird.

Polska · 02.2026

Krajowy pakiet biurowy

COI zapowiada pakiet open source; od 2027 r. Polska w Digital Commons EDIC.

Francja · 04.2026

Linux w administracji

DINUM przechodzi na Linuxa; ministerstwa przygotowują plany wyjścia.

EU OS · 2025–2026

Wspólny pulpit dla UE?

Oddolny proof-of-concept Linuxa (Fedora + KDE) — jeszcze nie projekt Komisji.

Oprogramowanie to już nie tylko narzędzie — to ryzyko geopolityczne

Źródła: heise (06.2025); The Stack (11.2025); The Register (10.2025); Spider's Web (02.2026); CRN (10.2026); TechCrunch (04.2026); eu-os.eu

Cena outsourcingu

Polskie lekcje: gdy kontrola jest u kogoś innego, kryzys przychodzi z zewnątrz

07.2024

CrowdStrike: jedna aktualizacja

Błędna aktualizacja oprogramowania bezpieczeństwa unieruchomiła Windows na świecie. W Polsce: Baltic Hub w Gdańsku, odprawy na Lotnisku Chopina, klienci banków.

Technologia

09.2026

PUZ Suwałki: bez kopii zapasowych

Ransomware zaszyfrował serwery uczelni, która straciła też dostęp do kopii zapasowych. Dziekanat, kadry i płace stanęły; zagrożone dane studentów i pracowników.

Bezpieczeństwo

2026

MyDr: ryzyko u podwykonawcy

Atak na dostawcę oprogramowania dla ok. 12 tys. placówek medycznych: dane nawet 18,8 mln pacjentów, w tym PESEL i notatki z wizyt. Umowy nie wymuszały zabezpieczeń.

Dane

Suwerenność to nie logo na fakturze — to pytanie, kto ma klucze do danych i systemów w kryzysie

Źródła: Spider's Web, Telepolis (19.07.2024); TVN24, Podlaskie24 (30.09.2026); Bezprawnik, RMF24 (2026) — skala MyDr wg Ministerstwa Cyfryzacji

Polska: lokalnie nie znaczy suwerennie

Polski kontekst: rynek chmury, regiony hiperskalerów i własny model językowy

Raport ITCI

Ponad 70% rynku chmury w rękach firm z USA

Microsoft, AWS i Google dominują polski rynek chmurowy, wzmacniając pozycję lokalnymi regionami i współpracą z Operatorem Chmury Krajowej.

Rynek

2021–2023

Regiony hiperskalerów w Polsce

Google Cloud (Warszawa, 2021) i Microsoft (Poland Central, 2023): dane w kraju, ale spółka-matka w USA. Bez dodatkowych zabezpieczeń to poziom SEAL-1.

Jurysdykcja

02.2025

PLLuM — polski model państwowy

Rodzina polskich modeli językowych rozwijana przez konsorcjum uczelni i instytutów przy Ministerstwie Cyfryzacji; ma wspierać usługi publiczne, m.in. mObywatel.

AI

Pytanie dla polskiej organizacji: nie „gdzie stoi serwer?”, tylko „kto może go wyłączyć?”

Źródła: ITCI / Leaders Hub, „W dążeniu do suwerenności cyfrowej” (wg bank.pl); Google Cloud (04.2021); Microsoft (04.2023); Ministerstwo Cyfryzacji (02.2025)

Polska stawia na własne strefy kontroli

Suwerenna AI w praktyce: bank buduje własnych agentów, regulator podnosi poprzeczkę

PKO Bank Polski · 08.2026

Pierwszy suwerenny agent AI

Zbudowany w banku: Formacja Hiperautomatyzacji i Centrum Kompetencji AI.

Zadanie: analizuje i klasyfikuje dziesiątki tysięcy e-maili klientów miesięcznie, proponuje dalsze kroki.

Kontrola: decyduje człowiek (human-in-the-loop).

Efekt: odpowiedź do 70% szybciej (deklaracja banku); 30 kolejnych agentów do końca 2026 r.

Regulator · 17.01.2025

KNF: DORA zamiast komunikatu chmurowego

Uchylona Rekomendacja D i komunikat chmurowy; obowiązują twarde wymogi DORA wobec dostawców ICT.

Regulator · 22.07.2026

UKNF: rekomendacje dotyczące Frontier AI

Ataki wspierane AI w analizie ryzyka ICT, weryfikacja dostawców, izolacja systemów krytycznych.

Kontrola nad modelem, danymi i dostawcą to dziś wymóg nadzorczy — nie wybór działu IT

Źródła: bank.pl, Computerworld (08.2026); KNF, komunikat z 16.01.2025; KNF, rekomendacje ws. Frontier AI (22.07.2026)

AI Operating Model

Jak budować i eksploatować AI — z kontrolą i zwrotem z inwestycji

AI przyspiesza, przewaga konkurencyjna — nie

Adopcja AI jest wszędzie, zwrot z inwestycji — rzadko

88%

przedsiębiorstw już używa AI

2,59 bln $

prognozowane wydatki na AI w 2026 r. (+47% r/r)

20%

firm ma szansę osiągnąć zwrot z inwestycji w AI

6%

organizacji widzi istotną wartość z AI w kosztach lub przychodach

To problem operacyjny — a problem operacyjny wymaga modelu operacyjnego

Źródła: McKinsey & Company, The State of AI: Global Survey; Gartner, 05.2026 i Gartner AI Survey; Boston Consulting Group, 08.2026

Trzy ery infrastruktury

Każde obciążenie AI łączy decyzje o danych, aplikacjach, kosztach i kontroli

Przed 2010

Dedykowana infrastruktura

Projektowanie w znanej pojemności i ograniczeniach operacyjnych

Gdzie działa: Własna

2010–2025

Chmura na żądanie

Projektowanie pod elastyczną pojemność i usługi rozproszone

Gdzie działa: Własna · Hiperskalerzy

2026 i dalej

AI w środowiskach hybrydowych

Łączenie wymagań obciążeń z danymi, modelami, mocą obliczeniową i kontrolą

Gdzie działa: Własna · Hiperskalerzy · Suwerenna · Neo-cloud

Chmura suwerenna to dziś pełnoprawne miejsce dla AI — obok własnej infrastruktury i hiperskalerów

Opracowanie na podstawie: IBM, TechXchange 2026 — „AI Operating Model”

AI zwielokrotnia złożoność

Cztery wymiary — i pytanie o suwerenność w każdym z nich

Wiele danych

Z rozproszonych danych → do zaufanego kontekstu na bieżąco

Suwerenność:
Gdzie są dane i klucze? (SOV-3)

Wiele agentów

Z odizolowanych agentów → do skoordynowanej pracy

Suwerenność:
Kto autoryzuje agentów? (SOV-7)

Wiele modeli

Z reaktywnego zarządzania → do ciągłej optymalizacji

Suwerenność:
Czy wybór modelu jest nasz? (SOV-3, SOV-6)

Wiele chmur

Z silosów → do otwartej podstawy hybrydowej bez vendor lock-in

Suwerenność:
Czy możemy odejść w 72 h? (SOV-6)

Opracowanie na podstawie: IBM, TechXchange 2026 — „AI Operating Model”; cele SOV wg KE, Cloud Sovereignty Framework v1.2.1

Czyj jest model?

Trzy sposoby korzystania z modeli — każdy z innym poziomem kontroli

Frontier przez API

Kontrola: niska — wersja, cennik i dostępność po stronie dostawcy.

Zalety: najwyższa jakość w najtrudniejszych zadaniach, zero infrastruktury.

Ryzyko: wycofanie modelu, odcięcie dostępu, dane poza organizacją.

Przykłady: GPT, Claude, Gemini.

Open-weight u siebie

Kontrola: wysoka — wagi, wersja i dane zostają u Ciebie.

Zalety: przewidywalny koszt, praca on-prem i w trybie air-gap.

Ryzyko: własne GPU i kompetencje; nieco niższa jakość w zadaniach granicznych.

Przykłady: IBM Granite, Mistral, Bielik.

Model dostrojony na własnych danych

Kontrola: pełna — także nad wiedzą domenową.

Zalety: najlepsza trafność w wąskim zadaniu; mniejszy i tańszy model.

Ryzyko: koszt danych treningowych i utrzymania cyklu życia modelu.

Przykłady: Granite lub PLLuM dostrojone na danych klienta.

Warunek suwerenności modelu: możliwość jego zmiany bez przepisywania aplikacji

Opracowanie własne; IBM Granite (licencja Apache 2.0); Bielik — SpeakLeash i ACK Cyfronet AGH; PLLuM — Ministerstwo Cyfryzacji

Gdzie znika przewaga z AI

Cztery objawy braku modelu operacyjnego — i lekcje z rynku

Objaw	Dźwignia
Pilotaże, które nigdy nie trafiają do produkcji	Działanie
Agenci mnożący się bez nadzoru	Zaufanie
Prognozy oparte na nieaktualnych danych	Inteligencja
Brak wglądu w koszt AI	Operacje

Ucz się na cudzych błędach

Zillow, 2021 — Inteligencja

Algorytm wyceny domów rozminął się z rynkiem — firma zamknęła biznes skupu domów i odpisała setki mln $

Samsung, 2023 — Zaufanie

Inżynierowie wkleili poufny kod źródłowy do publicznego czatu AI — firma zakazała narzędzi GenAI

Uber — Operacje

Roczny budżet tokenów AI wyczerpany w pięć miesięcy

Źródła: Zillow Group, wyniki za III kw. 2021; Bloomberg, 02.05.2023 (Samsung); Uber — wg materiałów IBM „The AI Operating Model”

AI bez modelu operacyjnego

Technologia działała — zabrakło właściciela, nadzoru i ograniczeń

Air Canada · 02.2024 — Zaufanie

Chatbot wymyślił zasady zwrotu biletów. Trybunał orzekł, że linia odpowiada za słowa swojego bota jak za stronę WWW.

Deloitte Australia · 10.2025 — Zaufanie

Raport dla rządu za 440 tys. AUD zawierał przypisy i cytaty wygenerowane przez AI, które nie istniały. Firma zwróciła część honorarium.

Replit / SaaStr · 07.2025 — Operacje

Agent AI do kodowania usunął produkcyjną bazę danych mimo zamrożenia zmian — miał uprawnienia, których nie powinien mieć.

Klarna · 2024–2025 — Działanie

AI przejęła pracę ok. 700 konsultantów. Gdy spadła jakość obsługi, firma zaczęła ponownie zatrudniać ludzi.

95% pilotaży GenAI nie daje mierzalnego wpływu na wynik — barierą jest wykonanie, nie model

Źródła: BC Civil Resolution Tribunal, Moffatt v. Air Canada (14.02.2024); AFR (10.2025); Fortune (07.2025); Bloomberg (05.2025); MIT NANDA, „The GenAI Divide" (08.2025)

Ani suwerenności, ani modelu

Dwie osie, cztery scenariusze — i przypadki z rynku

Suwerenność →

Suwerenność: tak · Model: brak

Kontrola bez wartości

Dane i modele są u siebie, ale AI utyka w pilotażach. Koszt infrastruktury bez zwrotu i bez przewagi.

Suwerenność: tak · Model: tak

Suwerenna AI, która się opłaca

Kontrola nad danymi, modelami i operacjami — plus mierzalny zwrot. Do tego prowadzą cztery dźwignie.

Suwerenność: brak · Model: brak

Podwójne ryzyko

McHire (07.2025): bot rekrutacyjny dostawcy, hasło admina „123456”, do 64 mln rekordów kandydatów.

DeepSeek (2025): Shadow AI wysyła dane do Chin; Włochy i Korea Płd. blokują aplikację.

Suwerenność: brak · Model: tak

Wartość bez kontroli

AI działa i się skaluje — dopóki sankcje, regulator lub dostawca nie wyłączą usługi (Nayara, Windsurf, GPT-4o).

AI Operating Model →

Źródła: I. Carroll i S. Curry / Wired (07.2025); Garante Privacy (30.01.2025); PIPC Korea (17.02.2025); przypadki z poprzednich slajdów

Cztery dźwignie modelu AI

Barierą nie jest już finansowanie eksperymentów, tylko wykonanie



Inteligencja

Przygotuj dane dla AI

Confluent · watsonx.data · Db2



Operacje

Skaluj bez psucia

Terraform · Apptio · Red Hat

AI
Operating Model

Aplikacje/Działanie

Zaprzęgnij inteligencję do pracy



Bob · Orchestrate · Integration

Zaufanie

Zarządzaj tym, co uruchamiasz



Vault · Lightwell · Quantum Safe

Dźwignie celowo się nakładają — wybierz jedną, zdobądź pierwszą bazę, potem rozszerzaj

Opracowanie na podstawie: IBM, „The AI Operating Model” (2026); IBM, TechXchange 2026

Kto buduje model operacyjny AI

Każdy zespół ma inne zadanie — i inne pytanie o suwerenność

Zespół danych

Dostarczać aktualny kontekst

„Gdzie są nasze dane i kto ma do nich dostęp?”

Deweloperzy aplikacji

Budować szybciej, z kontrolą

„Czy asystent AI może działać u nas?”

Zespół platformy

Automatyzować operacje

„Czy utrzymamy usługę własnymi siłami?”

Bezpieczeństwo

Kontrolować ryzyko, gdy AI rośnie

„Kto zarządza kluczami i tożsamością agentów?”

Infrastruktura

Uruchamiać AI blisko biznesu

„Czy przeniesiemy obciążenie w 72 h?”

Finanse

Łączyć wydatki z wartością

„Ile kosztuje AI i kiedy się zwróci?”

Opracowanie na podstawie: IBM, TechXchange 2026 — „Practitioners build and operate the AI Operating Model”

Suwerenność, która się opłaca

Co wdrożyć najpierw — i kiedy wróci inwestycja

Ile kosztuje suwerenność?

Uczciwy rachunek: premia za kontrolę ma sens tam, gdzie ryzyko jest wysokie

Co płacisz

Infrastruktura: wyższy koszt jednostkowy niż u hiperskalera, zwłaszcza przy małej skali.

GPU: trudniejszy dostęp do najnowszych akceleratorów i dłuższe terminy dostaw.

Modele: open-weight wciąż ustępują modelom frontier w najtrudniejszych zadaniach.

Ludzie: mniej gotowych usług zarządzanych — więcej pracy zespołu lub partnera.

Kiedy się zwraca

Dane regulowane: RODO, DORA, KSC — kara do 4% obrotu i odpowiedzialność zarządu.

Procesy krytyczne: przestój po odcięciu usługi kosztuje więcej niż premia.

Przetargi publiczne: Sovereignty Score decyduje o wygranej (KE: 180 mln €).

Duża, stała skala: własna platforma inferencji bywa tańsza niż płacenie za tokeny.

Nie wszystko musi być suwerenne — suwerenne musi być to, co krytyczne

Opracowanie własne na podstawie: RODO art. 83; KE, przetarg na suwerenną chmurę (17.04.2026); IBM, „The AI Operating Model” (2026)

Które obciążenie gdzie?

Wrażliwość danych i krytyczność procesu wyznaczają miejsce — nie moda →

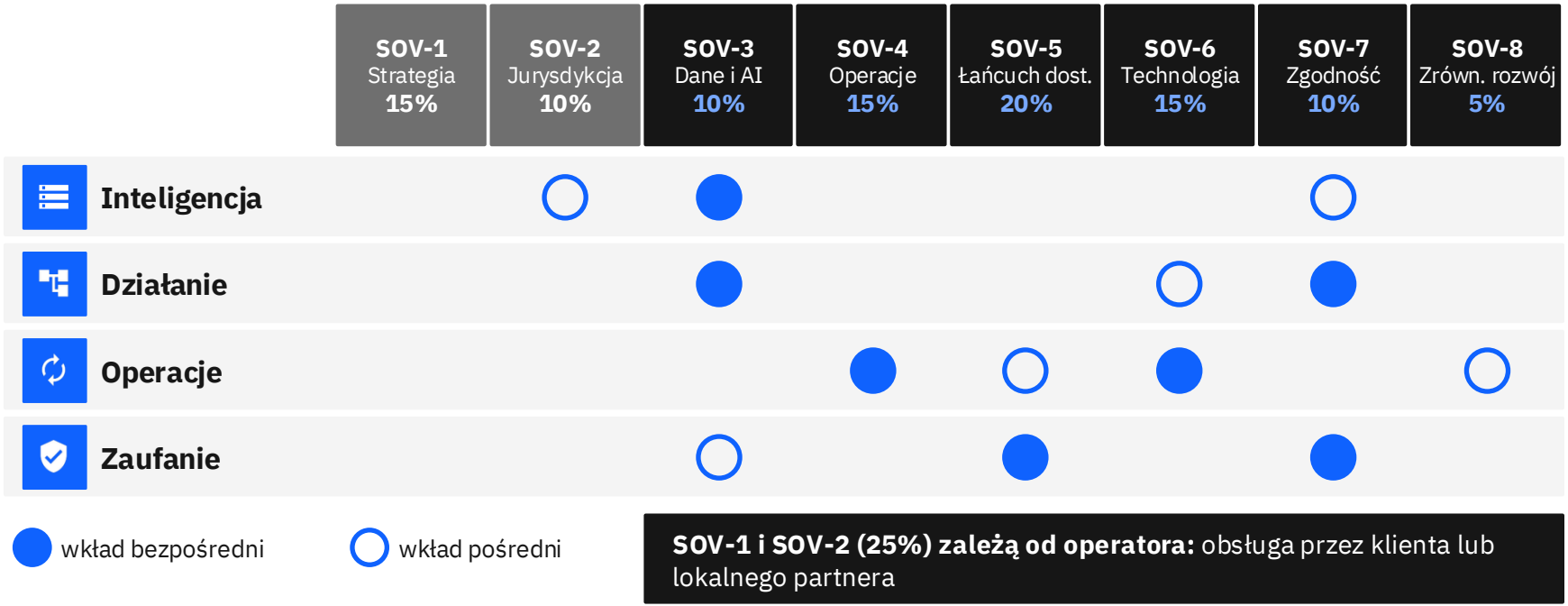
Chmura publiczna	Chmura suwerenna (UE)	Własna platforma	Air-gap
Dla: dane publiczne i niekrytyczne. **Przykłady:** treści marketingowe, prototypy na danych syntetycznych. **Poziom:** SEAL-0–1	**Dla:** dane osobowe i procesy regulowane. **Przykłady:** obsługa klienta, asystent HR, analityka sprzedaży. **Poziom:** SEAL-2–3	**Dla:** tajemnica przedsiębiorstwa i systemy core. **Przykłady:** kod źródłowy, dane klientów banku, agenci w systemach transakcyjnych. **Poziom:** SEAL-3+	**Dla:** infrastruktura krytyczna i dane niejawne. **Przykłady:** energetyka, obronność, systemy sterowania. **Poziom:** SEAL-4

Jedna organizacja, wiele miejsc — wspólne zasady i jedna płaszczyzna sterowania

Opracowanie własne; poziomy SEAL poglądowe wg KE, Cloud Sovereignty Framework v1.2.1

Model AI a Sovereignty Score

Każda dźwignia wzmacnia inne cele suwerenności



Opracowanie własne na podstawie: IBM, „The AI Operating Model”; KE, Cloud Sovereignty Framework v1.2.1 — mapa poglądowa, nie ocena SEAL

Elementy gotowe na suwerenność

Nie trzeba wdrażać wszystkiego naraz — każdy element ma własny zwrot

Element	Cele SOV	Wartość biznesowa	Pierwsze korzyści
Dynamiczne sekrety i tożsamości Vault, IBM Agent Identity	SOV-3, 7	Hasła żyją minuty, nie lata; mniej incydentów, gotowość na NIS2 i DORA	3–6 mies.
Zaufane źródło open source Lightwell	SOV-5, 7	Mniej pilnych łatek i podatności, kontrola pochodzenia pakietów	3–6 mies.
Tokenomia AI Apptio	ROI	Koszt AI wg zespołu i modelu, alerty budżetu, chargeback	3–6 mies.
Polityki, IaC i dowody zgodności Terraform, Ansible, Compliance Center	SOV-4, 7	Szybszy provisioning, ślad audytowy, krótsze audyty	3–6 mies.
Lokalna inferencja i Bob On-prem Red Hat AI, Bob, watsonx Orchestrate	SOV-3, 6	Produktywność bez wysyłania danych poza organizację	6–9 mies.
Dane w czasie rzeczywistym Confluent, watsonx.data	SOV-3	Nowcasting zamiast prognoz, mniej kopii i potoków	6–12 mies.
Przenośność i strategia wyjścia OpenShift, kontenery, LinuxONE	SOV-5, 6	Brak vendor lock-in, zgodność z Data Act, siła negocjacyjna	6–12 mies.

Czas do pierwszych korzyści: szacunek orientacyjny, do potwierdzenia w ocenie wartości dla klienta. Elementy można wdrażać niezależnie

IBM jako Klient Zero

Model operacyjny AI wdrożony najpierw u siebie — i rozliczony z wyniku

Trzy lata transformacji

4,5 mld $

wzrostu produktywności dzięki AI, chmurze hybrydowej, automatyzacji i doradztwu — i liczba wciąż rośnie

1 Nastawienie

Kwestionuj status quo, usuwaj złożoność, automatyzuj powtarzalne zadania, wbuduj AI w procesy.

2 Tempo

Zwinne dostarczanie: MVP mniej więcej co dwa tygodnie — postęp ponad perfekcję.

3 Pomiar

Każda inicjatywa jest rozliczana z wyniku biznesowego, nie z liczby pilotaży.

4 Sponsoring

Komitet sterujący prowadzony przez CEO; pracownicy mogą kwestionować procesy.

Ponad 155 przypadków użycia AI · 15 tys. pomysłów na agentów od pracowników (2025)

Źródło: IBM, „IBM as Client Zero: Productivity with AI and innovation” (ibm.com/case-studies/ibm-client-zero, 02.2026); wyniki IBM mają charakter ilustracyjny.

Policzmy: asystent AI w firmie

Przykład: 5 000 pracowników, asystent HR i IT na własnej platformie

Założenia

Wolumen: 5 000 osób × 2 zgłoszenia/mies. = 120 tys./rok

Koszt obsługi: 12 € za zgłoszenie obsłużone przez człowieka

Skuteczność AI: 60% zgłoszeń (AskHR w IBM: 94%)

Czas pracownika: 10 min oszczędności na zgłoszeniu

Koszty: wdrożenie 400 tys. € (rok 1); platforma i inferencja on-prem 200 tys. € rocznie

ok. 7 mies.
okres zwrotu po uruchomieniu

864 tys. €
oszczędności na obsłudze rocznie (72 tys. × 12 €)

12 tys. h
czasu pracowników rocznie — poza rachunkiem ROI

ok. 160%
ROI w trzy lata (2,6 mln € korzyści / 1 mln € kosztów)

Przykład ilustracyjny — w ocenie wartości podmieniamy założenia na dane klienta

Opracowanie własne; skuteczność AskHR wg IBM, „IBM as Client Zero” (02.2026)

Cztery pytania na start

Wybierz jedną dźwignię, zdobądź pierwszą bazę, potem rozszerzaj



Inteligencja

„Czy Twoje dane są gotowe na AI — czy tylko dostępne?”

Jakość, właściciel i aktualność danych



Działania/Aplikacje

„Co działa teraz w Twoim środowisku — i kto jest właścicielem?”

Inwentarz aplikacji, agentów i Shadow AI



Operacje

„Ile kosztowała Cię AI w zeszłym miesiącu i który zespół to wydał?”

Widoczność i przypisanie kosztów tokenów



Zaufanie

„Jak długo możesz czekać z wdrożeniem krytycznej łatki?”

Ekspozycja łańcucha dostaw i sekretów

Opracowanie na podstawie: IBM, „The AI Operating Model” (2026)

Zadanie po konferencji: test 72 godzin

Jedno ćwiczenie, które pokaże więcej niż niejeden audyt

1

Wybierz

Jedno krytyczne obciążenie AI lub danych — takie, bez którego firma staje.

2

Zapytaj

Gdzie są dane i klucze? Kto może wyłączyć usługę? Ile trwa przeniesienie?

3

Sprawdź

Spróbuj uruchomić je w innym środowisku w 72 godziny. Zapisz, co blokuje.

Wynik testu to Twoja mapa luk — i pierwszy krok ścieżki 0–3 miesięcy

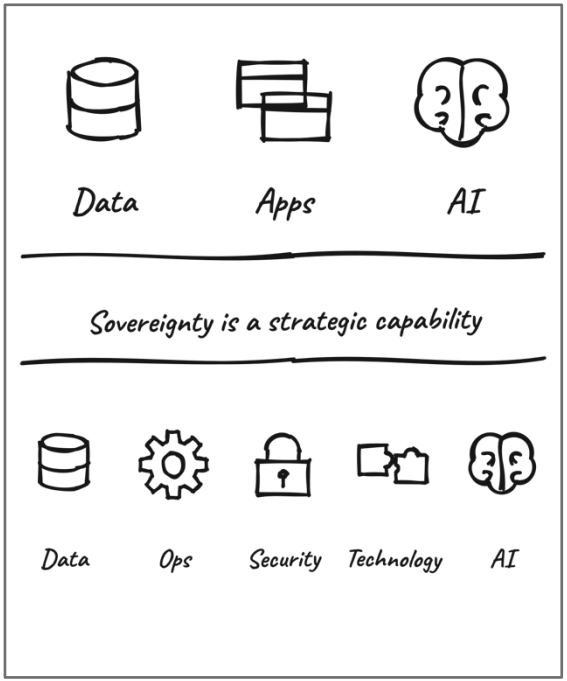
Porozmawiajmy o wynikach: piotr.benke@pl.ibm.com lub linkedin.com/in/piotrbenke

Innowacja + Zaufanie + Kontrola

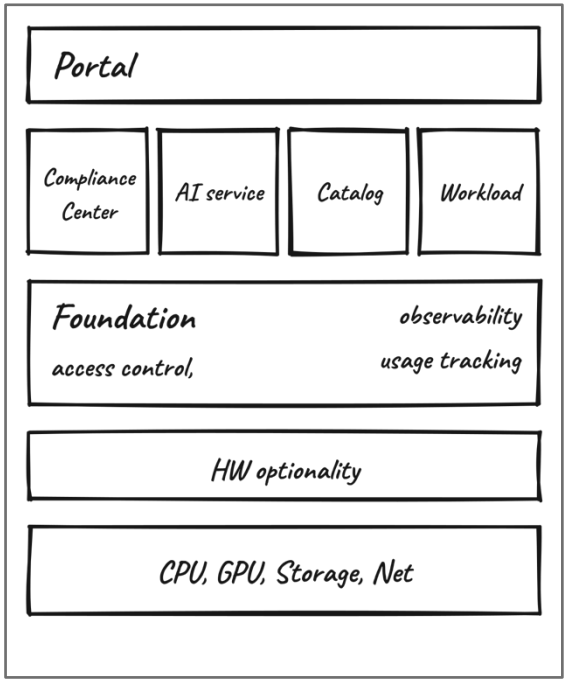
Innowacja (AI) **+** **Zaufanie** **+** **Kontrola**

= Suwerenność cyfrowa

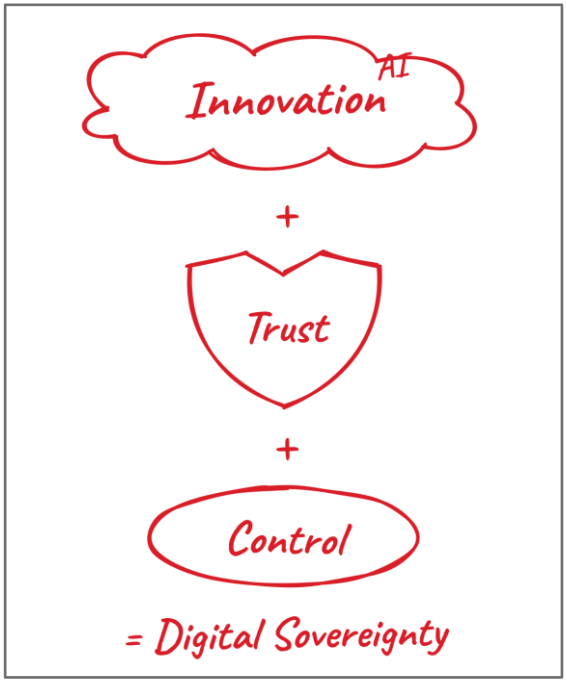
Podsumowanie - suwerenność



Filary suwerenności

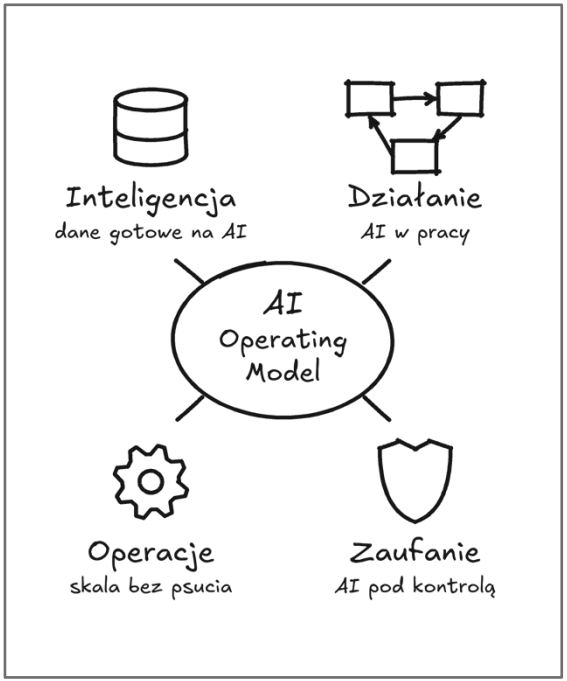


Sovereign Core

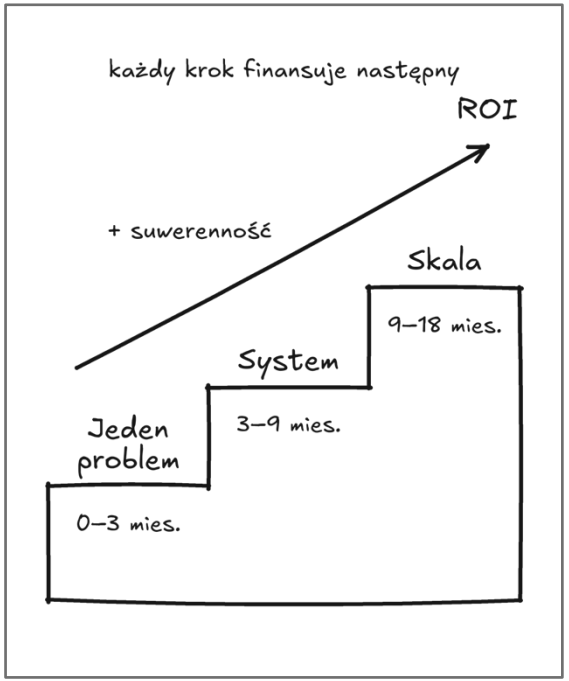


Równanie

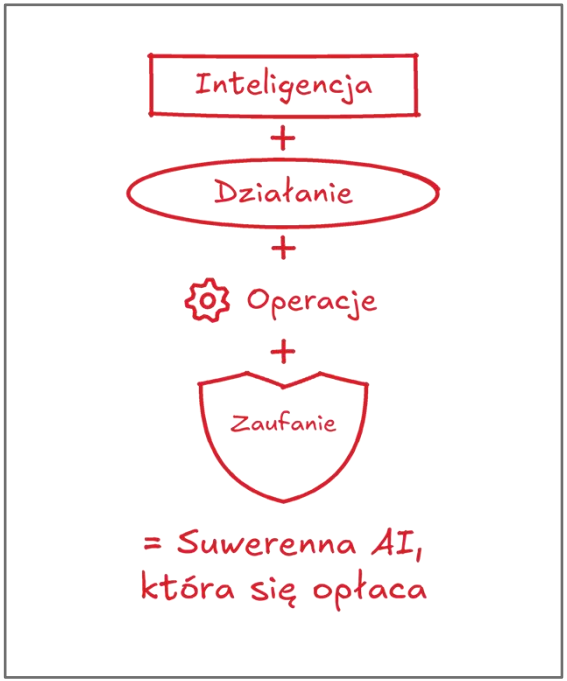
Podsumowanie - AI Operating Model



Cztery dźwignie AI



Ścieżka do skali



Równanie wartości

Źródła

KE — Cloud Sovereignty Framework v1.2.1 (10.2025)

KE — przetarg na suwerenną chmurę (17.04.2026)

Gartner — 61% CIO w Europie Zachodniej (12.11.2025)

EDPS — KE i Microsoft 365 (11.03.2024)

DPC — kara dla TikTok 530 mln € (05.2025)

Hunton — kara dla Meta 1,2 mld € (05.2023)

Linklaters — kara dla Uber 290 mln € (08.2024)

PPC Land — Microsoft France przed Senatem (06.2025)

The Register — Szlezwik-Holsztyn (15.10.2025)

Computing — Dania i LibreOffice (07.2025)

The Stack — MTK i openDesk (04.11.2025)

ITwiz — nowelizacja ustawy o KSC (02.04.2026)

Dodatkowo: NL Times (20.05.2025), Digital Health (21.10.2025) oraz prezentacje IBM: „Sovereignty” (B. Havers), „Put AI to Work: Od zasad do działania”, TechXchange 2026 „AI Operating Model”. AI Operating Model: Gartner (04.2026, 05.2026, Top Trends 2026), BCG (08.2026), IBM IBV i Oxford Economics (2026), IBM IBV (06.2026), Omdia/Cisco (08.2026); IBM „The AI Operating Model” (2026), McKinsey „The State of AI”, Gartner AI Survey, Black Duck OSSRA, Zillow Group (III kw. 2021), Bloomberg (02.05.2023). Przypadki AI: US BIS (01.2025, 05.2025), TechCrunch (06.2025), Reuters (07.2025, Nayara), The Verge (08.2025), BC CRT Moffatt v. Air Canada (02.2024), AFR (10.2025, Deloitte), Fortune (07.2025, Replit), Bloomberg (05.2025, Klarna), MIT NANDA (08.2025), Wired (07.2025, McHire), Garante Privacy (01.2025), PIPC Korea (02.2025). IBM Client Zero: ibm.com/case-studies/ibm-client-zero (02.2026). Polska i modele: KNF — uchylenie Rekomendacji D i komunikatu chmurowego (16.01.2025), KNF — rekomendacje ws. Frontier AI (22.07.2026), PKO BP — agent AI (bank.pl, Computerworld, 08.2026), CrowdStrike w Polsce (Spider's Web, 19.07.2024), PUZ Suwałki (TVN24, 30.09.2026), MyDr (Bezprawnik, RMF24, 2026), ITCI / Leaders Hub — rynek chmury (bank.pl). Efekt MTK: heise (Dania, 06.2025), The Stack (MTK i openDesk, 11.2025), Spider's Web (COI, 02.2026), CRN (Digital Commons EDIC, 10.2026), TechCrunch i CRN (Francja, 04.2026), eu-os.eu (EU OS), Google Cloud region Warszawa (04.2021), Microsoft Poland Central (04.2023), Ministerstwo Cyfryzacji — PLLuM (02.2025), SpeakLeash / ACK Cyfronet AGH — Bielik, IBM Granite. Regulacje: DORA art. 5, NIS2 art. 20, RODO art. 83.