

COORD CONTROL — ZBUDOWANY POD EU AI ACT

Od sierpnia 2026 prawo UE wymaga dowodu, co zrobiła Twoja AI. Tylko my go dostarczamy.

Coord Control nadzoruje agentów AI pracujących na komputerach firmy:
blokuje niebezpieczne działania, zapisuje, co naprawdę się stało, w sposób,
którego nikt nie podrobi, i cofa szkody z dowodem. Dokładnie to, czego dziś
wymagają EU AI Act, DORA i NIS2. Żaden inny produkt nie robi tego
wewnątrz systemów klienta.

EU AI ACT · ART. 12 · 13 · 14

DORA

NIS2

DZIAŁA NA TWOICH KOMPUTERACH

PATENT ZGŁOSZONY



Strażnik między agentem AI a Twoimi komputerami.

Agent AI to program, który działa sam: uruchamia komendy, zmienia pliki, sięga do baz danych. Coord Control stoi obok niego i robi cztery rzeczy.

1

Agent chce coś zrobić

Skasować folder, zmienić ustawienie, uruchomić komendę na serwerze.



2

Najpierw sprawdzamy

Wolno? Niebezpieczne? Potrzebna zgoda człowieka? Złe działania nigdy się nie wykonują.



3

Patrzymy na prawdziwy skutek

Co agent zapowiedział, a co naprawdę zmieniło się na maszynie.



4

Wystawiamy paragon, którego nikt nie podrobi

Podpisany, spięty w łańcuch. Audytor sprawdza go sam. Jeśli coś się zepsuło, przywracamy stan i to udowadniamy.

Nikt inny tego nie robi. Sprawdziliśmy 24 dostawców. Wielkie chmury robią to tylko we własnej chmurze, z której regulowane firmy w Europie nie mogą korzystać. Reszta zapisuje tylko to, co AI napisała.

Od 2 sierpnia 2026 EU AI Act wymaga trzech rzeczy od każdej firmy używającej AI na ważnych systemach.

ARTYKUŁ 12

Zapisuj, co zrobiła AI

Automatyczne logi, przechowywane co najmniej 6 miesięcy, pokazujące każde działanie.

ARTYKUŁ 14

Człowiek musi móc ją zatrzymać

Ktoś musi wiedzieć, co AI robi, i móc ją zatrzymać w każdej chwili.

ARTYKUŁ 13

Pokaż dowód audytorowi

Dowód, który zewnętrzny audytor sprawdzi bez zaufania do dostawcy.

€15M

lub 3% światowego obrotu: kara za niespełnienie

27

krajów UE, plus banki pod DORA i infrastruktura krytyczna pod NIS2

To nie jest opcja i nie jest przyszłość. Termin minął. Każdy bank, ubezpieczyciel, telekom, szpital, zakład energetyczny i urząd w UE, który używa agentów AI, musi to mieć dziś. Większość nie ma nic.

Prawo wymaga czterech rzeczy. Tylko Coord Control dostarcza wszystkie cztery.

KTO	DZIAŁA WEWNĄTRZ TWOICH SYSTEMÓW wymóg: suwerenność	ZATRZYMUJE DZIAŁANIA, CZŁOWIEK MOŻE PRZERWAĆ art. 14	ZAPISUJE, CO NAPRAWDĘ SIĘ STAŁO art. 12	AUDYTOR SPRAWDZA BEZ DOSTAWCY art. 13
Narzędzia agentowe Microsoft, Google, Anthropic	nie, tylko chmura	częściowo	loguje, o co proszono, nie co się stało	nie
Oprogramowanie AI governance (Credo AI, IBM, OneTrust)	w większości nie	nie, tylko raporty	nie	nie
Guardraile AI (Lakera, Galileo, NVIDIA)	nie	filtruje tylko tekst	nie	nie
Coord Control	tak, nawet bez internetu	tak, sześć bramek + kill switch	tak, zmierzone na maszynie	tak, jedna komenda, offline

Dokumentacja Microsoftu o własnym toolkicie: „does not verify whether the action actually succeeded”. Anthropic: „fully on-premise isn’t possible”. Przegląd 24 produktów, czerwiec 2026.

MACP to nasz system paragonów. Sprawia, że dowodu nie da się podrobić.

MACP (Multi-Agent Coordination Protocol) to nasz własny wynalazek. Każde działanie dostaje podpisany cyfrowy paragon, spięty z poprzednim jak ogniwa łańcucha. Zmień jeden, a łańcuch widocznie pęka. Audytor sprawdza cały łańcuch na własnym laptopie, offline, bez nas.

Chroniona technologia

Dziś tajemnica przedsiębiorstwa. Jedno zgłoszenie patentowe już złożone: jak paragony dowodzą prawdziwych skutków. Dziewięć kolejnych rodzin patentowych przygotowanych lub zidentyfikowanych (następny slajd), w tym sam MACP; do zgłoszenia pozostają poufne.

```
# agent AI próbuje:
$ rm -rf /srv/prod/data
ZABLOKOWANE brak uprawnień · exit 2
# paragon zapisany automatycznie:
paragon nr    18422    podpis ważny
wynik         nic nie zmieniono, udowodnione
# audytor sprawdza sam, offline:
$ verify paragon.json
paragon autentyczny: true
```

Demo w 60 sekund: agent próbuje skasować produkcję. Zablokowane, zanim się wykona. Paragon dowodzi, że nic się nie zmieniło. Wyciągnij kabel sieciowy, nadal działa.

Działa dziś, codziennie prowadzi naszą własną firmę i opiera się na 10 rodzinach patentowych.

501,000

podpisanych paragonów na prawdziwym ruchu agentów,
~2 800 dziennie

2,745

testów automatycznych przy każdej zmianie · 222 000+
linii kodu

10

rodzin patentowych: 1 zgłoszona, 2 gotowe do zgłoszenia,
3 kontynuacje, 4 kolejni kandydaci

Portfel patentowy

ZGŁOSZONE

1. Zobowiązanie efektu i weryfikowalne przywracanie stanu (CObS) · P.456328, UPRP, lipiec 2026 · okno PCT/EPO/US do lipca 2027

KONTYNUACJE PRZYGOTOWANE

- 4. Wykrywanie dryfu semantycznego
- 5. Weryfikacja przywrócenia ograniczona obserwacją
- 6. Wykrywanie nadwykonania

Tylko nazwy. Wszystko, co jeszcze nie zgłoszone, jest tajemnicą przedsiębiorstwa; szczegóły pod NDA w data roomie IP.

GOTOWE DO ZGŁOSZENIA

- 2. Suwerenny control plane: broker wstrzymujący poświadczenia
- 3. Kumulatywne egzekwowanie wielu działań

KOLEJNI KANDYDACI · POUFNE

- 7. Łańcuch nadzoru MACP
- 8. Federacyjny Coord Control
- 9. Ciągłość pracy (Work Continuity Control Plane)
- 10. Samobroniąca się polityka egzekucji

Gotowe dla enterprise

Single sign-on, role, eksport do narzędzi bezpieczeństwa, kopie zapasowe, podpisane pakiety. Działa z Claude, OpenAI Codex, Google Gemini i modelami open source.

Bez owijania

Jeszcze bez płacących klientów. Dwoje współzałożycieli, bez zespołu sprzedaży. Certyfikaty SOC 2 i FIPS niegotowe. Ta runda płaci dokładnie za te trzy rzeczy.

Sprzedawane firmom, które prawo zmusza do zakupu.

KROK 1

Płatny pilotaż

€10–30k

6–10 tygodni z 3–5 design partnerami, potem umowa roczna.

KROK 2

Umowa roczna

\$150–400k / rok

Banki, ubezpieczyciele, telekomy. Cena liczona względem kar, których unikają.

KROK 3

Wersja w pełni odizolowana

\$250k + \$288k / rok

Obronność i infrastruktura krytyczna, bez internetu.

Kto kupuje: najpierw banki i ubezpieczyciele, potem infrastruktura krytyczna, sektor publiczny, obronność, w całej UE-27, Wielkiej Brytanii, Izraelu i krajach NATO. **Jak:** przez integratorów IT, którzy już ich obsługują; pierwszy partner w Polsce w rozmowach, potem Niemcy, Skandynawia, Izrael.

RUNDA —

\$2,5 mln pre-seed na SAFE.

Prawo obowiązuje. Produkt jest zbudowany. Pieniądze zaniósł go do pierwszych regulowanych klientów. Pierwsze zamknięcie październik/listopad 2026, seed po dowodach w Q2 2027.

Na co idą: 56% zespół \$1.4M · 18% go-to-market \$450k · 14% patenty \$350k · 12% infrastruktura i certyfikaty \$300k. Burn ~\$130 tys./mies., 18+ miesięcy runway.

Co musi się udać

- 3–5 płacących design partnerów w regulowanych firmach
- 1 klient referencyjny, który mówi „kupiliśmy przez AI Act”
- Patenty rozszerzone międzynarodowo (PCT)
- SOC 2 zrobione, runda seed po dowodach w Q2 2027

Właściwy inwestor

Rozumie branże regulowane, cyberbezpieczeństwo lub obronność, w UE lub Izraelu.

Piotr Kędzierski · współzałożyciel i CTO · drugi raz founder (Flexee, exit \$7M) · autor zgłoszeń patentowych
Marta Kowalczyk-Kędzierska · współzałożycielka, prawo i GTM · adwokat, doktor prawa, MKK.legal
piotr@gotitlab.eu · marta@gotitlab.eu · gotitlab.eu · demo na żywo na życzenie