

REZYLIENCJA - BUDOWANIE ODPORNOŚCI SPOŁECZNEJ, GOSPODARCZEJ I TECHNOLOGICZNEJ PAŃSTWA



*Od państwa reagującego po fakcie do państwa,
które widzi wcześniej, wytrzymuje uderzenia i rozwija się dalej.*



Trzy filary odporności spięte państwem-regulatorem pod demokratyczną kontrolą Narodu.

Dokument programowy do publikacji na [TechnoSanacja.pl/postulat](https://technosanacja.pl/postulat)

Warszawa, lipiec 2026

SPIS TREŚCI

1. Definicja odporności społecznej, gospodarczej i technologicznej państwa
2. Diagnoza obecnego stanu odporności państwa
3. Mapa struktury odporności państwa
4. AI jako mechanizm wspomagający odporność
5. Elektroniczna dokumentacja i RAG budowania wiedzy
6. Gotowość organizacyjna administracji i prawo do sprawnego procesu lokalnego
7. Prawa obywatelskie w systemie odporności
8. KPI, KRI, publiczny rejestr i niezależny audyt
9. Polska mapa drogowa do nowego systemu odporności
10. Słownik skrótów
11. Źródła

FORMUŁA NACZELNA

ODPORNÓŚĆ TO ZDOLNOŚĆ, NIE DEKLARACJA

Odporność państwa jest zdolnością Narodu, instytucji i gospodarki do przewidywania zakłóceń, utrzymania funkcji krytycznych, szybkiego odtworzenia działania, adaptacji do trwałej zmiany oraz wykorzystania kryzysu do budowy nowych przewag. Nie mierzy się liczbą strategii, lecz czasem utrzymania usług, skalą strat, szybkością korekty i poziomem zaufania.

Rzeczpospolita traktuje odporność jako wspólny system trzech filarów: społecznego, gospodarczego i technologicznego. System ten jest koordynowany przez prezydencką administrację państwową, kontrolowany przez 100-osobowy Senat, korygowany przez rozstrzygające referendum i zasilany wiedzą lokalnych wspólnot reprezentowanych w Sejmikach samorządowych.

Celem nie jest państwo koszarowe ani społeczeństwo żyjące w lęku. Celem jest państwo spokojne, przygotowane i uczące się: takie, które w czasie pokoju poprawia jakość życia, w kryzysie chroni ludzi i ciągłość usług, a po kryzysie nie wraca mechanicznie do starego układu, lecz usuwa ujawnione słabości.

HASŁO PROGRAMU

Nie bunkier zamiast przyszłości. Infrastruktura, która służy codziennie i ratuje w kryzysie.

Nie centralizacja wszystkiego. Jedna strategia, jasne standardy, lokalna wiedza i pełna odpowiedzialność za wynik.

ARCHITEKTURA ODPORNOŚCI TECHNOREPUBLIKI

przewidzieć → wytrzymać → odtworzyć → zaadaptować → rozwinąć



Rysunek 1. Architektura odporności TechnoRepubliki Polskiej.

Nowe propozycje ustrojowe Rzeczypospolitej:

Element ustroju	Rola w systemie odporności	Bezpiecznik
Naród i referendum rozstrzygające	Nadaje mandat strategiczny i może skorygować kierunek w sprawach o najwyższym znaczeniu.	Jawna informacja, równy dostęp do debaty, kontrola zgodności pytania z Konstytucją.
Prezydent i administracja państwowa	Jeden właściciel strategii, portfela misji, budżetu, wykonania i ciągłości działania państwa.	Kadencyjność, publiczny dashboard, kontrola Senatu, audyt i prawo do odwołania.
Senat 100	Ustanawia prawo, zatwierdza ramy finansowania i kontroluje wykonanie programów odporności.	Jawne wystuchania, komisja odporności, raporty mniejszości.
Sejmiki samorządowe	Opiniują decyzje regionalne, ujawniają wiedzę lokalną, oceniają ryzyka i skutki dla wspólnot.	Brak własnej biurokracji wykonawczej, publikacja opinii i zdań odrębnych.
Administracja terenowa Prezydenta	Wojewoda, starosta i burmistrz jako państwowi właściciele ciągłości usług i lokalnych planów odporności.	Standard krajowy + lokalny audyt + mierzalne SLA.

1. DEFINICJA ODPORNOŚCI SPOŁECZNEJ, GOSPODARCZEJ I TECHNOLOGICZNEJ PAŃSTWA

Odporność państwa to zdolność wspólnoty narodowej do zachowania życia, praw obywatelskich, tożsamości, sterowności i podstawowych funkcji mimo wojny, katastrofy, pandemii, blackoutu, cyberataku, kryzysu finansowego, przerywania łańcuchów dostaw albo gwałtownej zmiany technologicznej.

Definicja TechnoRepubliki łączy pięć kolejnych zdolności: przewidywanie, absorpcję, odtworzenie, adaptację i transformację. Pierwsze trzy odpowiadają za „odbicie” po szoku. Dwie ostatnie pozwalają przejść naprzód, gdy stara norma już nie wróci: na przykład w obliczu starzenia społeczeństwa, rewolucji AI, trwałej fragmentacji handlu lub zmiany klimatu.

CYKL ODPORNOŚCI: POWRÓT I PRZEJŚCIE NAPRZÓD



Rysunek 2. Cykl odporności: od przewidywania do transformacji.

1.1. Odporność społeczna

Odporność społeczna jest zdolnością ludzi i wspólnot do współdziałania pod presją, zachowania zdrowia psychicznego i fizycznego, rozpoznawania manipulacji, korzystania z wiarygodnych informacji, udzielania wzajemnej pomocy oraz odbudowy zaufania po konflikcie lub katastrofie.

- kapitał społeczny pomostowy: współpraca między pokoleniami, środowiskami i regionami, nie tylko wewnątrz własnej grupy;
- kompetencje kryzysowe i cyfrowe: pierwsza pomoc, cyberhigiena, komunikacja, korzystanie z usług publicznych online i offline;
- odporność poznawcza: prebunking, edukacja medialna, jawne źródła i umiejętność odróżniania faktu, opinii i manipulacji;
- gotowość domowa i lokalna: minimalne zapasy, plan kontaktu, wiedza o schronieniu, ewakuacji i pomocy osobom zależnym;
- sojusz Gen Z i Seniorów: cyfrowa sprawność młodych połączona z doświadczeniem, pamięcią instytucjonalną i lokalnymi sieciami seniorów.

1.2. Odporność gospodarcza

Odporność gospodarcza jest zdolnością państwa i przedsiębiorstw do utrzymania produkcji, energii, finansów, logistyki, zatrudnienia i dostaw dóbr podstawowych mimo szoku. Nie oznacza autarkii. Oznacza zarządzanie zależnościami, dywersyfikację, rezerwy o policzonym koszcie oraz zdolność szybkiego przestawienia zasobów.

- energia i paliwa: stabilne zasilanie przemysłu, usług publicznych, centrów danych i gospodarstw domowych;
- produkcja strategiczna i dual-use: zdolność wytwarzania urządzeń, leków, komponentów, oprogramowania i środków ochrony;
- łańcuchy dostaw i rezerwy: mapa wąskich gardeł, wielu dostawców, substytuty, zapasy rotowane i zdolność naprawy;
- finanse i ubezpieczenia: bufor fiskalny, warstwowanie ryzyka, fundusze awaryjne i transfer ryzyka ex ante;
- rynek bez prywatnych bram: przeciwdziałanie monopolom i uzależnieniu od pojedynczych platform, które mogą blokować dostęp do klienta, kapitału lub danych.

1.3. Odporność technologiczna

Odporność technologiczna jest zdolnością do utrzymania, naprawy, bezpiecznego rozwoju i suwerennego kontrolowania infrastruktury danych, AI, łączności, cyberbezpieczeństwa, chmury, energii, transportu i systemów sterowania. Kluczowe jest nie tylko posiadanie technologii, lecz wiedza, jak ją modyfikować, integrować i zastąpić.

- odporność „by design”: bezpieczeństwo, redundancja, tryb degradacji i odtworzenie projektowane od początku;
- suwerenne dane i modele: możliwość migracji, przenoszalność, otwarte standardy i brak uzależnienia od jednego dostawcy;
- cyberodporność: zero trust, kopie offline, segmentacja, ćwiczenia, zarządzanie podatnościami i bezpieczeństwo łańcucha software’u;
- zdolność absorpcyjna: kadry, laboratoria, zamówienia innowacyjne i zdolność państwa do uczenia się technologii;
- infrastruktura dual-use: obiekty, które w pokoju służą gospodarce i mieszkańcom, a w kryzysie zapewniają zasilanie, łączność, schronienie lub logistykę.

FORMUŁA OPERACYJNA

Odporność państwa = (zdolność przewidywania × ciągłość działania × szybkość odtworzenia × adaptacja) – podatność na zależności i przechwycenie.

Każdy składnik musi być mierzony, mieć właściciela i próg alarmowy.

2. DIAGNOZA OBECNEGO STANU ODPORNOŚCI PAŃSTWA

Polska weszła w okres kumulacji ryzyk: wojny na wschodzie, presji hybrydowej, starzenia ludności, niepewności energetycznej, cyfrowej zależności, niedoboru specjalistów i gwałtownego przyspieszenia AI. Jednocześnie posiada mocne zasoby: duży rynek, rozwiniętą łączność stacjonarną, rosnące kompetencje technologiczne, aktywne wspólnoty lokalne, przemysł, diasporę oraz doświadczenie pokoleń.

PUNKT WYJŚCIA 2026

Rama prawna ochrony ludności istnieje i jest finansowana. Luka przesuwana się z poziomu „brak ustawy” na poziom wykonania: jakości projektów, kadr, interoperacyjności, ćwiczeń, danych, zaufania i rozliczalności.

2.1. Osiem luk systemowych

1. Rozproszenie odpowiedzialności. Wiele instytucji uczestniczy w przygotowaniu i reakcji, lecz obywatel nie widzi jednego właściciela wyniku, terminu i kosztu.
2. Brak wspólnej mapy ryzyk i zależności. Rejestry są sektorowe, a awarie kaskadowe przechodzą między energią, telekomunikacją, finansami, transportem i zdrowiem.
3. Przewaga procedury nad zdolnością. Raportuje się liczbę zakupów, szkoleń i posiedzeń, zamiast czasu utrzymania usług, skuteczności ostrzeżenia i tempa odtworzenia.
4. Niski poziom zaufania do instytucji politycznych oraz wyraźna luka pokoleniowa. Bez wiarygodności komunikatu nawet najlepszy plan kryzysowy będzie ignorowany.
5. Niedostateczna absorpcja technologii w przedsiębiorstwach i administracji. Polska ma dobre podstawy cyfrowe, lecz wolno wdraża zaawansowane technologie i odczuwa niedobór specjalistów ICT.
6. Uzależnienia od zewnętrznych platform, chmur, komponentów i oprogramowania. Brak planów wyjścia oraz testowanej przenoszalności zwiększa ryzyko przestoju i utraty autonomii.
7. Słaba pamięć instytucjonalna. Wnioski z ćwiczeń, awarii i kryzysów są rozproszone w dokumentach, a zmiana kadr często zrywa ciągłość wiedzy.
8. Nierówny dostęp lokalny. Mieszkaniec ma inne szanse na ostrzeżenie, pomoc, energię awaryjną i kompetentną obsługę zależnie od regionu, wieku, sprawności i jakości lokalnej administracji.

2.2. Wybrane dane diagnostyczne

Wskaźnik	Stan / sygnał	Wniosek programowy
Zaufanie do rządu krajowego	32% osób w Polsce deklarowało wysokie lub umiarkowanie wysokie zaufanie w badaniu OECD 2025; średnia OECD: 40%.	Odporność wymaga wiarygodności, jawności dowodów i realnego wpływu obywatela.
Zaufanie do służby cywilnej	34% w Polsce wobec 45% średnio w OECD.	Profesjonalizacja kadr, przejrzyste konkursy, stabilna pamięć instytucjonalna.
Luka pokoleniowa zaufania	18% wśród młodych wobec 43% w grupie 50+.	Program 2G: realne role młodych i seniorów, nie komunikacja symboliczna.
Wykorzystanie AI przez przedsiębiorstwa	8,4% polskich przedsiębiorstw w 2025 r.; średnia UE: 20%.	Misje wdrożeniowe, zamówienia innowacyjne, kompetencje i bezpieczna infrastruktura AI.
Cyfrowe kompetencje i kadry ICT	Komisja Europejska wskazuje niski poziom umiejętności cyfrowych, różnice wieś–miasto i między grupami wieku oraz niedobór specjalistów ICT.	Powszechna edukacja, reskilling, lokalne centra kompetencji i dostęp offline.
Finansowanie ochrony ludności	Program 2025–2026: minimum 0,3% PKB; 16,7 mld zł w 2025 r. i 17,2 mld zł w 2026 r.	Budżet trzeba powiązać z wynikiem, cyklem życia aktywów i audytem.

2.3. Diagnoza trzech filarów

Filar	Mocne strony	Główne podatności	Pierwsza dźwignia
Społeczny	silne więzi rodzinne i lokalne; wolontariat; aktywność obywatelska; zasób doświadczenia seniorów	polaryzacja, niski poziom zaufania politycznego, nierówne kompetencje cyfrowe, dezinformacja	wiarygodna komunikacja, ćwiczenia lokalne, program 2G, prawo do wyjaśnienia
Gospodarczy	duży rynek, przemysł, położenie logistyczne, rosnący sektor technologiczny	energia, import komponentów i surowców, koncentracja dostawców, niedostateczne bufory	mapa zależności, zamówienia strategiczne, dywersyfikacja i rezerwy rotowane
Technologiczny	dobra łączność stacjonarna, e-usługi publiczne, rozwój polskich modeli i kompetencji	niska adopcja AI, niedobór ICT, vendor lock-in, cyberzagrożenia i silosy danych	suwerenny graf wiedzy, standardy interoperacyjności, cyberodporność i testy wyjścia

DIAGNOZA W JEDNYM ZDANIU

Polsce nie brakuje pojedynczych zasobów; brakuje systemu, który łączy je w mierzalną zdolność, nadaje odpowiedzialnego właściciela, zapewnia pełny ślad i szybko koryguje błąd.

3. MAPA STRUKTURY ODPORNOŚCI SPOŁECZNEJ, GOSPODARCZEJ I TECHNOLOGICZNEJ PAŃSTWA

MAPA 15 DOMEN ODPORNOŚCI PAŃSTWA



Warstwa wspólna: prawo • administracja • pomiar • audyt • komunikacja • współpraca 20

Rysunek 3. Piętnaście domen odporności państwa.

3.1. Struktura zarządzania

Poziom	Główna funkcja	Produkty obowiązkowe
Naród	mandat, kontrola i korekta strategiczna	referendum rozstrzygające; prawo do informacji; konsultacja planów wieloletnich
Prezydent	właściciel narodowej strategii odporności i ciągłości państwa	Narodowy Plan Odporności; portfel misji; decyzje międzysektorowe; komunikat strategiczny
Prezydenckie Centrum Odporności i Ciągłości	integracja danych, ryzyk, budżetu, ćwiczeń i alarmów	Krajowy Rejestr Ryzyk; dashboard; cyfrowy bliźniak; kanał algedoniczny
Senat 100	prawo, budżet, kontrola i wystuchanie publiczne	ustawy ramowe; komisja odporności; jawny raport roczny; kontrola założeń krytycznych
Agencje misyjne i operatorzy krytyczni	wykonanie zdolności sektorowych	plany ciągłości, paszporty odporności, rezerwy, ćwiczenia i raporty incydentów
Administracja terenowa Prezydenta	lokalne wykonanie, integracja służb, ochrona ludności	plan regionalny, mapa obiektów, centra wsparcia, SLA usług i ćwiczenia
Sejmiki samorządowe	lokalna wiedza, konsultacja i społeczna kontrola	opinia regionalna, lista ryzyk lokalnych, zdanie odrębne, ocena skutków społecznych
Wspólnoty, firmy, uczelnie, NGO i obywatele	współprodukcja zdolności i sygnał zwrotny	lokalne zespoły, rezerwa kompetencji, pilotaże, zgłoszenia i ocena usług

3.2. Dwanaście funkcji krytycznych do utrzymania

Funkcja	Minimalny standard ciągłości	Przykładowy miernik
kierowanie państwem	ciągłość konstytucyjna i zastępowalność centrów decyzyjnych	czas przełączenia centrum kierowania
energia	zasilanie usług krytycznych, black-start, mikrosieci i paliwa awaryjne	godziny autonomii obiektów krytycznych
łączność i informacja	wielokanałowe ostrzeganie, łączność zapasowa, komunikat wiarygodny	udział ludności osiągniętej w 10 minut
woda i żywność	bezpieczne dostawy, rezerwy, dystrybucja do osób zależnych	dni pokrycia i czas uruchomienia punktów
zdrowie	masowe zdarzenia, zapasy leków, ciągłość e-zdrowia i tryb offline	czas zwiększenia pojemności systemu
transport i logistyka	korytarze awaryjne, paliwa, porty i kolej	czas przywrócenia kluczowego korytarza
finanse i płatności	gotówka, płatności awaryjne, ciągłość banków i rozliczeń	czas działania w trybie ograniczonym
administracja i tożsamość	rejestry, dokumenty, obsługa praw i świadczeń	odsetek usług dostępnych offline
cyberbezpieczeństwo	detekcja, izolacja, kopie, odtworzenie i wymiana informacji	MTTD/MTTR dla incydentów krytycznych
produkcja strategiczna	zdolność zwiększenia produkcji i naprawy	czas osiągnięcia 150% produkcji bazowej
porządek i ratownictwo	koordynacja służb, rezerwy, interoperacyjna łączność	czas mobilizacji zasobów regionalnych
spójność społeczna	pomoc sąsiedzka, informacja, ochrona grup wrażliwych	udział gmin z aktywną siecią wsparcia

3.3. Zasada rekursji

Ten sam schemat musi działać w skali kraju, regionu, miasta, przedsiębiorstwa i obiektu krytycznego: cel, właściciel, dane, zasoby, wskaźniki, kanał alarmowy, plan odtworzenia i audyt. Lokalna autonomia wykonawcza jest dopuszczalna tylko przy wspólnych standardach, interoperacyjności i jawnej odpowiedzialności.

ZASADA SUBSYDIARNOŚCI OPERACYJNEJ

Centrum nie ma wykonywać wszystkiego. Ma ustalić minimalny standard, zapewnić finansowanie, dane, interoperacyjność i rozliczenie.

Lokalny poziom dobiera środki do realnych warunków i odpowiada za wynik.

4. AI JAKO MECHANIZM WSPOMAGAJĄCY ODPORNOŚĆ PAŃSTWA

Sztuczna inteligencja ma zwiększać wymaganą różnorodność państwa: szybciej wykrywać słabe sygnały, łączyć dane z wielu sektorów, tworzyć warianty, wskazywać zależności i wspierać koordynację. Nie może zastąpić mandatu demokratycznego, odpowiedzialności urzędnika ani prawa obywatela do wyjaśnienia i odwołania.

4.1. Architektura agentowa

System odporności może wykorzystywać wyspecjalizowanych agentów AI: badawczego, ryzyka, prawnego, logistycznego, cyber, komunikacyjnego, audytowego i obywatelskiego. Każdy agent ma kartę: właściciela, mandat, zakres danych, narzędzia, poziom autonomii, log, testy, termin przeglądu i wyłącznik awaryjny.

ZASADA „ŻADEN AGENT BEZ WŁAŚCICIELA”

AI nie jest anonimowym uczestnikiem decyzji. Każde użycie systemu musi pozostawić niezaprzeczalny ślad: kto uruchomił, na jakich danych, z jakim celem, jaką rekomendację otrzymał, co zatwierdził człowiek i jaki był wynik.

4.2. Główne zastosowania

Obszar	Rola AI	Wymagany bezpiecznik
horizon scanning	wykrywanie słabych sygnałów w danych gospodarczych, cyber, zdrowiu, pogodzie i mediach	jawne źródła, ocena błędów, ekspert domenowy
mapa zależności	graf dostawców, infrastruktury, przepływów energii, danych i własności	ochrona tajemnic, walidacja podmiotów, aktualność danych
wczesne ostrzeżenie	prognoza przeciążeń, awarii kaskadowych i zmian ryzyka	próg alarmowy zatwierdzony przez człowieka, zakaz automatycznej eskalacji represyjnej
symulacje polityk	cyfrowe bliźniaki, agent-based modelling, Monte Carlo, AHP/MCDA	publikacja założeń, scenariusze alternatywne, red teaming
koordynacja zasobów	dobór zespołów, tras, magazynów, energii i kolejności interwencji	człowiek w dowodzeniu, log decyzji, możliwość ręcznego przejęcia
obsługa obywatela	informacja, tłumaczenie, wyszukanie uprawnienia, status sprawy	brak ostatecznej decyzji bez człowieka, dostęp kanałem tradycyjnym
audyt i kontroling	wykrywanie anomalii, konfliktów interesów, opóźnień i rozbieżności budżetowych	niezależny audyt modelu, ochrona sygnalistów, prawo do zakwestionowania
uczenie po kryzysie	analiza logów, decyzji, czasu i skutków; automatyczne lessons learned	zatwierdzenie wniosków przez wielodyscyplinarny zespół

4.3. Czerwone linie

- zakaz niejawnego profilowania politycznego i manipulowania obywatelami pod pozorem odporności poznawczej;
- zakaz automatycznych, niewyjaśnialnych decyzji ograniczających prawa, świadczenia, swobodę przemieszczania lub dostęp do usług;
- zakaz uzależnienia krytycznej funkcji od pojedynczego modelu, chmury, dostawcy lub połączenia internetowego;
- obowiązek testu dyskryminacji, cyberbezpieczeństwa, odporności na prompt injection, zatrucie danych i manipulację agentów;
- obowiązek ręcznego trybu działania, planu wyjścia, przenoszalności danych i regularnych ćwiczeń bez AI.

5. ELEKTRONICZNE ZARZĄDZANIE DOKUMENTACJĄ I RAG BUDOWANIA WIEDZY O ODPORNOŚCI

DOKUMENTACJA + RAG: PAŃSTWO UCZY SIĘ Z WŁASNEGO ŚŁADU



Rysunek 4. Elektroniczna dokumentacja i RAG jako pamięć instytucjonalna państwa.

5.1. Cel

Państwo odporne nie może uczyć się wyłącznie z pamięci pojedynczych urzędników. Każdy plan, ćwiczenie, incydent, decyzja, koszt, opinia Sejmiku, wynik audytu i wniosek po kryzysie powinny trafiać do ustrukturyzowanego, wersjonowanego i bezpiecznego zasobu wiedzy.

5.2. Narodowy Graf Wiedzy o Odporności

- jednolita taksonomia zagrożeń, usług krytycznych, zasobów, obiektów, kompetencji, podmiotów i decyzji;
- powiązania między dokumentami, wersjami, autorami, podstawami prawnymi, danymi, założeniami i miernikami;
- odrębne warstwy: publiczna, służbowa, poufna i niejawna, z zasadą najmniejszych uprawnień;
- obowiązkowa proveniencja: każde twierdzenie i rekomendacja wskazują źródło, datę, wersję i poziom pewności;
- mechanizm korekty: błąd w rejestrze lub dokumencie można zgłosić, ocenić, poprawić i prześledzić historię zmiany.

5.3. Standard elektronicznej dokumentacji

Element	Standard minimalny	Efekt
identyfikacja	unikalny identyfikator sprawy, dokumentu, obiektu, ryzyka i agenta	pełny ślad i brak duplikacji
metadane	autor, właściciel, data, wersja, podstawa prawna, poziom dostępu, termin przeglądu	wyszukiwalność i odpowiedzialność
format	otwarte formaty, eksport, podpis i pieczęć elektroniczna, archiwizacja długoterminowa	brak vendor lock-in
workflow	jedna sprawa, jeden właściciel, role RACI, terminy, eskalacja i decyzja	krótsza pętla i brak rozmycia
RAG	wyszukiwanie w zatwierdzonym korpusie, cytowanie źródła i sygnalizowanie braku danych	mniej halucynacji i szybsza analiza
logowanie	kto czytał, zmieniał, pytał model, zatwierdzał i eksportował	audyt i cyberbezpieczeństwo
retencja	jasny cykl życia i automatyczne terminy przeglądu	aktualność i ograniczenie nadmiaru danych
ciągłość	kopie geograficzne, offline, testy odtworzenia i alternatywne kanały	działanie podczas awarii

5.4. Jak działa RAG

RAG — generowanie wspomagane wyszukiwaniem — nie „uczy” modelu wszystkiego na stałe. Najpierw wyszukuje właściwe, aktualne i uprawnione dokumenty, a następnie tworzy odpowiedź z ich kontekstu. W systemie publicznym odpowiedź musi pokazywać użyte źródła, wersje i zakres niepewności. Brak źródła jest sygnałem do wstrzymania odpowiedzi, a nie do zgadywania.

ZASADA PAMIĘCI PAŃSTWA

Dokument bez metadanych jest trudny do znalezienia. Wiedza bez właściciela szybko się starzeje. Rekomendacja AI bez źródła nie może stanowić podstawy decyzji publicznej.

6. GOTOWOŚĆ ORGANIZACYJNA ADMINISTRACJI I PRAWO DO SPRAWNEGO LOKALNEGO PROCESU DECYZYJNEGO

Zmiana technologiczna bez zmiany odpowiedzialności automatyzuje chaos. Dlatego wdrożenie odporności zaczyna się od modelu operacyjnego: kto rozpoznaje ryzyko, kto jest właścicielem usługi, kto dysponuje zasobami, kto podejmuje decyzję, kto komunikuje ją obywatelowi i kto odpowiada za wynik.

PRAWO DO SPRAWNEGO PROCESU LOKALNEGO



**Prawa: ostrzeżenie • ciągłość • wyjaśnienie
prywatność • równy dostęp**

Sejmik: opinia • ryzyka • zdanie odrębne

Rysunek 5. Prawo obywatela do sprawnego procesu i rola Sejmiku samorządowego.

6.1. Docelowy model operacyjny

Warstwa	Odpowiedzialność	Narzędzie
Prezydent	ustala misję, priorytety, progi ryzyka i rozstrzyga konflikty międzysektorowe	Prezydencki Dashboard Odporności
Centrum Odporności i Ciągłości	prowadzi Krajowy Rejestr Ryzyk, model zależności, ćwiczenia i kanał alarmowy	graf wiedzy, cyfrowy bliźniak, centrum sytuacyjne
Sekretariaty i agencje	budują zdolności sektorowe i rozliczają operatorów	kontrakty wynikowe, KPI/KRI, audyt
Administracja terenowa	zapewnia lokalną ciągłość, ostrzeganie, schronienie, pomoc i obsługę spraw	lokalny plan odporności, centrum 24/7, SLA
Sejmiki samorządowe	opiniują wpływ decyzji na wspólnotę, wskazują ryzyka i proponują warianty	publiczne posiedzenie, opinia, zdanie odrębne
Obywatel	zgłasza, współtworzy, kontroluje, korzysta z prawa do informacji i odwołania	jedno wejście, status, konsultacja, odwołanie

6.2. Test gotowości organizacyjnej

1. Czy każda funkcja krytyczna ma jednego właściciela końcowego i wyznaczonego zastępcę?
2. Czy znane są minimalne poziomy usługi, progi alarmowe, maksymalny czas przerwy i kolejność odtworzenia?
3. Czy zasoby, umowy, dane, kompetencje i zapasy są zinwentaryzowane oraz sprawdzane w ćwiczeniu?
4. Czy system może działać bez internetu, chmury, jednego budynku lub kluczowej osoby?
5. Czy administracja zna zależności od firm prywatnych i ma zapewniony dostęp do informacji w kryzysie?
6. Czy komunikat dla obywatela jest prosty, spójny, wielokanałowy i dostępny dla osób starszych oraz z niepełnosprawnościami?
7. Czy po ćwiczeniu powstaje plan korekty z terminem, budżetem i odpowiedzialnym, a nie tylko raport?
8. Czy obywatel może zobaczyć status, podstawę decyzji, źródła i tryb odwołania?

6.3. RACI po polsku

Litera	Znaczenie	Zasada
R — realizuje	osoba lub zespół wykonujący zadanie	może być kilku wykonawców, ale zakres jest jawny
A — odpowiada	jeden właściciel wyniku, który zatwierdza i ponosi odpowiedzialność	dla jednego zadania tylko jedna osoba A
C — konsultowany	podmiot dostarczający wiedzę przed decyzją	tu mieści się Sejmik, ekspert, operator i wspólnota
I — informowany	podmiot otrzymujący wynik i status	obywatel nie może być ostatnim, który dowiaduje się o zmianie

6.4. Prawo do sprawnego procesu lokalnego

Obywatel nie powinien znać mapy urzędów. Państwo powinno znać mapę odpowiedzialności. Każda sprawa lokalna dotycząca ryzyka, inwestycji krytycznej, ewakuacji, infrastruktury, świadczenia lub ciągłości usług otrzymuje jeden identyfikator, właściciela, termin, status, podstawę prawną i ścieżkę odwołania.

STANDARD „JEDNA SPRAWA — JEDEN WŁAŚCICIEL — PEŁNY ŚLAD”

Nawet gdy w procesie uczestniczy wiele instytucji, obywatel komunikuje się z jednym odpowiedzialnym prowadzącym. Administracja sama organizuje współpracę agentów, a nie przerzuca koszt koordynacji na mieszkańca.

7. PRAWA OBYWATELSKIE W ODNIESIENIU DO ODPORNOŚCI PAŃSTWA

Odporność nie może być pretekstem do nieograniczonego nadzoru, centralizacji i ograniczania praw. Silne państwo wymaga równie silnej kontroli regulatora. Dlatego każda zdolność kryzysowa musi mieć podstawę prawną, cel, czas obowiązywania, proporcjonalność, nadzór, ślad i możliwość odwołania.

7.1. Katalog praw

Prawo	Treść praktyczna	Obowiązek państwa
do ostrzeżenia	szybki, zrozumiały i wielokanałowy komunikat o zagrożeniu	utrzymywać systemy, testować zasięg, podawać źródło i instrukcję działania
do ciągłości usług	dostęp do podstawowych usług także w trybie ograniczonym lub offline	określić minimalny standard i kolejność odtworzenia
do informacji o ryzyku	poznanie ryzyka lokalnego, planów, miejsc ochrony i odpowiedzialnych podmiotów	publikować jawne części rejestru ryzyk i plany lokalne
do wyjaśnienia decyzji	poznanie kryteriów, danych, źródeł, udziału AI i osoby zatwierdzającej	zapewnić czytelne uzasadnienie i pełny ślad
do odwołania i kontroli człowieka	zakwestionowanie automatycznej rekomendacji lub błędnych danych	zapewnić człowieka, termin, niezależny organ i sąd
do prywatności	minimalizacja danych, ograniczenie celu, kontrola dostępu i retencji	prowadzić rejestr użycia danych i audyt bezpieczeństwa
do równego dostępu	brak wykluczenia z powodu wieku, miejsca zamieszkania, niepełnosprawności lub braku kompetencji cyfrowych	utrzymywać kanały tradycyjne, dostępność i wsparcie
do udziału lokalnego	możliwość zgłoszenia wiedzy, opinii i alternatywy przed decyzją regionalną	konsultować przez Sejmiki i odpowiadać na uwagi
do korekty strategicznej	udział w referendum w sprawach ustrojowych i o najwyższym znaczeniu	zapewnić pluralistyczną informację i integralność głosowania

7.2. Bezpieczniki nadzwyczajne

- zasada konieczności i proporcjonalności: tylko środki niezbędne do konkretnego zagrożenia;
- ograniczenie czasowe i automatyczny wygaśnik; przedłużenie wymaga jawnego uzasadnienia;
- kontrola Senatu i niezależnego sądu, w tym szybka ścieżka skargi;
- zakaz wykorzystywania danych kryzysowych do marketingu politycznego, komercyjnego profilowania lub represji niezwiązanej z zagrożeniem;
- publiczny raport po zakończeniu stanu nadzwyczajnego: decyzje, koszty, błędy, skutki dla praw i plan naprawczy;
- ochrona sygnalistów, dziennikarzy, ekspertów i obywateli zgłaszających błąd systemu.

MORAL POWER

Siła państwa jest legalna i trwała tylko wtedy, gdy pozostaje ograniczona Konstytucją, przejrzysta, rozliczalna i używana w obronie dobra wspólnego. Odporność bez praw tworzy państwo nadzoru; prawa bez zdolności tworzą państwo bezsilne.

8. KPI, KRI, PUBLICZNY REJESTR ORAZ NIEZALEŻNY AUDYT ODPORNOŚCI

NARODOWY INDEKS ODPORNOŚCI

ZDOLNOŚĆ
czas utrzymania

PODATNOŚĆ
zależności

GOTOWOŚĆ
ćwiczenia

ADAPTACJA
czas korekty

ZAUFANIE
wiarygodność

SUWERENNOŚĆ
dane i energia

Mapa zdolności i ryzyk — nie ranking.

Rysunek 6. Narodowy Indeks Odporności jako mapa podatności i zdolności.

8.1. Narodowy Indeks Odporności

Narodowy Indeks Odporności nie powinien być pojedynczą liczbą używaną do propagandy lub rankingu regionów. Ma być wielowarstwowym dashboardem pokazującym zdolności, podatności, trendy, progi alarmowe i nierówności terytorialne. Wskaźnik krajowy agreguje dane, ale zawsze pozwala zejść do domeny, regionu, usługi i obiektu.

8.2. KPI — mierniki zdolności i wyniku

KPI	Definicja	Częstotliwość	Właściciel
ciągłość funkcji krytycznych	odsetek funkcji spełniających minimalny standard w ćwiczeniu i incydencie	kwartalnie / po incydencie	Prezydenckie Centrum Odporności
czas ostrzeżenia	mediana czasu od wykrycia do dotarcia instrukcji do 90% ludności objętej zagrożeniem	każde ćwiczenie	administracja terenowa
autonomia energetyczna	godziny działania obiektów krytycznych bez zasilania zewnętrznego	półrocznie	agencja energii i operatorzy
czas odtworzenia	RTO dla energii, łączności, danych, zdrowia, płatności i administracji	kwartalnie	właściciel usługi
skuteczność ćwiczeń	odsetek działań wykonanych w czasie i zgodnie ze standardem	po każdym ćwiczeniu	niezależny zespół oceny
zamknięcie wniosków	odsetek działań naprawczych wykonanych w terminie	miesięcznie	delivery unit
dywersyfikacja dostaw	udział produktów krytycznych bez pojedynczego dostawcy >40%	kwartalnie	agencja gospodarcza
adopcja AI i automatyzacji	udział podmiotów i procesów z wdrożeniem spełniającym standard bezpieczeństwa	rocznie	agencja technologiczna
kompetencje społeczne	udział mieszkańców znających lokalny plan, alarmy i podstawy cyberhigieny	rocznie	administracja terenowa
zaufanie i legitymizacja	zaufanie do komunikatów, służby cywilnej i sposobu użycia danych	rocznie	niezależny ośrodek badawczy

8.3. KRI — wskaźniki ryzyka i podatności

KRI	Próg alarmowy — przykład	Reakcja
koncentracja dostawcy	>40% krytycznej dostawy od jednego podmiotu lub kraju	plan dywersyfikacji, rezerwa i substytut
zależność chmurowa	brak testowanego eksportu lub alternatywnego środowiska	test wyjścia, kopia danych, kontrakt migracyjny
dług technologiczny	system po wsparciu producenta lub z krytyczną podatnością >30 dni	izolacja, aktualizacja, wymiana
brak kadr	obsada funkcji krytycznej poniżej 80% lub brak zastępcy	rezerwa kompetencji, szkolenie, wsparcie międzyregionowe
starzenie danych	kluczowe dane bez aktualizacji dłużej niż ustalony cykl	blokada automatycznej rekomendacji, przegląd właściciela
spadek zaufania	spadek o >10 p.p. w grupie lub regionie	audyt komunikacji, dialog lokalny, korekta procesu
niewykonane wnioski	>20% działań po ćwiczeniu po terminie	eskalacja do Prezydenta i Senatu, zmiana właściciela
jednoczesność ryzyk	korelacja lub kaskada między co najmniej trzema funkcjami krytycznymi	uruchomienie scenariusza wielosektorowego

8.4. Publiczny Rejestr Odporności

Publiczny rejestr pokazuje dla każdego programu: cel, właściciela, budżet, harmonogram, KPI, KRI, stan realizacji, wyniki ćwiczeń, istotne ryzyka, decyzje korygujące i wnioski audytu. Informacje niejawne są chronione, ale ich istnienie, zakres oraz organ kontroli pozostają jawne w stopniu bezpiecznym.

8.5. Niezależny audyt

- audyt zdolności: czy system rzeczywiście działa w ćwiczeniu i podczas awarii;
- audyt danych i AI: jakość danych, bezpieczeństwo, bias, wyjaśnialność, odporność na atak i zgodność z prawami;
- audyt finansowy i koszt efektu: nie tylko zgodność wydatku, lecz cena uzyskanej zdolności;
- audyt społeczny: dostępność, równość, zaufanie, udział wspólnot i skutki dla praw;
- red team i test zaskoczenia: niezapowiedziane scenariusze, awaria dostawcy, brak internetu, utrata budynku, dezinformacja;
- jawny plan naprawczy z terminem, właścicielem i możliwością zakończenia programu nieskutecznego.

NIE PROPAGANDA SUKCESU — PUBLICZNY ŚLAD ODPOWIEDZIALNOŚCI

Program skuteczny może być skalowany. Program nieskuteczny wymaga korekty, zmiany właściciela, ograniczenia budżetu albo zakończenia. Brak wyniku nie może być ukrywany liczbą konferencji, dokumentów i wydanych środków.

9. POLSKA MAPA DROGOWA DO NOWEGO SYSTEMU ODPORNOŚCI

MAPA DROGOWA: OD POMIARU DO ZDOLNOŚCI



Rysunek 7. Horyzonty wdrożenia systemu odporności.

9.1. Pierwsze 100 dni — mandat i widzialność

1. Powołanie Prezydenckiego Centrum Odporności i Ciągłości oraz wskazanie jednego właściciela programu.
2. Przyjęcie definicji, taksonomii i minimalnych standardów dla 12 funkcji krytycznych.
3. Uruchomienie jawnego Krajowego Rejestru Ryzyk z częścią ostrą i chroniczną.
4. Mapa 50 największych podatności: energia, łączność, zdrowie, dane, finanse, transport, żywność, woda i produkcja.
5. Inwentaryzacja krytycznych umów, dostawców, chmur, licencji, zapasów, kompetencji i planów wyjścia.
6. Wybór trzech pilotaży regionalnych reprezentujących metropolię, region przemysłowy i obszar peryferyjny.
7. Przyjęcie Karty Agenta AI, standardu logowania i zakazu decyzji wysokiego wpływu bez człowieka.
8. Uruchomienie publicznego dashboardu z baseline, nie z obietnicami.

9.2. Dwanaście miesięcy — pilotaż i pomiar

- pierwsza wersja Narodowego Indeksu Odporności oraz paszporty odporności obiektów krytycznych;
- Narodowy Graf Wiedzy o Odporności, standard metadanych i RAG dla zatwierdzonego korpusu;
- ćwiczenie wielosektorowe: blackout + cyberatak + dezinformacja + presja na zdrowie i płatności;
- program 2G Odporność: młodzi trenerzy cyfrowi i seniorzy jako mentorzy ciągłości, lokalnej pamięci i pomocy;
- pilotaż regionalnych mikrosieci, łączności zapasowej, centrów wsparcia i mobilnych punktów usług;
- ustawa o Publicznym Rejestrze Programów Odporności i niezależnym audycie algorytmicznym.

9.3. Trzy lata — zdolności regionalne

- każdy region posiada przećwiczony plan ciągłości, mapę zależności, centrum operacyjne i sieć lokalnych partnerów;
- każdy operator krytyczny ma paszport odporności, test wyjścia technologicznego i program naprawczy;
- system ostrzegania obejmuje wszystkie grupy ludności, a komunikaty są dostępne w wielu kanałach i formatach;
- rezerwy są rotowane, powiązane z logistyką i produkcją, a ich koszt oraz cel są jawne;
- zamówienia publiczne tworzą krajowe zdolności w cyber, AI, energii, medtech, dronach, łączności i produkcji dual-use.

9.4. Pięć lat — odporna infrastruktura i gospodarka zdolności

- mikrosieci i magazyny energii w kluczowych węzłach, zdolność black-start i zwiększona autonomia obiektów;
- redundantne centra danych, suwerenna warstwa chmurowa i interoperacyjny graf wiedzy państwa;
- krajowe łańcuchy dla wybranych technologii strategicznych oraz zweryfikowani dostawcy sojusznicy;
- cykliczne ćwiczenia całego społeczeństwa bez militaryzacji codziennego życia;
- stały mechanizm finansowania ryzyka: bufory, fundusz awaryjny, ubezpieczenia i obligacje katastroficzne tam, gdzie racjonalne.

9.5. Dziesięć lat — Polska jako europejski węzeł odporności

Docelowo Polska powinna stać się regionalnym centrum produkcji, energii, logistyki, cyberbezpieczeństwa, danych, AI i wiedzy kryzysowej dla Europy Środkowej. Odporność przestaje być kosztem ochronnym, a staje się przewagą gospodarczą: przyciąga inwestycje, obniża ryzyko, zwiększa wiarygodność sojuszniczą i tworzy wysokiej jakości miejsca pracy.

9.6. Pakiet ustaw i standardów

Instrument	Cel
Ustawa o Narodowym Systemie Odporności	mandat, role, 12 funkcji krytycznych, rejestr ryzyk, wskaźniki i audyt
Ustawa o Publicznym Rejestrze Programów Państwowych	jawny cel, właściciel, budżet, termin, KPI/KRI, status i wynik
Ustawa o administracji prezydenckiej i agencjach misyjnych	jedna egzekutywa, kontrakty wynikowe, interoperacyjność i odpowiedzialność
Ustawa o danych i grafie wiedzy państwa	standardy, prawa dostępu, proveniencja, przenoszalność, archiwizacja i RAG
Ustawa o audycie algorytmicznym i prawie do wyjaśnienia	rejestr AI, ocena wpływu, niezależny audyt, odwołanie i człowiek w decyzji
Standard paszportu odporności	obiekty, usługi i operatorzy: robustność, zasoby, odtworzenie, redundancja i zależności
Standard lokalnego procesu decyzyjnego	jedna sprawa, właściciel, SLA, opinia Sejmiku, status, uzasadnienie i odwołanie

ZASADA WDROŻENIA

Najpierw baseline i mały pilotaż. Potem niezależny audyt. Dopiero później skala. Żaden system nie otrzymuje większego mandatu tylko dlatego, że dobrze wygląda na prezentacji.

10. SŁOWNIK SKRÓTÓW

Skrót	Rozwinięcie	Znaczenie w dokumencie
AI	Artificial Intelligence — sztuczna inteligencja	systemy wspierające analizę, prognozowanie, koordynację i obsługę, pod nadzorem człowieka
AHP	Analytic Hierarchy Process	metoda wielokryterialnego porównywania wariantów i priorytetów
C4ISR	Command, Control, Communications, Computers, Intelligence, Surveillance and Reconnaissance	zintegrowane dowodzenie, łączność, informacja, rozpoznanie i obserwacja
CER	Critical Entities Resilience	unijna dyrektywa o odporności podmiotów krytycznych
DPI	Digital Public Infrastructure	publiczna infrastruktura cyfrowa: tożsamość, płatności, rejestry, wymiana danych
DRFI	Disaster Risk Financing and Insurance	finansowanie i ubezpieczenie ryzyka katastroficznego
EWS / MHEWS	Early Warning System / Multi-Hazard Early Warning System	system wczesnego ostrzegania, także przed wieloma rodzajami zagrożeń
FIMI	Foreign Information Manipulation and Interference	zagraniczna manipulacja informacyjna i ingerencja
ICT	Information and Communication Technologies	technologie informacyjno-komunikacyjne
KPI	Key Performance Indicator	miernik osiągniętej zdolności lub wyniku
KRI	Key Risk Indicator	miernik narastającego ryzyka lub podatności
MCDA	Multi-Criteria Decision Analysis	analiza decyzji według wielu kryteriów
NIO	Narodowy Indeks Odporności	publiczny dashboard zdolności, podatności, gotowości i adaptacji
NIS2	Network and Information Security Directive 2	unijne ramy wysokiego poziomu cyberbezpieczeństwa
OODA	Observe–Orient–Decide–Act	pętla obserwuj–orientuj–decyduj–działaj
RACI	Responsible–Accountable–Consulted–Informed	macierz: realizuje–odpowiada–konsultowany–informowany

Skrót	Rozwinięcie	Znaczenie w dokumencie
RAG	Retrieval-Augmented Generation — generowanie wspomagane wyszukiwaniem	AI odpowiada na podstawie znalezionych, zatwierdzonych i cytowanych źródeł
RTO	Recovery Time Objective	docelowy maksymalny czas odtworzenia usługi
SLA	Service Level Agreement	mierzalny standard i czas wykonania usługi
VSM	Viable System Model	Model Systemu Żywowego Stafforda Beera: operacje, koordynacja, kontrola, przyszłość i tożsamość
Zero Trust	model „nigdy nie ufaj domyślnie, zawsze weryfikuj”	tożsamość, najmniejsze uprawnienia, segmentacja i ciągły monitoring

11. ŹRÓDŁA

Źródła podzielono na materiały programowe TechnoSanacji, akty prawne i dokumenty urzędowe oraz literaturę koncepcyjną i standardy. Dostęp do źródeł internetowych: lipiec 2026.

11.1. Materiały programowe TechnoSanacji

- TechnoSanacja.pl — <https://technosanacja.pl/>
- Narodowa Strategia Bezpieczeństwa — <https://technosanacja.pl/strategia/>
- Wizja — <https://technosanacja.pl/wizja/>
- Struktura Multi-Agentowa — <https://technosanacja.pl/struktura/>

11.2. Akty prawne i dokumenty urzędowe

- Ustawa z 5 grudnia 2024 r. o ochronie ludności i obronie cywilnej, Dz.U. 2024 poz. 1907 — <https://eli.gov.pl/eli/DU/2024/1907/ogl>
- Ustawa z 17 kwietnia 2026 r. zmieniająca ustawę o ochronie ludności i obronie cywilnej, Dz.U. 2026 poz. 646 — <https://isap.sejm.gov.pl/isap.nsf/DocDetails.xsp?id=WDU20260000646>
- Program Ochrony Ludności i Obrony Cywilnej na lata 2025–2026 — <https://www.gov.pl/web/olioc/program-ochrony-ludnosci-i-obrony-cywilnej-na-lata-2025-2026>
- NATO, Resilience, civil preparedness and Article 3 — <https://www.nato.int/en/what-we-do/deterrence-and-defence/resilience-civil-preparedness-and-article-3>
- European Commission, EU Preparedness Union Strategy, 2025 — https://commission.europa.eu/topics/preparedness_en

- European Commission, 2025 Strategic Foresight Report — Resilience 2.0 — https://commission.europa.eu/strategy-and-policy/strategic-foresight/2025-strategic-foresight-report_en
- Directive (EU) 2022/2557 on the resilience of critical entities — CER — <https://eur-lex.europa.eu/eli/dir/2022/2557/oj>
- Directive (EU) 2022/2555 on cybersecurity — NIS2 — <https://eur-lex.europa.eu/eli/dir/2022/2555/oj>
- OECD Survey on Drivers of Trust in Public Institutions 2026 — Poland — https://www.oecd.org/en/publications/oecd-survey-on-drivers-of-trust-in-public-institutions-2026-results_c88c8869-en/poland_05dea001-en.html
- European Commission, Poland 2025 Digital Decade Country Report — <https://digital-strategy.ec.europa.eu/en/factpages/poland-2025-digital-decade-country-report>
- Eurostat, 20% of EU enterprises use AI technologies, 2025 data — <https://ec.europa.eu/eurostat/web/products-eurostat-news/w/ddn-20251211-2>

11.3. Literatura i standardy

- M. Mazzucato, The Entrepreneurial State, Demos, 2011 — państwo jako twórca rynków i zdolności innowacyjnych.
- A. C. Karp, N. W. Zamiska, The Technological Republic: Hard Power, Soft Belief, and the Future of the West, 2025 — powrót technologii do misji publicznej i bezpieczeństwa.
- W. R. Ashby, An Introduction to Cybernetics, 1956; R. C. Conant, W. R. Ashby, Every Good Regulator of a System Must Be a Model of That System, 1970.
- S. Beer, Brain of the Firm; The Heart of Enterprise — Model Systemu Żywnotnego i rekursywna organizacja zdolna do przetrwania.
- C. S. Holling, Resilience and Stability of Ecological Systems, 1973; C. Folke, Resilience Thinking, 2010 — odporność, adaptacja i transformacja.
- NIST SP 800-160 Vol. 2 Rev. 1, Developing Cyber-Resilient Systems — anticipate, withstand, recover, adapt.
- ISO 22301 — Business Continuity Management; ISO 22316 — Organizational Resilience; ISO 22320 — Emergency Management.
- UNDRR, Sendai Framework for Disaster Risk Reduction 2015–2030 i wytyczne Multi-Hazard Early Warning Systems.
- OECD, Vulnerability Indicators i Resilient Public Administrations — pomiar podatności i ciągłości działania administracji.
- American Economic Liberties Project, The Other Red Tape, 2021 — prywatni gatekeeperzy, koncentracja rynku i dostęp do rynków.

KONKLUZJA

POLSKA ODPORNA TO POLSKA ZDOLNA DO DZIAŁANIA

Odporność nie jest magazynem strachu. Jest zdolnością wspólnoty do zachowania kierunku. Generacja Z wnosi narzędzia przyszłości. Seniorzy wnoszą pamięć, doświadczenie i odpowiedzialność. Państwo łączy te zasoby w jeden system: dane → wiedza → decyzja → wykonanie → wynik → korekta.

Program budowania odporności społecznej, gospodarczej i technologicznej ma przekształcić Polskę z kraju reagującego na kryzysy w państwo, które rozpoznaje je wcześniej, chroni obywateli bez odbierania im praw, utrzymuje gospodarkę i usługi, rozwija własne technologie i uczy się szybciej niż zmienia się otoczenie.

Polska, 27.07.2026. - Materiał udostępniony na licencji Creative Commons - Uznanie autorstwa

