CYFROWA POLSKA

Warszawa, dnia 4 grudnia 2025 r.

Opinia Związku Cyfrowa Polska do Strategii Cyfryzacji Państwa

Związek Cyfrowa Polska, reprezentujący podmioty sektora cyfrowego i nowoczesnych technologii w Polsce, przedstawia niniejsze stanowisko w ramach konsultacji publicznych projektu **Strategii Cyfryzacji Państwa**, dokumentu o fundamentalnym znaczeniu dla kierunków rozwoju cyfrowego Polski do roku **2035**. Skala wyzwań stojących przed państwem, gospodarką i społeczeństwem - w szczególności w kontekście transformacji usług publicznych, rosnących ryzyk cyberbezpieczeństwa oraz dynamicznego rozwoju sztucznej inteligencji i chmury obliczeniowej - wymaga, aby Strategia była spójnym, ponadsektorowym planem działań, wzmacniającym zarówno konkurencyjność kraju, jak i jego odporność.

Z uznaniem odnotowujemy ambicję dokumentu oraz jego próbę kompleksowego ujęcia kluczowych obszarów cyfryzacji. Jednocześnie, w naszej ocenie, Strategia powinna zostać doprecyzowana tak, by lepiej odzwierciedlała realia rynku technologicznego, zapewniała skuteczne mechanizmy wdrożeniowe oraz jednoznacznie wzmacniała fundamenty nowoczesnego państwa cyfrowego, a także praktyczne podejście do budowania **odporności** i bezpieczeństwa w wymiarze cywilnym i państwowym (dual-use).

Przedstawione uwagi i rekomendacje koncentrują się na elementach niezbędnych dla skutecznej realizacji celów Strategii, w tym w szczególności:

- właściwym rozumieniu **suwerenności cyfrowej** jako swobody wyboru i możliwości zmiany technologii oraz dostawców, a nie izolacji od globalnych rozwiązań;
- usprawnieniu mechanizmów zakupowych i wdrożeniowych w sektorze publicznym (w tym w obszarze chmury obliczeniowej), tak aby administracja mogła szybciej i efektywniej dostarczać usługi cyfrowe;
- wzmocnieniu architektury bezpieczeństwa i odporności (m.in. cyberbezpieczeństwo, odporność na zagrożenia kwantowe, sieci 5G, bezpieczeństwo infrastruktury i danych);
- uporządkowaniu ekosystemu **tożsamości cyfrowej i podpisu elektronicznego**, ze szczególnym uwzględnieniem roli kwalifikowanego podpisu i kwalifikowanej walidacji w ograniczaniu nadużyć i fraudów.

Porozmawiajmy o technologii!

Związek Cyfrowa Polska
ul. Twarda 2, 00-105 Warszawa
e-Doręczenia:
AE:PL-30344-97239-IDAR.I-15

+48 (22) 666 222 46
biuro@cyfrowapolska.org
cyfrowapolska.org

KRS: 0000250359
REGON: 140463214
NIP: 5222802518

Naszym celem jest wsparcie procesu konsultacyjnego poprzez przedstawienie propozycji zmian, które zwiększą wykonalność Strategii, wzmocnią jej spójność z ramami UE oraz przyczynią się do osiągnięcia mierzalnych efektów: poprawy jakości usług publicznych, wzrostu innowacyjności i produktywności gospodarki oraz trwałego podniesienia poziomu bezpieczeństwa i odporności państwa w środowisku cyfrowym.

1. Suwerenność cyfrowa – definicja, rola globalnych dostawców i otwartego rynku

1.1. Szeroka, nieprotekcjonistyczna definicja

Nie zgadzamy się z ujęciem suwerenności cyfrowej, które sugeruje konieczność uniezależniania się od „największych globalnych graczy" poprzez przenoszenie całego stosu technologicznego do Europy.

Proponujemy, aby Strategia:

- definiowała **suwerenność technologiczną** jako zdolność państwa (lub UE) do autonomicznego kształtowania rozwoju w domenie cyfrowej oraz korzystania z technologii zgodnie z własnymi wartościami i interesami, **bez utożsamiania jej z izolacjonizmem** czy zamykaniem się na globalne rozwiązania;
- kładła nacisk na **wolność wyboru, interoperacyjność i przenaszalność danych**, tak, aby administracja i sektor publiczny mogli **swobodnie wybierać, łączyć i zmieniać dostawców** technologii, bez nadmiernego ryzyka vendor lock-in.

To właśnie **wolność technologicznego wyboru** powinna być fundamentem suwerenności cyfrowej.

1.2. Wkład globalnych firm technologicznych w gospodarkę

Strategia wspomina, że *„największe globalne firmy technologiczne (...) muszą uczciwie kontrybuować do rozwoju państwa, również w obszarze podatkowym"*, co może sugerować, że dziś tego nie robią.

Podkreślamy, że:

- **gospodarka cyfrowa w Polsce** to ok. **10% PKB** i ok. **1,5 mln miejsc pracy**
- w relacji CIT/przychód **firmy technologiczne nie odbiegają od innych branż**, a zatrudniając wysoko wykwalifikowanych specjalistów znacząco zasilają budżety (PIT, składki ZUS, VAT przez konsumpcję);
- międzynarodowe firmy technologiczne budują ekosystem lokalnych dostawców i partnerów oraz oferują szerokie programy szkoleniowe (często bezpłatne) dla uczelni, administracji i biznesu;
- dla wielu MŚP **reklama online** i narzędzia chmurowe są kluczowe, by konkurować z większymi markami. Ok. 40% polskich firm wskazuje reklamę online jako narzędzie wyrównujące szanse.

Strategia powinna ten wkład **uczciwie odnotować,** a nie sugerować domyślne nadużycia podatkowe.

1.3. Suwerenność a współpraca międzynarodowa

W obszarze cyberbezpieczeństwa i kryptografii popieramy wzmacnianie **lokalnych kompetencji i rozwiązań,** ale:

- przestrzegamy przed **wąsko pojmowaną, protekcjonistyczną suwerennością,** która może podnosić koszty, obniżać bezpieczeństwo i spowalniać innowacje;
- postulujemy aktywny udział Polski w **europejskich i globalnych procesach standaryzacji kryptografii (w tym postkwantowej),** w ścisłej synchronizacji z inicjatywami Komisji Europejskiej, tak, aby polskie rozwiązania były zgodne z najlepszymi praktykami międzynarodowymi, a nie tworzyły barier regulacyjnych;
- podkreślamy konieczność ścisłej współpracy w ramach **UE i NATO** jako warunku utrzymania przewagi technologicznej wobec zagrożeń ze strony Rosji, państw trzecich i ich stref wpływów.

1.4. Zamówienia publiczne a promowanie „polskich / unijnych" dostawców

Postulaty, aby w postępowaniach zakupowych ICT „promować polskich i unijnych dostawców", w brzmieniu zbyt ogólnym mogą być:

- potencjalnie **sprzeczne z prawem UE** (ryzyko dyskryminacji),
- szkodliwe dla konkurencyjności i jakości rozwiązań.

Rekomendujemy:

- oprzeć się na **Cloud Sovereignty Framework** Komisji Europejskiej – definiując **konkretne wymagania techniczne i bezpieczeństwa**, a nie kryteria terytorialne;
- promować **otwarte standardy, interoperacyjność, przenaszalność danych i multi-cloud,** zamiast sztywnego preferowania określonej narodowości dostawcy.

2. Analiza SWOT – uzupełnienie części „Gospodarka cyfrowa"

W części SWOT „Gospodarka cyfrowa" proponujemy dopisać w **„Słabych stronach":**

h) Bariery związane z brakiem **skonstruowanego mechanizmu generowania popytu** na komercyjne rozwiązania IT przez sektor publiczny.

i) **Skomplikowany proces zamówień publicznych,** ograniczający udział małych i średnich firm IT w przetargach.

To dobrze oddaje realne utrudnienia we współpracy MŚP z administracją.

3. Cyberbezpieczeństwo i infrastruktura krytyczna

3.1. Wzmocnienie systemu cyberbezpieczeństwa

Strategia trafnie zakłada rozwój dojrzałego krajowego systemu cyberbezpieczeństwa, security by design, privacy by design i ethics by design. Postulujemy, aby:

- wzmocnić merytorycznie działania Ministerstwa Cyfryzacji oraz Pełnomocnika ds. Cyberbezpieczeństwa, w tym poprzez **inicjowanie warsztatów z branżą i ekspertami** dla wdrożenia tych zasad w praktyce (standardy, wytyczne, dobre praktyki).

3.2. Odizolowane centra przetwarzania danych

W części dotyczącej **Krajowego Centrum Przetwarzania Danych (KCPD),** obejmującego trzy nowoczesne centra, rekomendujemy doprecyzować, że:

- centra te powinny być **fizycznie i logicznie odizolowane** od innych systemów,
- powinny dysponować własną, odrębną infrastrukturą łączności (m.in. **wydzielone światłowody,** mechanizmy izolacji, w przyszłości **zabezpieczenia kwantowe),**
- ich architektura ma z założenia zapewniać **ciągłość działania w warunkach kryzysowych** (w tym zakłóceń GNSS).

3.3. Odporność na zagrożenia kwantowe

Strategia sygnalizuje rozwój kryptografii kwantowej i postkwantowej. Proponujemy:

- rozszerzyć podejście z poziomu **tylko zaplecza naukowego** na **praktyczne wdrażanie dostępnych komercyjnych rozwiązań** (m.in. zabezpieczenia światłowodowe i satelitarne),
- traktować KCPD i inne krytyczne węzły jako **pilotażowe pola do zastosowania post-quantum/quantum-safe rozwiązań,**
- zorganizować **warsztaty w MC** poświęcone praktycznej odporności na zagrożenia kwantowe, z udziałem operatorów, dostawców technologii i środowiska naukowego.

3.4. Prywatne i dedykowane sieci 5G

Pozytywnie oceniamy uwzględnienie **prywatnych i samorządowych sieci 5G.** Proponujemy, aby Strategia:

- wyraźnie podkreśliła potrzebę **koordynacji** rozwoju takich sieci między sektorami: publicznym, prywatnym i obronnym,
- uwzględniła zarządzanie **widmem radiowym** (spectrum) w czasie pokoju i na wypadek wojny, we współpracy z **UKE oraz WBZC,**

- przewidziała **programy pilotażowe i centra technologiczne 5G,** finansowane m.in. ze środków publicznych, obniżające próg wejścia dla firm i budujące lokalne ekosystemy innowacji (use-cases przemysłowe, miejskie, logistyczne).

3.5. Bezpieczne sieci optyczne – Passive Optical LAN

Dokument nie wspomina o **Passive Optical LAN**, które jest kluczowe dla:

- pełnego cyberbezpieczeństwa wewnątrz budynków,
- niskiego zużycia energii i materiałów (zrównoważony rozwój).

Rekomendujemy dopisanie Passive Optical LAN jako **preferowanej architektury LAN** w nowych i modernizowanych obiektach administracji oraz infrastruktury krytycznej.

3.6. U-Space i regulacje dla „niskiego powietrza"

Strategia nie odnosi się do **U-Space** i regulacji dla **niskiego pułapu przestrzeni powietrznej** (drony, pojazdy bezzałogowe). Proponujemy:

- dodać zapisy dotyczące budowy **ram regulacyjnych i infrastruktury cyfrowej** dla zarządzania ruchem dronów (U-Space),
- powiązać ten obszar z rozwojem **sieci 5G/6G, sensorów, systemów lokalizacji i nadzoru.**

3.7. Zintegrowana świadomość sytuacyjna (sensing)

Postulujemy ujęcie w Strategii potrzeby budowy **zintegrowanego systemu świadomości sytuacyjnej,** opartego na:

- integracji **radarów, sensorów akustycznych, fiber sensingu, a w przyszłości funkcji sensingu sieci 5G/6G,**
- wykorzystaniu sieci telekomunikacyjnych do **korekcji zakłóceń GNSS** (GPS itd.) poprzez rozwiązania typu **Mission Critical Synchronization and Time,**
- wdrożenia tych rozwiązań w sektorach energetyki, broadcastu, służb granicznych, infrastruktury krytycznej.

4. Cyfrowa tożsamość i podpis elektroniczny (rozdział 2.4)

Doceniamy dążenie do budowy **Europejskiego Portfela Tożsamości Cyfrowej (EUDI)** z darmowym kwalifikowanym podpisem elektronicznym dla użytku nieprofesjonalnego oraz ułatwienie składania zdalnych podpisów we wszystkich usługach publicznych.

Zwracamy jednak uwagę, że:

- Strategia przewiduje, że obywatel będzie mógł używać **trzech rodzajów podpisów:** kwalifikowanego, osobistego i zaufanego,
- równolegle istnieje w Polsce **wiele sektorowych „narzędzi podpisowych”,** co generuje złożoność i koszty.

Postulujemy:

1. **Przeprowadzenie kompleksowej inwentaryzacji** istniejących mechanizmów podpisu i uwierzytelniania w administracji.
2. **Skarb Państwa nie powinien utrzymywać trzech równoległych systemów podpisów**, skoro kwalifikowany podpis elektroniczny:
    - **nie ma ograniczeń formalnoprawnych,**
    - jest ważny w usługach publicznych i prywatnych w całej UE,
    - może być udostępniany obywatelowi w EUDI jako narzędzie powszechne.
3. Przy projektowaniu usług publicznych dążyć do tego, by **obywatel nie musiał w ogóle wybierać rodzaju podpisu.** Mechanizmy podpisu powinny być „zaszyte” w procesie, a system sam dobierać właściwe rozwiązanie.
4. Wraz z pełnym wdrożeniem EUDI i powszechnego kwalifikowanego podpisu należy **rozważyć docelowe wycofanie się Państwa z innych rodzajów podpisów elektronicznych,** które mają lokalne czy formalne ograniczenia.

4.1. Walidacja (weryfikacja) podpisów – kluczowa dla cyberbezpieczeństwa

Szczególnie podkreślamy rolę **kwalifikowanych usług walidacji:**

- obecnie tylko **kwalifikowany podpis elektroniczny** jest automatycznie weryfikowany na zgodność z eIDAS w kwalifikowanych usługach walidacji;
- tylko dla kwalifikowanego podpisu można automatycznie potwierdzić **poprawność i status prawny** podpisu (w całej UE);
- ekosystem kwalifikowanego podpisu i kwalifikowanej walidacji to element jednolitego rynku usług zaufania UE.

W warunkach rosnącej liczby fraudów związanych z dokumentami:

- **usługa walidacji staje się krytycznym elementem ochrony cyberbezpieczeństwa,**

- Strategia powinna jednoznacznie wzmacniać i promować **kwalifikowaną walidację jako obowiązkowy element** procesów akceptacji i archiwizacji podpisanych dokumentów w administracji.

5. Chmura obliczeniowa, WIIP, ZUCH, „Cloud First" i ambasady danych

5.1. Obraz rynku chmury i „nierównowaga" sił

Strategia sugeruje, że dominacja komercyjnych usług chmurowych przez globalnych dostawców tworzy „istotną nierównowagę" na niekorzyść pojedynczych instytucji publicznych.

Zwracamy uwagę, że:

- wg danych Gartner mniej niż **15% globalnych wydatków IT** dotyczy chmury, a ok. **70% workloadów IT nadal jest on-premises**. Rynek jest **zróżnicowany,** z silną konkurencją i spadającymi cenami;
- współcześni dostawcy chmury oferują **zaawansowane mechanizmy suwerenności i bezpieczeństwa:**
  - kontrolę lokalizacji danych (rezydencja danych),
  - domyślne szyfrowanie danych w spoczynku, w tranzycie i w użyciu,
  - złożone polityki dostępu i zgodności (RODO itp.),
  - kontrolę usług VPC i mechanizmy zapobiegania eksfiltracji danych.

„Nierównowaga" wynika raczej z **opóźnień technologicznych administracji** i braku nowoczesnych mechanizmów zakupowych niż z samej obecności globalnych dostawców.

5.2. Rządowa chmura vs. chmura publiczna – rola WIIP i SCCO

Strategia akcentuje **Rządową Chmurę Obliczeniową.** Podkreślamy, że:

- już dziś **Wspólna Infrastruktura Informatyczna Państwa (WIIP) oraz Standardy Cyberbezpieczeństwa Chmur Obliczeniowych (SCCO)** umożliwiają sektorowi publicznemu korzystanie z **chmury publicznej,**
- w praktyce globalni dostawcy chmury obsługują **najbardziej wymagające sektory regulowane i krytyczne** (zdrowie, bankowość, sektor obronny, energetyka) na świecie,
- Strategia powinna jasno wskazywać, że **rządowa chmura i chmury komercyjne są komplementarne**, a nie konkurencyjne, i że państwo świadomie korzysta z obu filarów.

Związek Cyfrowa Polska
ul. Twarda 2, 00-105 Warszawa
e-Doręczenia:
AE:PL-30344-97239-IDAR.I-15
+48 (22) 666 222 46
biuro@cyfrowapolska.org
cyfrowapolska.org
KRS: 0000250359
REGON: 140463214
NIP: 5222802518

5.3. Mechanizmy zakupowe – reforma ZUCH

W odpowiedzi na diagnozę wysokich kosztów procesów IT i powolnej implementacji e-usług apelujemy o **stworzenie skutecznego mechanizmu zakupowego** dla rozwiązań chmurowych:

- System Zapewnienia Usług Chmurowych (**ZUCH**) w obecnej formie **nie spełnił swojej roli**, co potwierdziła NIK,
- brak sprawnego mechanizmu zakupowego utrudnia rozwój rynku dostawców IT dla administracji, w tym udział **polskich MŚP,** które mają trudność z przebiciem się przez Prawo zamówień publicznych w każdym urzędzie osobno.

Proponujemy:

1. **Reformę lub zastąpienie ZUCH** mechanizmem wzorowanym na brytyjskim **G-Cloud** – szeregu umów ramowych + marketplace dla usług chmurowych:
    - w UK program G-Cloud umożliwił zawarcie tysięcy kontraktów z ponad 5000 dostawców (ponad 90% z nich to MŚP), o łącznej wartości ok. 11,5 mld funtów, z czego ok. 4 mld trafiło do MŚP;
2. Uproszczenie procedur zakupowych, zwiększenie katalogu usług dostępnych na platformie oraz **dostosowanie mechanizmów rozliczeń** do modeli „pay-as-you-go" i innych modeli chmury publicznej.

Dodatkowo wskazujemy na **potencjalną niespójność** w Strategii między celem b) (umowy ramowe), a celem c) (reforma ZUCH); warto doprecyzować, **którą ścieżką** będą biegły zakupy i dla jakich typów usług.

5.4. Polityka „Cloud First" na poziomie ustawowym

Rekomendujemy przyjęcie **holistycznej polityki „Cloud First":**

- na **poziomie ustawy**, a nie tylko uchwały WIIP,
- jako zasady, że administracja publiczna **w pierwszej kolejności ocenia chmurę publiczną** przy zakupie nowych rozwiązań IT, a dopiero potem rozważa on-prem / chmurę prywatną,
- z warunkiem spełnienia przez dostawcę **wymogów bezpieczeństwa i zgodności z międzynarodowymi standardami.**

Kluczowe elementy polityki „Cloud First", które Strategia powinna uwzględnić:

1. **Definicja „Cloud First"** – obowiązek uzasadnienia decyzji o niewykorzystaniu chmury (w szczególności publicznej).
2. **Multicloud i chmura hybrydowa** – zachęcanie administracji do stosowania strategii multi-cloud/hybrid w celu ograniczenia vendor lock-in i podniesienia niezawodności.

3. **Przenośność danych** – wymaganie oceny rozwiązań pod kątem łatwości migracji i eksportu danych.
4. **Rezydencja i klasyfikacja danych** – zamiast sztywnej lokalizacji danych Strategia powinna:
    - odrzucać wymagania lokalizacji sprzeczne z RODO i regulacjami UE,
    - definiować klarowną **klasyfikację danych** (jakie typy danych mogą i powinny być migrowane do chmury publicznej).
5. **Kryterium środowiskowe** – zrównoważony rozwój środowiska jako obowiązkowe kryterium wyboru dostawców chmury.
6. **Prywatność i bezpieczeństwo** – minimalny zestaw uznanych międzynarodowych standardów i certyfikacji, które dostawcy muszą spełniać.
7. **Model współodpowiedzialności** – wyraźne podkreślenie modelu „shared responsibility" między klientem a dostawcą.
8. **Elastyczne ramy umowne i zamówienia** – możliwość stosowania różnych modeli zakupowych (umowy ramowe, marketplace, zakupy bezpośrednie), zgodnie z potrzebami jednostek.
9. **Walidacja i ocena kosztów** – narzędzia do mierzenia oszczędności i efektów biznesowych migracji do chmury; wskaźniki oparte nie tylko na cenie, ale na **wartości i innowacyjności.**
10. **Otwarte dane i AI/ML** – wykorzystanie chmury jako nośnika dla otwartych zbiorów danych publicznych do badań i trenowania modeli ML/AI.
11. **Ambasadorzy chmury i podnoszenie kompetencji** – wyznaczenie „Cloud Ambassadors" w administracji oraz programy szkoleń dla kadr publicznych.

5.5. Ambasady danych

Strategia zakłada tworzenie **„ambasad danych"** poza granicami kraju. Popieramy kierunek wzmacniania odporności, ale wskazujemy, że:

- samo składowanie danych bez przeniesienia **aplikacji i architektury systemów** może być niewystarczające,
- model pojedynczej fizycznej ambasady danych tworzy **single point of failure** w porównaniu z rozproszonymi architekturami chmurowymi (multi-region, multi-cloud),
- współczesne chmury publiczne zapewniają **replikację w czasie rzeczywistym, automatyczne failover, zaawansowane funkcje bezpieczeństwa** oraz opcje „chmury suwerennej",

- w sytuacji skrajnego kryzysu korzystniejsze może być oparcie się na globalnej infrastrukturze chmury publicznej (nawet kosztem części suwerenności), niż utrzymywanie „pustych" centrów danych tylko na wszelki wypadek.

Rekomendujemy, aby ambasady danych były **tylko jednym z elementów** systemu odporności, a Strategia mocniej akcentowała **rozproszone, chmurowe modele zapewnienia ciągłości działania.**

6. AI, HPC, startupy i technologie dual-use

6.1. Infrastruktura i dane dla AI/HPC, dual-use, multi-cloud

Postulujemy dopisanie w części ogólnej Strategii, że:

- obejmuje ona spójny program rozwoju **infrastruktury i danych dla AI/HPC** (fabryki AI, krajowy broker danych),
- program ten jest projektowany jako **dual-use**, z myślą zarówno o rozwoju rynku, jak i odporności państwa (w tym chmury niejawnej EU/NATO),
- wymogiem operacyjnym jest **multi-cloud i interoperability-by-design**.

6.2. Nowy cel 4.5.3 – pozafinansowe wsparcie startupów i scale-upów

Proponujemy dodać cel **4.5.3 „Pozafinansowe wsparcie startupów i scale-up'ów":**

- wprowadzenie łatwego dostępu (np. w formie „bonów") **do wsparcia merytorycznego i mocy obliczeniowych** dla firm wdrażających AI (nie tylko LLM, lecz szeroko rozumiane modele AI),
- realizacja tego wsparcia przez **fabryki AI oraz ośrodki HPC,**
- **standaryzacja technologii i platform AI,**
- preferencje dla firm rozwijających technologie **dual-use,**
- szeroka adaptacja koncepcji **digital twins** w biznesie, administracji (w tym zarządzanie kryzysowe i obronność), z naciskiem na **interoperacyjność.**

6.3. Regionalny VC dla technologii dual-use

Postulujemy utworzenie **regionalnego podmiotu VC** (obok EBOR i IFC) wspierającego:

- geograficznie rozproszone w Europie Środkowo-Wschodniej firmy wdrażające technologie **dual-use,**
- projekty z zakresu AI, cyberbezpieczeństwa, 5G/6G, kwantowych zabezpieczeń, infrastruktury chmurowej i HPC.

6.4. Niska adopcja chmury i AI – potrzeba przyspieszenia

Według danych KE:

- wykorzystanie chmury przez przedsiębiorstwa w UE to ok. **39% (2023),**
- adopcja AI w biznesie to ok. **13,5% (2024),** przy celach Cyfrowej Dekady (75% do 2030 r.).

Strategia powinna wprost powiązać cele:

- **100% cyfrowej dostępności kluczowych usług publicznych** z koniecznością **przyspieszenia adopcji chmury i AI** zarówno w sektorze publicznym, jak i prywatnym.

7. Rynek cyfrowy, popyt publiczny i MŚP

W nawiązaniu do SWOT i części dot. gospodarki cyfrowej:

- brak **skonstruowanych mechanizmów generowania popytu** na komercyjne rozwiązania IT w sektorze publicznym oraz
- **skomplikowane zamówienia publiczne**

powodują, że polskie MŚP IT mają utrudniony dostęp do projektów rządowych.

Strategia powinna:

- wyraźnie wspierać **mechanizmy agregacji popytu** (platformy typu G-Cloud/ZUCH 2.0),
- promować **modułowe zakupy usług IT**, umożliwiające start-upom i MŚP udział w mniejszych, wyspecjalizowanych komponentach systemów,
- traktować sektor publiczny jako **aktywny generator popytu** na innowacje (m.in. AI, chmura, 5G, cyberbezpieczeństwo), a nie wyłącznie biernego odbiorcę.

Podsumowanie

Związek Cyfrowa Polska:

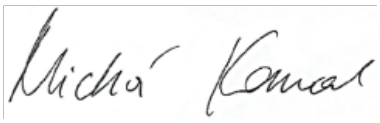
1. **Popiera główny kierunek Strategii**, ale postuluje jej doprecyzowanie w duchu:
    - otwartej, nieprotekcjonistycznej **suwerenności cyfrowej**,
    - intensywnego wykorzystania **chmury (Cloud First),** AI i HPC,

- **multi-cloud, interoperacyjności i standardów międzynarodowych**.

2. Wskazuje na konkretne uzupełnienia:
    - w obszarze **cyfrowej tożsamości i podpisu kwalifikowanego**,
    - **cyberbezpieczeństwa i infrastruktury** (KCPD, 5G, Passive Optical LAN, U-Space, sensing, odporność kwantowa),
    - **chmury** (reforma ZUCH, wzorce G-Cloud, Cloud First, ambasady danych),
    - **AI/HPC i wsparcia startupów** (cel 4.5.3, dual-use, VC regionalny, digital twins),
    - **gospodarki cyfrowej i rynku IT** (dopisy w SWOT, rola MŚP, mechanizmy popytowe).
3. Podkreśla, że **strategiczna współpraca** między państwem, biznesem (w tym globalnymi graczami), nauką i sektorem obronnym jest niezbędna, aby Polska do 2035 r. osiągnęła ambitne cele cyfrowe, pozostała konkurencyjna i bezpieczna.

Z wyrazami szacunku,

Michał Kanownik



Prezes Zarządu

Związek Cyfrowa Polska