Warszawa dnia 9 grudnia 2024 r.

Szanowny Pan
Krzysztof Gawkowski
Wicepremier,
Minister cyfryzacji,
Pełnomocnik Rządu ds. Cyberbezpieczeństwa

Ministerstwo Cyfryzacji
ul. Królewska 27
00-060 Warszawa

Opinia Związku Cyfrowa Polska do Strategii Cyfryzacji Państwa – Projekt do konsultacji społecznych.

Szanowny Panie Premierze,

Projekt Strategii Cyfryzacji Państwa do 2035 roku jest ambitnym dokumentem wyznaczającym cele i kierunki działań w obszarze cyfryzacji Polski. Jednakże jako reprezentant sektora cyfrowego, Związek Cyfrowa Polska dostrzega zarówno pozytywne aspekty strategii, jak i obszary wymagające poprawy, szczególnie w zakresie współpracy z sektorem prywatnym, rozwoju polskich innowacji oraz promowania lokalnych rozwiązań IT.

Strategia Cyfryzacji Państwa jest niezwykle istotnym dokumentem, który stanowi fundament dla przyszłego rozwoju cyfrowego Polski. Z uznaniem przyjmujemy fakt, że została ona opracowana, ponieważ jej realizacja jest kluczowa dla skutecznego sprostania wyzwaniom, jakie niesie ze sobą dynamicznie zmieniający się świat technologii. Dokument ten wyznacza kierunki działań, które mogą przyczynić się do poprawy jakości życia obywateli oraz zwiększenia efektywności funkcjonowania administracji publicznej i gospodarki.

Szczególnie cenne jest uruchomienie konsultacji z rynkiem, co wskazuje na otwartość autorów strategii na dialog z interesariuszami. Ważne jest jednak, aby przed jej ostatecznym uchwaleniem zidentyfikować wszystkie kluczowe strony zainteresowane jej realizacją – zarówno z sektora publicznego, jak i prywatnego. Tylko w ten sposób można zagwarantować, że strategia będzie odpowiadać na potrzeby wszystkich uczestników rynku, uwzględniając zarówno przedsiębiorstwa technologiczne, jak i użytkowników końcowych e-usług.

Jednocześnie pragniemy wskazać na potrzebę przyjęcia bardziej holistycznego podejścia do cyfryzacji. **Strategia nie powinna ograniczać się wyłącznie do cyfryzacji administracji publicznej,** lecz powinna traktować cyfryzację jako proces obejmujący całość współdziałania państwa – **zarówno w sferze publicznej, jak i gospodarczej**. Wzmocnienie potencjału cyfrowego państwa powinno być postrzegane jako kluczowy proces gospodarczy, który wspiera rozwój technologii, innowacyjność oraz konkurencyjność polskiej gospodarki na arenie międzynarodowej.

Niniejsza analiza skupia się na kluczowych wnioskach i spostrzeżeniach dotyczących strategii, podkreślając zarówno jej mocne strony, jak i obszary wymagające dalszej pracy, aby skutecznie realizować wizję cyfrowego rozwoju Polski. Realizując przegląd Strategii Cyfryzacji przedstawionej do opinii przez Ministra Cyfryzacji, w poniższej analizie szczególną uwagę poświęciliśmy wątkom związanym z chmurą, cyberbezpieczeństwem, AI, tożsamością cyfrową, identyfikacją elektroniczną oraz podpisem elektronicznym. Nasze uwagi umieściliśmy w formie tabelarycznej, odnosząc się do poszczególnych punktów strategii. Jednocześnie chcielibyśmy zgłosić kilka spostrzeżeń dotyczących całej strategii, wskazując na potrzebę holistycznego podejścia oraz konieczność uwzględnienia szerokiego kontekstu współdziałania państwa z rynkiem i społeczeństwem w procesie cyfryzacji.

- **Brak współpracy z sektorem prywatnym i rynkiem IT**
  Strategia marginalizuje współpracę z krajowymi przedsiębiorstwami IT oferującymi rozwiązania i usługi na rzecz zarówno podmiotów publicznych jak i przedsiębiorstw. Brakuje mechanizmów partnerstwa publiczno-prywatnego, realizacji wspólnych inicjatyw oraz dialogu z polskimi dostawcami usług cyfrowych. Dominują działania w obszarze administracji publicznej pomijające wpływ na sektor prywatny, co może prowadzić do nieefektywności oraz ograniczania potencjału rozwoju tego sektora.

- **Zwiększenie nacisku strategii na rozpowszechnianie AI**
  Strategia powinna bardziej podkreślać rolę sztucznej inteligencji jako kluczowej technologii transformacji cyfrowej. Konieczne jest wspieranie jej wdrażania w różnych sektorach gospodarki, rozwijanie zarówno podstawowych umiejętności w zakresie AI, jak i zaawansowanych kompetencji technologicznych, a także promowanie odpowiedzialnego wykorzystania generatywnej sztucznej inteligencji. Jednocześnie należy zadbać o zrównoważone, innowacyjne podejście regulacyjne, które będzie sprzyjać dynamicznemu rozwojowi AI przy jednoczesnym minimalizowaniu ryzyk związanych z jej zastosowaniem.

- **Słabe uwzględnienie polskiej gospodarki cyfrowej**
  Gospodarka cyfrowa nie została uznana za kluczowy element strategii, a rozwój cyfryzacji ogranicza się głównie do sektora administracji publicznej. Brakuje narzędzi promujących innowacje i adaptację rozwiązań technologicznych w polskich przedsiębiorstwach.

- **Brak kompleksowych standardów i normalizacji**
  Brakuje jednolitych standardów technicznych, które mogłyby ułatwić interoperacyjność systemów oraz zwiększyć efektywność wdrożeń. Niezbędne jest zaangażowanie w procesy normalizacji na poziomie krajowym, europejskim i międzynarodowym. Nie uwzględniono znaczenia Polskiego Komitetu Normalizacyjnego, komitetów europejskich ETSI I CEN. Tworzenie standardów powierza się urzędnikom, a nie dialogowi tworzonemu w oparciu o otwarte ramy standaryzacji.

- **Problemy z koordynacją działań w administracji**
  Strategia utożsamia cyfryzację z informatyzacją administracji publicznej, co ogranicza jej zasięg i potencjalny wpływ. Brakuje skoordynowanego podejścia do wykorzystywania dostępnych danych i istniejących usług oraz zasobów technologicznych. W szczególności nie uwzględniono potencjału innowacyjnego polskiego sektora prywatnego.

www.zipsee.pl
Związek Cyfrowa Polska
ul. Ogrodowa 58
00-876 Warszawa
Tel. +48 (22) 666 22 46
Fax: +48 (22) 666 22 47
biuro@zipsee.pl
KRS: 0000250359
NIP: 522-280-25-18
REGON 140463214

W realizacji celów strategii brakuje mechanizmów pozwalających na integrację innowacyjnych rozwiązań z sektora prywatnego z systemami publicznymi. Przykładem jest brak platformy integracyjnej umożliwiającej testowanie nowych usług w bezpiecznym środowisku.

- **Niedostateczne przygotowanie do wyzwań w zakresie cyberbezpieczeństwa**
  Brakuje programów edukacyjnych na wszystkich poziomach szkolnictwa oraz spójnych działań zwiększających świadomość w zakresie cyberbezpieczeństwa. Strategia nie przewiduje kompleksowych działań w zakresie edukacji i prewencji.

- **Niewystarczające wsparcie dla małych i średnich przedsiębiorstw (MŚP)**
  Działania wspierające cyfryzację przedsiębiorstw, takie jak program "Cyfrowy start dla biznesu", powinny bardziej promować wykorzystanie polskich rozwiązań IT, wspierać lokalnych dostawców i rozwijać kompetencje cyfrowe w sektorze MŚP.

- **Brak jednolitych zasad dostępu do danych publicznych**
  Strategia nie definiuje jasnych zasad udostępniania danych publicznych, co ogranicza możliwości ich wykorzystania przez sektor prywatny oraz uniemożliwia pełne wykorzystanie potencjału danych rejestrowych.

Cyfrowa tożsamość jest jednym z kluczowych obszarów rozwoju technologicznego w Unii Europejskiej, co znalazło swoje odzwierciedlenie w Strategii Cyfryzacji Państwa. Dokument ten stanowi ważny krok w kierunku budowy nowoczesnych i bezpiecznych rozwiązań, które wspierają rozwój e-usług oraz integrację Polski w ramach jednolitego rynku cyfrowego UE. W obliczu postępującej cyfryzacji, zrozumienie otoczenia strategicznego Unii Europejskiej i dostosowanie działań na poziomie krajowym jest kluczowe dla osiągnięcia spójności i skuteczności strategii.

Polecamy uwadze szczegółową analizę otoczenia strategicznego UE w następujących aspektach:

a) **Cele definiowane przez Komisję Europejską w ramach eIDAS2** – Warto uwzględnić zarówno oficjalne założenia, jak i bardziej realistyczne scenariusze formułowane przez ekspertów z ETSI i European Signature Dialog. To podejście pozwoli na odpowiednie przygotowanie do wdrożeń i adaptacji zaawansowanych rozwiązań.
b) **Strategie realizacji eIDAS2 w kluczowych państwach UE** – Doświadczenia takich krajów jak Niemcy, Francja, Włochy, Hiszpania czy Belgia wskazują, że nadrzędnym celem jest cyberbezpieczeństwo i suwerenność technologiczna. Warto przeanalizować ich podejście, nawet jeśli wiąże się to z koniecznością zaangażowania większych zasobów i wydłużonym czasem realizacji celów.
c) **Plany operacyjne wdrożenia zobowiązań eIDAS** – Ważne jest etapowe podejście, uwzględniające priorytet wpływu wdrażanych usług na obniżenie kosztów oraz ryzyka wynikające z niewłaściwej implementacji. Obszary takie jak identyfikacja, poświadczenia atrybutów oraz usługi zaufania, powinny być analizowane pod kątem ich potencjalnych korzyści dla całych łańcuchów dostaw.

www.zipsee.pl
Związek Cyfrowa Polska
ul. Ogrodowa 58
00-876 Warszawa
Tel. +48 (22) 666 22 46
Fax: +48 (22) 666 22 47
biuro@zipsee.pl
KRS: 0000250359
NIP: 522-280-25-18
REGON 140463214

d) **Równa gra konkurencyjna między sektorami publicznym i prywatnym** – Komisja Europejska kładzie nacisk na zapewnienie „equal playing field" pomiędzy podmiotami publicznymi i prywatnymi oraz utrzymania konkurencyjności, a przez to długofalowego wysokiego tempa rozwoju rynku cybersec. Wyraz tego odzwierciedla nie tylko w deklaracjach medialnych, ale także kluczowych aktach prawnych EU np. Dyrektywie NIS2, Art.24: *„…państwa członkowskie zachęcają podmioty kluczowe i ważne do korzystania z kwalifikowanych usług zaufania…"*.

e) Planowanie działań powinno uwzględniać wyzwania związane z presją polityczną oraz biznesową, które mogą wpływać na rozwój sektora cyfrowego.

Dodatkowo, analiza ryzyk i korzyści współpracy między sektorem publicznym a prywatnym w Polsce wskazuje, że tylko bliska kooperacja w zakresie planowania i realizacji cyfrowego rozwoju kraju pozwala skutecznie adresować zagrożenia. Różnice w ekspozycji na ryzyka (np. polityczne i biznesowe) wymagają synergii w obszarach takich jak cyberbezpieczeństwo, szczególnie w kontekście usług zaufania. Współpraca z sektorem prywatnym, w tym z ekspertami zaangażowanymi w organizacje międzynarodowe (np. European Signature Dialog, ETSI), może znacząco wzmocnić polską pozycję na arenie międzynarodowej.

Polscy dostawcy usług zaufania, działający aktywnie na rynkach globalnych, np. w Azji i Afryce, mają potencjał, by pełnić rolę „cyfrowej Szwajcarii" dzięki neutralności politycznej i wysokim kompetencjom. Włączenie ich wiedzy i doświadczenia w działania państwa może nie tylko wspierać rozwój cyfrowej tożsamości, ale także pozytywnie wpływać na bilans globalnej wymiany handlowej i wzmacniać dyplomację cyfrową Polski.

Z poważaniem
Michał Kanownik

Prezes
Związek Cyfrowa Polska

Szczegółowe uwagi i propozycje zmian.

Lp.	Zapisy Strategii Cyfryzacji Państwa	Uwagi i spostrzeżenia dotyczące zapisów Strategii Cyfryzacji Państwa
1.	**Analiza SWOT** **Infrastruktura (str. 31)** Zagrożenia: • Brak udziału w międzynarodowych projektach wdrażania 5G;	Zwracamy uwagę, że w Polsce zlokalizowane są centra badawczo-rozwojowe (B+R) wiodących firm, które są producentami sprzętu telekomunikacyjnego. To znaczący atut, którym nasz kraj może się szczycić i który warto wyeksponować w Strategii Cyfryzacji Państwa. Dzięki obecności tych centrów, Polska ma bezpośredni udział w realizacji globalnych projektów wdrażania technologii 5G, a polscy specjaliści uczestniczą w najbardziej zaawansowanych procesach innowacji technologicznej, które kształtują przyszłość sektora TMT (Technologie, Media, Telekomunikacja). W tych placówkach, zatrudniających kilkanaście tysięcy inżynierów, prowadzone są prace badawcze, które wykraczają poza lokalny rynek i mają wpływ na rozwój technologii na skalę międzynarodową. Jednocześnie, aby skuteczniej adresować zidentyfikowane w analizie SWOT zagrożenie związane z ograniczonym udziałem Polski w międzynarodowych projektach wdrażania 5G, rekomendujemy uwzględnienie w strategii wyraźnej roli Ministerstwa Obrony Narodowej. MON, jako instytucja odpowiedzialna za bezpieczeństwo narodowe, powinno aktywnie uczestniczyć w rozwijaniu sektora nowoczesnej gospodarki, w tym telekomunikacji, poprzez wspieranie inwestycji w technologie 5G i współpracę międzynarodową. W szczególności, zaangażowanie MON w promocję i wspieranie rozwoju centrów B+R oraz zachęcanie do ulokowania kolejnych międzynarodowych inwestycji w Polsce mogłoby wzmocnić pozycję naszego kraju jako regionalnego lidera w innowacjach telekomunikacyjnych. Eksponowanie roli centrów B+R i zaangażowania polskich specjalistów w projekty 5G ma również znaczenie strategiczne w kontekście budowy pozytywnego wizerunku Polski na arenie międzynarodowej, jako kraju posiadającego wysoko wykwalifikowaną kadrę inżynierską oraz nowoczesną infrastrukturę badawczą. Jest to nie tylko szansa na przyciąganie inwestycji, ale również na promowanie Polski jako ważnego partnera w globalnym łańcuchu wartości w obszarze nowych technologii.

2.	**Cele i czynniki umożliwiające ich realizację (str.38)** **g) Zapewnienie partnerskiej współpracy międzynarodowej**, a także między państwem a biznesem. Gospodarka cyfrowa jest globalna, a istotna część polskiego prawa cyfrowego bierze swój początek w Unii Europejskiej. Tym samym bez dobrej współpracy międzynarodowej rozwój cyfrowego państwa będzie napotykał na istotne przeszkody. Konieczne jest też zapewnienie uczciwych i partnerskich relacji z firmami z sektora ICT. Na szczególną uwagę zasługują relację z największymi globalnymi firmami technologicznymi. Choć funkcjonowanie bez ich produktów często jest niemożliwe, to zarazem muszą one uczciwie kontrybuować do rozwoju państwa, również w obszarze podatkowym.	**Podatek cyfrowy** Zwracamy uwagę, że dyskusje na temat podatku cyfrowego są prowadzone od wielu lat na poziomie OECD i w UE. Dwufilarowy plan OECD dotyczący globalnej reformy podatkowej jest już uzgodniony i ma na celu rozwiązanie problemów podatkowych wynikających z cyfryzacji gospodarki. Podejście Polski do opodatkowania cyfrowego będzie musiało być zgodne z tymi międzynarodowymi procesami. Unilateralne przyjęcie podatku cyfrowego przez Polskę osłabi polską gospodarkę w stosunku do partnerów z UE i OECD. Ramy przyjęte przez OECD, dotyczące międzynarodowej reformy podatkowej, które zostały zatwierdzone przez G20 są lepsze niż podatki od usług cyfrowych (DST), które postrzegamy jako dyskryminujące i szkodliwe. DST tworzą niepewność, mogą prowadzić do odwetowych podwyżek podatków i ostatecznie są przerzucane na konsumentów. DST opierają się na błędnym założeniu, że gospodarka cyfrowa powinna być traktowana inaczej do celów podatkowych. Międzynarodowe traktaty podatkowe zazwyczaj wymagają od firm płacenia większości podatków tam, gdzie tworzone są ich produkty i usługi. Uznajemy potrzebę zmian w międzynarodowym systemie podatkowym i wspieramy wysiłki OECD w celu osiągnięcia rozwiązania opartego na konsensusie.
3.	**1.2 "Kompetencje przyszłości" (Str.47-56)**	Dodać Cel 7. "Cel 7: Rozwinięcie szerokiej bazy umiejętności związanych ze sztuczną inteligencją wśród pracowników. a) Rozbudowanie programów nauczania w szkołach zawodowych i uczelniach wyższych o moduły dotyczące AI i analizy danych b) Wspieranie programów podnoszenia kwalifikacji dla pracowników w celu zdobycia stosowanych umiejętności AI w ich obszarach zawodowych c) Promowanie podstawowej znajomości AI w różnych zawodach poprzez krótkie kursy i certyfikaty."
4.	**1.3 Cyberbezpieczeństwo (str. 57)**	Podkreślenie znaczenia cyberbezpieczeństwa w strategii cyfryzacji jest niezwykle istotne, biorąc pod uwagę dynamiczny wzrost zagrożeń w cyberprzestrzeni oraz ich wpływ na bezpieczeństwo obywateli, funkcjonowanie gospodarki i infrastrukturę krytyczną państwa.

		Szczególnie ważne jest, że strategia uwzględnia rosnącą rolę cyberprzestrzeni jako domeny operacyjnej w wymiarze wojskowym oraz jej znaczenie w kontekście działań hybrydowych i operacji militarnych, zwłaszcza na wschodniej flance NATO. Warto jednak wyraźniej uwypuklić rolę Ministerstwa Obrony Narodowej jako kluczowego partnera w rozwijaniu krajowego systemu cyberbezpieczeństwa. MON, będąc odpowiedzialnym za obronność państwa, odgrywa fundamentalną rolę w przeciwdziałaniu zagrożeniom w cyberprzestrzeni, w tym w budowaniu zdolności ofensywnych i defensywnych w ramach cyberobrony. Synergia między wojskowym a cywilnym wymiarem cyberbezpieczeństwa jest szczególnie ważna, aby zapewnić spójność działań, optymalne wykorzystanie zasobów oraz wzmocnienie zdolności Polski do reagowania na współczesne zagrożenia. Ponadto, dalsze wzmocnienie współpracy między MON a innymi instytucjami państwa, np. poprzez wspólne inicjatywy szkoleniowe i technologiczne, może przyczynić się do skuteczniejszego zwiększania poziomu odporności cyberprzestrzeni Polski. Takie działania powinny być traktowane jako priorytetowe w kontekście zacieśniania współpracy międzynarodowej, w tym w ramach NATO, co pozwoli nie tylko na podniesienie bezpieczeństwa narodowego, ale także na wzmocnienie pozycji Polski jako lidera w obszarze cyberbezpieczeństwa w regionie.
5.	**1.3 Cyberbezpieczeństwo (str. 61 oraz str. 184)** **Cel 3: Krajowa baza technologiczno-przemysłowa w obszarze cyberbezpieczeństwa posiada rozwinięty potencjał i cechuje się wysokim stopniem suwerenności technologicznej.** b) Wykluczenie produktów ICT, rodzajów usług ICT lub konkretnych procesów ICT pochodzących od dostawców wysokiego ryzyka	Wykluczenie HRV za pośrednictwem KSC jest wymienione jako jedno z zadań w ramach części dotyczącej cyberbezpieczeństwa (Cel 3) z terminem realizacji w 2026 roku (strona 184). Rekomendujemy nieodkładanie tak kluczowej kwestii jak bezpieczeństwo infrastruktury krytycznej do końca 2026 roku i wnosimy o modyfikację wskaźnika na - przed końcem **2025 roku.**

	(wykorzystując mechanizm prawny z ustawy KSC); (str.184) Lp. 10 Wdrożenie mechanizmu umożliwiającego wykluczanie dostawców wysokiego ryzyka	
6.	**2.1 "E-usługi publiczne" (Str. 72)**	Cyfrowe usługi publiczne / zamówienia publiczne Rekomendujemy przyjęcie holistycznej polityki 'Cloud First'. Niedawna nowelizacja uchwały WIIP jest krokiem w dobrym kierunku, jednak nie uchwała z uwagi na niższą rangę aktu prawnego nie powinna być stanem docelowym. Przyjęcie polityki 'Cloud First' na poziomie ustawowym może być ważną dźwignią symulującą adopcję chmury obliczeniowej w sektorze publicznym i potencjalnie innych branżach regulowanych, takich jak opieka zdrowotna i usługi finansowe. Dobre praktyki w zakresie wdrażania chmury istnieją w różnych regionach świata, w tym w Australii (Australijska strategia chmury obliczeniowej z 2014 r.), Wielkiej Brytanii (Polityka „Chmura przede wszystkim" z 2013 r.), Stanach Zjednoczonych (Federalna strategia chmury obliczeniowej z 2011 r.; Strategia „Cloud Smart" z 2018 r.). Skuteczna polityka "Cloud First" zalecałaby, aby usługi chmury publicznej były rozważane w pierwszej kolejności w przypadku infrastruktury IT agencji rządowych i miały pierwszeństwo przed rozwiązaniami wyłącznie lokalnymi i chmurą prywatną – pod warunkiem, że dostawcy usług chmurowych spełniają niezbędne wymogi bezpieczeństwa i międzynarodowe standardy. Poniżej przedstawiamy kluczowe obszary, na których należy się skupić, aby polityka „Chmura przede wszystkim" odniosła sukces: • Definiowanie „Cloud First'". Istnieją różne globalne podejścia do definiowania, co „Cloud First" oznacza dla zasad zamówień publicznych w sektorze publicznym. Uważamy, że polityka „Cloud First" powinna wymagać od organizacji publicznych, aby najpierw oceniały chmurę publiczną, zanim rozważą inne rozwiązania przy

		zakupie usług IT, a także jasno wyjaśniały, jeśli zdecydują się nie korzystać z tej opcji. • Multicloud i chmura hybrydowa. W ramach zamówień publicznych organizacje publiczne byłyby zachęcane do rozważenia strategii multicloud i chmury hybrydowej. • Wymagania dotyczące przenośności. Aby wesprzeć realizację strategii multicloud/lub chmury hybrydowej, rozwiązania obejmujące wymagania migracji i przenoszenia danych muszą zostać uwzględnione w ogólnej ocenie w ramach procesów zamówień publicznych przez organizacje publiczne jako jedno z podstawowych kryteriów. Powyższe może również pomóc w zapewnieniu technicznego rozwiązania chroniącego przed ryzykiem nadmiernej koncentracji (tzw. vendor lock-in). • Rezydencja i klasyfikacja danych. Polityka „Cloud First" musi wyraźnie zabraniać zamawiającym nakładania warunków dotyczących lokalizacji danych w określonej lokalizacji i segmentacji danych, ponieważ postanowienia te byłyby sprzeczne z RODO i rozporządzeniem UE w sprawie swobodnego przepływu danych nieosobowych. Jednak polityka „Cloud First" musi definiować jasne i kompleksowe podejście do klasyfikacji danych, które między innymi mogłoby określić, które typy danych i systemów byłyby uważane za gotowe do migracji do chmury publicznej. • Zrównoważony rozwój środowiska. Zrównoważony rozwój środowiska powinien być traktowany jako obowiązkowe kryterium przez organizacje publiczne wybierające swoich dostawców usług chmurowych. • Zasady prywatności i bezpieczeństwa oraz międzynarodowe standardy. Aby zapewnić agencjom sektora publicznego maksymalną ochronę prywatności i bezpieczeństwa w przypadku outsourcingu do chmury, polityka „Cloud First" może definiować zasady wysokiego poziomu i/lub ramy kontroli oparte na ryzyku, które będą kierować ich procesem wyboru dostawców. Jednym ze sposobów osiągnięcia tego celu byłoby ustalenie minimalnego zestawu uznanych na arenie międzynarodowej standardów, zgodnie z którymi dostawcy muszą posiadać certyfikaty, a także obowiązujących dobrowolnych kodeksów postępowania branżowego.

		• Współodpowiedzialność. W środowisku chmurowym klienci i dostawcy usług działają w oparciu o model współodpowiedzialności, który musi być podkreślony w polityce „Cloud First” . • Ramy umowne i model zamówień. Polityka „Cloud First” musi zachować elastyczność w odniesieniu do ram umownych, w ramach których organizacje publiczne dokonywałyby zakupów u dostawców. • Walidacja i ocena kosztów. Aby dodatkowo stymulować przyspieszenie wdrażania chmury w sektorze publicznym i zachęcać organizacje publiczne do wprowadzania innowacji i eksperymentowania z rozwiązaniami chmurowymi, polityka „Cloud First” mogłaby pomóc w opracowaniu narzędzi do ustalania i monitorowania celów oszczędności kosztów wynikających z outsourcingu w chmurze, w tym jasnych wskaźników ilustrujących progres osiągany dzięki chmurze. Wskaźniki te nie powinny opierać się wyłącznie na cenie, ale mogłyby obejmować mechanizm oceny oparty na wartości dla potencjalnych rozwiązań outsourcingowych. • Polityka otwartych danych w celu zwiększenia wykorzystania uczenia maszynowego za pośrednictwem chmury. Ponieważ platformy chmurowe ułatwiły dostęp do technologii sztucznej inteligencji (AI) i uczenia maszynowego (ML), umożliwiając firmom i organizacjom sektora publicznego wprowadzanie innowacji w tej dziedzinie, polityka „Cloud First” może stać się ważną dźwignią promującą dostęp do otwartych zbiorów danych rządowych do celów badawczych i szkoleniowych ML poprzez zasady otwartych danych. • Dalsze promowanie wdrażania chmury i podnoszenie kwalifikacji. W ramach wdrażania polityki „Cloud First” organizacje publiczne mogą wyznaczać „Ambasadorów Chmury” w sektorze publicznym, którzy będą pełnić rolę liderów i promować chmurę. Krytyczne znaczenie ma również zaspokojenie potrzeby podnoszenia kwalifikacji pracowników sektora publicznego, których obciążenia pracą zostaną przekształcone za pomocą technologii chmurowych.
6.	**2.1 "E-usługi publiczne" (Str. 75)**	Dodać punkt f) w Celu 1: "f) Wyznaczenie konkretnego celu w zakresie wdrożenia AI dla każdego departamentu administracji publicznej i głównego obszaru e-usług publicznych."

7.	**2.4 Cyfrowa tożsamość (str.91)** **Diagnoza – jak jest?** „W Polsce od wielu lat z powodzeniem funkcjonuje federacyjny model tożsamości cyfrowej, w którym to użytkownik decyduje, z jakiego środka identyfikacji chce skorzystać w e-usłudze publicznej. Obecnie do dyspozycji użytkowników w ramach publicznego systemu identyfikacji elektronicznej są takie środki jak profil zaufany, profil osobisty (tzw. e-dowód) oraz profil mObywatel. Profil osobisty i profil mObywatel może być wykorzystywany również przez komercyjnych dostawców e-usług publicznych do uwierzytelniania użytkowników. Dodatkowo polscy obywatele i rezydenci mogą także korzystać z tzw. środków bankowych dostępnych w ramach systemu mojeID.„	Głównym czynnikiem umożliwiającym szeroką dostępność środków identyfikacji elektronicznej są rozwiązania bankowe, które pozwoliły szybko wdrożyć efektywne mechanizmy identyfikacji dla wielu uczestników rynku. Państwo nie ułatwia podmiotom prywatnym łatwego i szybkiego podłączenia do systemów identyfikacji elektronicznej, takich jak Profil Osobisty czy mObywatel. Proces integracji jest skomplikowany i czasochłonny. Dostęp do informacji o tożsamości został faktycznie zmonopolizowany poprzez narzucanie warunków korzystania ze środków identyfikacji elektronicznej przez instytucje takie jak KIR i Ministerstwo Cyfryzacji. Administracja realizuje swoje cele, jednak brak ustalonych i transparentnych kryteriów dostępu do mechanizmów zarządzania tożsamością dla sektora biznesowego. Obecny model federacyjny nie monitoruje wystarczająco ryzyk ani nie zbiera danych o incydentach związanych z bezpieczeństwem. W rezultacie brak jest nawet podstawowych statystyk dotyczących oszustw w tym zakresie. Obecny model podłączenia przez węzeł krajowy narusza zasady ustanowione w Unii Europejskiej dotyczące nielinkowalności oraz braku śledzenia użycia środków identyfikacji elektronicznej. Te zasady mają kluczowe znaczenie dla ochrony prywatności użytkowników, jednak ich stosowanie w Polsce jest ograniczone.
8.	**2.4 Cyfrowa tożsamość (str.91)** **Diagnoza – jak jest?** „W powiązaniu z identyfikacją elektroniczną rozwijane są także usługi podpisów elektronicznych. Obecnie na rynku dostępne są publiczne, nieodpłatne rozwiązania: podpis zaufany oraz podpis osobisty, a także zapewniane na warunkach komercyjnych przez dostawców	Administracja publiczna w Polsce nie uznaje w pełni zarówno krajowych, jak i zagranicznych kwalifikowanych podpisów elektronicznych. Ponadto, nie wszystkie formaty podpisów wymagane przepisami unijnymi są obsługiwane, co znacząco ogranicza interoperacyjność i możliwości wykorzystania podpisów w praktyce. Brakuje również ram prawnych i technicznych umożliwiających integrację rozwiązań podpisu elektronicznego z usługami publicznymi. Polska administracja nie wdrożyła międzynarodowych standardów API, które umożliwiłyby sprawną integrację podpisów zdalnych, co utrudnia efektywne wykorzystanie tych narzędzi zarówno w sektorze publicznym, jak i komercyjnym.

	usług zaufania kwalifikowane podpisy elektroniczne.„	Rozwój usług kwalifikowanych jest świadomie ograniczany na rzecz usług administracji publicznej. Przykładem jest brak ustanowienia na poziomie krajowym akceptowalnych przez nadzór sposobów zdalnej rejestracji w krajowych usługach kwalifikowanych, przy jednoczesnym promowaniu rozwiązań zdalnej rejestracji na potrzeby podpisu zaufanego. Takie podejście hamuje innowacje i rozwój rynku usług zaufania. Rozwiązań na rynku związanych z podpisywaniem jest znacznie więcej. Oprócz wymienionych są także „silosowe" mechanizmy np. Podpis profilem PUE (ZUS). Dodatkowo na rynku istnieją technologie podpisu własnoręcznego utrwalonego elektronicznie, które administracja publiczna nie rozpoznaje i nie wspiera, mimo że w wielu procesach znacząco by usprawniły pracę.
9.	**2.4 Cyfrowa tożsamość (str.91)** **Diagnoza – jak jest?** „Powyższe modele obarczone są jednak ograniczeniami, które wpływają negatywnie na powszechność zastosowania środków identyfikacji elektronicznej, podpisów elektronicznych i szerzej e-usług publicznych."	Należy przeprowadzić inwentaryzację mechanizmów identyfikacji elektronicznej i podpisu elektronicznego stosowanych w Polsce oraz uporządkować ich funkcjonowanie w sektorze publicznym i komercyjnym. Przykładem braku spójności jest narzędzie do podpisywania dokumentów dostępne na stronach MC, z którego przedsiębiorcy korzystają często bez pełnej świadomości prawnych skutków użycia podpisu zaufanego w relacjach biznesowych. Obecny duopol MC i KIR w obszarze zarządzania tożsamością generuje bariery dostępu, które przenoszą ciężar kosztowy na mechanizmy identyfikacji, od których zależą usługi zaufania. W efekcie prowadzi to do relatywnie wysokich kosztów jednostkowych tych usług, takich jak kwalifikowany podpis elektroniczny. Kluczowe dla rozwoju usług cyfrowych jest zatem zmniejszenie barier dostępu do identyfikacji, co mogłoby stać się katalizatorem rozwoju całego rynku usług zaufania i e-usług. Analiza obecnego stanu powinna uwzględniać podział marży w łańcuchu dostaw usług cyfrowych. Wskazywanie wysokich kosztów na końcu tego łańcucha bez analizy struktury marż i kluczowych elementów może prowadzić do błędnych wniosków. Optymalizacja

		powinna dotyczyć tych etapów łańcucha, które generują rzeczywiste obciążenia dla konsumentów (podatników), a nie wyłącznie usług końcowych
10.	**2.4 Cyfrowa tożsamość (str.91)** **Diagnoza – jak jest?** „Ze środków identyfikacji elektronicznej korzystać mogą teraz wyłącznie osoby fizyczne, bez rozróżnienia na role czy konteksty, w których uwierzytelniają się online. Nie istnieją rozwiązania, które pozwalałyby na bezpośrednie uwierzytelnianie się spółek, instytucji czy innych podmiotów zbiorowych (osób prawnych), a także osób fizycznych działających jako pełnomocnik czy przedstawiciel osoby prawnej (w tym urzędników). Obecnie, aby doszło do uwierzytelnienia tych podmiotów, konieczne jest dodatkowe potwierdzenie uprawnień do reprezentacji oraz ich weryfikacja, co prowadzi do utrudnień w obsłudze spraw administracyjnych i wydłuża czas oczekiwania na załatwienie sprawy.”	Poruszane zagadnienie jest szczególnie ważne natomiast realizacja powinna być realizowana nie tylko w ujęciu potrzeb administracji publicznej w zakresie identyfikacji przedsiębiorstw a szerokiej analizie funkcjonowania przedsiębiorstw w procesach biznesowych, ich właściwej identyfikacji wobec innych podmiotów i szerokiego udostępniania w sposób bezpieczny informacji, które mają znaczenie dla usprawnienia konkurencyjności rynku.
11.	**2.4 Cyfrowa tożsamość (str.91)** **Diagnoza – jak jest?** „Aktualnie osoba fizyczna, która działa w imieniu i na rzecz osoby prawnej w e-usłudze publicznej musi po uwierzytelnieniu przedstawić dodatkowo informację, a często także stosowny	Należy dać możliwość stworzenia usługi (Q)EEA dedykowanej dla reprezentacji osób fizycznych i prawnych jako atrybutu. Już pierwszy eIDAS wprowadzał możliwość identyfikacji osoby prawnej oraz tworzenia odpowiednich reprezentacji, jednak nic się nie zadziało w kierunku stworzenia takich rozwiązań w PL, nawet mając na wyciągnięcie ręki gotowe fragmenty rozwiązania, np. rejestry KRS, CEiDG.

	dokument potwierdzający jej uprawnienia do reprezentacji, a po stronie urzędu musi nastąpić manualna weryfikacja tego faktu. W sytuacji, w której dana e-usługa publiczna skierowana jest wprost do osób prawnych (np. spółek handlowych), dostawca niejednokrotnie musi albo opierać się o niekonwencjonalne metody potwierdzania tożsamości osób prawnych, albo mierzyć się z koniecznością przeznaczenia dodatkowych zasobów kadrowych do weryfikacji praw do reprezentacji.”	
12.	**2.4 Cyfrowa tożsamość (str.91-92)** **Diagnoza – jak jest?** „Brak dostosowania e-usług publicznych do obsługi osób prawnych jest zauważalny także w aspekcie obsługi podpisów elektronicznych, w sytuacjach, w których wieloosobowa reprezentacja podmiotu wymaga złożenia więcej niż jednego podpisu elektronicznego pod pismem. Nie istnieje bowiem gotowe, nieodpłatne, proste do integracji narzędzie, które umożliwiałoby proste składanie wielu podpisów z poziomu e-usługi publicznej.”	Choć technicznie istnieją narzędzia umożliwiające składanie podpisów wielokrotnych, brakuje jednolitej polityki ich akceptacji. W rezultacie podpisy te są stosowane w różny sposób, przy użyciu różnych technologii, co prowadzi do braku spójności i ogranicza ich praktyczne zastosowanie. Administracja publiczna powinna zapewniać ramy prawne oraz warunki akceptacji, a nie rozwiązania informatyczne. Narzędzi (platform) do budowania określonych procesów biznesowych jest bardzo dużo na rynku. Należy współpracować z rynkiem w tym zakresie a nie dążyć do budowania konkurencyjnych narzędzi do istniejących rozwiązań rynkowych. Przy wyborze strategii rozwiązania postawionego powyżej problemu proponujemy zapoznać się z istniejącymi na rynku rozwiązaniami, które są oparte o europejskie standardy techniczne - mogą one skutecznie realizować wskazany model biznesowy bez konieczności budowy nowych rozwiązań po stronie Państwa. Natomiast należy określić warunki akceptacji podpisów wielokrotnych zarówno pod względem stosowanych formatów jak i zawartości informacyjnej. Wybór rozwiązania powinien być podyktowany przede wszystkim kosztem inwestycji i utrzymania, który obciąża podatnika. Jeśli Państwo chce utrzymać kontrolę nad usługą, powinno wywierać presję na jej długotrwały rozwój, efektywność ekonomiczną inwestycji i jej utrzymania.

		Doświadczenia dojrzałych państw UE wskazują jak ciężkie jest utrzymanie kluczowych parametrów e-usług bez presji (konkurencji rynkowej). W efekcie np. Niemcy podejmują próbę uwolnienia rynkowego usług i dopuszczenia do konkurencji pomiędzy podmiotami publicznymi i komercyjnymi (np. EUDIW) zapewniając sobie kontrolę i ciągłość działania w przypadku wycofania się graczy komercyjnych z rynku.
13.	**2.4 Cyfrowa tożsamość (str.92)** **Diagnoza – jak jest?** „Administracja publiczna mierzy się również z problemem rzetelnej weryfikacji złożonych podpisów elektronicznych z poziomu poszczególnych e-usług publicznych. Konieczne jest umożliwienie poprawnego składania i weryfikowania dokumentów opatrzonych, nie tylko podpisem zaufanym, ale także podpisem osobistym i kwalifikowanym podpisem elektronicznym oraz eliminacja błędów, które pojawiły się na przestrzeni lat rozwoju rynku podpisów elektronicznych.”	Od wielu lat istnieją zaawansowane rozwiązania weryfikacji podpisów i pieczęci z całej UE w tym na poziomie kwalifikowanym. Problemem jest to, że administracja dotychczas skupiła się na rozwoju akceptacji podpisu zaawansowanego. Rozwiązanie problemu powinno być systemowe i realizowane za pomocą usługi zaufania walidacji podpisów elektronicznych spełniającej normy techniczne, a nie w oparciu o budowanie narzędzi nie mających oparcia w normach i legislacji jak czyniono dotychczas. Należy też uwzględnić usługi i rozwiązania dostępne na rynku komercyjnym. Za weryfikację podpisów należy wziąć odpowiedzialność prawną i finansową i to jest istotne zagadnienie w tej materii. Problem ten dostrzegają także inne państwa członkowskie EU, m.in. ze względu na rosnącą wartość aktywów chronionych przez podpisy elektroniczne i zwiększoną liczbę fraudów dotyczących usługi podpisu. W tym kontekście odwołują się do doświadczeń i wiedzy eksperckiej podmiotów kwalifikowanych świadczących od wielu lat usługi kwalifikowanej walidacji, w szczególności z Polski i Luksemburga. Wydaje się, że warto wykorzystać tę wiedzę, skoro zainteresowane są nią inne państwa członkowskie EU.
14.	**2.4 Cyfrowa tożsamość (str.92)** **Diagnoza – jak jest?** „Ponadto, zauważalne są ograniczenia w transgranicznym korzystaniu z e-usług publicznych i to pomimo obowiązującej unijnej zasady wzajemnego uznawania przez państwa członkowskie notyfikowanych środków identyfikacji elektronicznej.”	Problem istnieje również poza Polską i wynika ze stagnacji i zamknięcia usług administracji publicznej dla użytkowników tylko swojego kraju.
15.	**2.4 Cyfrowa tożsamość (str.92)**	Powinien być notyfikowany trzeci środek identyfikacji ‘Profil mObywatel’.

	Diagnoza – jak jest? „Polska posiada dwa notyfikowane środki identyfikacji elektronicznej: profil zaufany i profil osobisty, jednak ich praktyczne użycie w usługach online innych państw członkowskich jest nieznaczne.”	Nie było realizowanej żadnej promocji ani kampanii informacyjnej o możliwości wykorzystania środków identyfikacji transgranicznie. Problem też nie dotyczy tylko Polski, inne kraje UE też nie promują znacząco identyfikacji elektronicznej na poziomie transgranicznym. Dodatkowo strategia powinna uwzlgędniać „poświadczenie obywatela” (Person Identification Data - PID) wystawiane przez administracę publiczną, jako dodatkowy środek identyfikacji, który może stanowić dodatkowe źródło uwierzytelnienia obywatela i może być przechowywane z zachowaniem najwyższych środków bezpieczeństwa w certyfikowanym prywatnym cyfrowym portfelu tożsamości.
16.	**2.4 Cyfrowa tożsamość (str.92)** **Diagnoza – jak jest?** „Jednak warto zauważyć, że do zdecydowanej większości krajowych usług online wymagany jest numer PESEL, co powoduje, że w praktyce akceptowalność notyfikowanych środków z innych państw członkowskich również jest na bardzo niskim poziomie. Komisja Europejska, dostrzegając te systemowe praktyczne problemy we wzajemnym uznawaniu środków identyfikacji elektronicznej, zaproponowała szereg rozwiązań nakierowanych na wzmocnienie bezpieczeństwa i swobody przeprowadzania transakcji elektronicznych w ramach jednolitego rynku cyfrowego, dla których postawą prawną jest rozporządzenie eIDAS 2.0. Przewiduje ono wprowadzenie do końca 2026 r. europejskich portfeli tożsamości cyfrowej, dzięki którym obywatele będą mogli swobodnie korzystać z publicznych i komercyjnych usług online oraz w sposób selektywny i bezpieczny dzielić się	Problem oparcia wszystkich usług publicznych w Polsce o numer PESEL jest znaczący i utrudnia obsługę spraw, które dotyczą osób nieposiadających takiego numeru. Jednocześnie żądanie, aby wszystkie usługi publiczne wymagały środka identyfikacji elektronicznej lub kwalifikowanego certyfikatu zawierającego numer PESEL w sposób nieuprawniony uniemożliwia korzystanie z usług transgranicznych. Jednocześnie należy wskazać, że w wielu procesach odbywających się na piśmie numer PESEL jest częścią deklaratywną wpisywaną w formularz i nie wymaga potwierdzenia. Wprowadzenie europejskich portfeli tożsamości cyfrowej daje możliwość selektywnego udostępniania numeru PESEL jedynie w tych sprawach, które wymagają jego potwierdzenia. Należy wskazać także na problem poruszany przez Głównego Inspektora Danych Osobowych, w związku z posługiwaniem się podpisami elektronicznymi ujawniającymi pesel we wszystkich sprawach służbowych realizowanych przez urzędników oraz osoby działające w imieniu osoby prawnej, gdzie ujawnienie tego numeru jest niepotrzebne procesowo i nadmiarowe w zakresie udostępnianych danych. Należy w tym zakresie stwierdzić, że ograniczenia nie wynikają z technologii i wymagań dla kwalifikowanych certyfikatów a jedynie z polskiej praktyki urzędowej.

	informacjami o sobie. Rozporządzenie zwraca szczególną uwagę na dobrowolność w korzystaniu z tego rozwiązania, a także na jego dostępność oraz ochronę danych osobowych i prywatności użytkowników portfeli.”	
17.	**2.4 Cyfrowa tożsamość (str.92)** **Diagnoza – jak jest?** „Kwalifikowane podpisy elektroniczne mają być dostępne w portfelach za darmo do użytku nieprofesjonalnego, a sam portfel ma stać się środkiem identyfikacji elektronicznej na wysokim poziomie bezpieczeństwa.”	Kluczowe zagadnienie to zdefiniowanie na poziomie UE co oznacza „użytek nieprofesjonalny” Proponuje się następującą definicję „użycia nieprofesjonalnego” *„Użycie odnoszące się do działań lub czynności podejmowanych przez jedną lub więcej osób fizycznych wyłącznie do użytku osobistego, rekreacyjnego lub prywatnego, bez związku z jakimikolwiek celami biznesowymi, komercyjnymi lub zawodowymi. Działania te nie mają na celu generowania dochodu, zysku ani żadnej formy wynagrodzenia i nie są wykonywane w imieniu organizacji, pracodawcy ani klienta.* *Ponadto dokumenty, które mają zostać podpisane, nie są przeznaczone do przekazania organizacji prywatnej, pracodawcy ani osobie prawnej jako Stronie Ufającej.”* Ww. definicja ta została zaproponowana Komisji Europejskiej przez stowarzyszenie czołowych dostawców usług zaufania (w tym sektora publicznego np. DE). Przy budowie strategii wdrożenia EUDIW należy wziąć pod uwagę ryzyka fragmentacji rynku, które mogą zmaterializować się w wyniku oddelegowania do Państw Członkowskich procesu certyfikacji portfeli. W efekcie wymagania bezpieczeństwa dla portfeli, które leżeć będą w gestii Państw Członkowskich mogą wpływać na ich funkcjonalność lub użyteczność. Przykładowo Francja zdecydowała się na ograniczenie funkcjonalności portfela do podstawowych obszarów identyfikacji i poświadczenia atrybutów pozostawiając integrację z usługami zaufania na kolejne etapy wdrażania EUDIW (także ze względu na wysokie ryzyka biznesowe i prawne). Profile zabezpieczeń (w metodologii Common Criteria) będą z dużą dozą prawdopodobieństwa tworzone pod gotowe rozwiązania rynkowe nie dające pewności interoperacyjności transgranicznej. Dopiero kolejne generacje portfeli implementowane na podstawie “Europejskiego Protection Profile” będą wspierać to pryncypium. W tym kontekście należy się spodziewać

		względnej izolacji rynków EU na poziomie usług identyfikacji, a następnie próbie ich harmonizacji na podstawie "lessons learned" lub "siły politycznej" kluczowych graczy EU. Zasadnym wydaje się możliwie wnikliwe przeanalizowanie strategii kluczowych Państw Członkowskich EU, które balansują pomiędzy ochroną własnych interesów, technologii i bezpieczeństwa (cyfrowej suwerenności), a celami zharmonizowanego rynku EU.
18.	**2.4 Cyfrowa tożsamość (str.92)** **Diagnoza – jak jest?** „W celu promowania i przyspieszania rozwoju systemów identyfikacji elektronicznej, a także jednoczesnego dbania o bezpieczeństwo ich licznych użytkowników, konieczne jest ciągłe podnoszenie poziomu cyberbezpieczeństwa środków. Niezbędna jest również dalsza edukacja publiczna w zakresie możliwości realizacji spraw urzędowych online oraz właściwego sposobu korzystania ze środków identyfikacji elektronicznej, tak aby zapobiegać kradzieżom tożsamości, naruszeniom danych osobowych, cyberatakom i innym niebezpiecznym sytuacjom w internecie."	W systemach administracji publicznej coraz częściej dochodzi do naruszeń bezpieczeństwa, takich jak użycie cudzych profili zaufanych i podpisów zaufanych. Państwo nie prowadzi odpowiedniego monitoringu tych środków ani nie zarządza ryzykiem związanym z nowymi formami ataków, co zwiększa zagrożenie dla środków publicznych i bezpieczeństwa całego systemu. Dodatkowym problemem jest konflikt interesów w nadzorze nad cyfrową tożsamością. Minister właściwy w tym zakresie jednocześnie nadzoruje usługi, które sam świadczy, co negatywnie wpływa na rozwój narzędzi oraz na jakość realizowanego nadzoru. Należy w tej materii szeroko rozmawiać z rynkiem komercyjnym.
19.	**2.4 Cyfrowa tożsamość (str.93)** **Cel 1: Osoby prawne mogą w prosty sposób i w krótkim terminie załatwiać sprawy urzędowe online** Co umożliwi realizację celu: a) Utworzenie w ramach publicznego systemu identyfikacji elektronicznej środka identyfikacji elektronicznej dla	Utworzenie środka identyfikacji dla osoby prawnej powinno być związane z europejskim portfelem cyfrowej tożsamości i zintegrowane z nowymi wymaganiami, stworzenie samego środka bez tej integracji może w rzeczywistości być nieużyteczne, ze względu na brak automatyzmu i powiązania z nowoczesnymi usługami. Tworzenie osobnego środka dla osoby fizycznej reprezentującej osobę prawną w rzeczywistości będzie miało zastosowanie tylko dla ograniczonego zakresu spraw, należy wskazać, że reprezentacja w podmiotach związana jest z zakresem uprawnień oraz pełnomocnictwami. Aktualnie rozwijane w ramach tzw. Large Scale Pilots wskazują na konieczność ustanowienia schematów uprawnień i pełnomocnictw dla osób fizycznych reprezentujących osoby prawne. Jednocześnie należy odejść od proponowanych w latach

	osoby prawnej oraz środka identyfikacji elektronicznej dla osoby fizycznej reprezentującej osobę prawną;	wcześniejszych rejestru pełnomocnictw – ponieważ nie może on mieć zastosowania biznesowego – ze względu na nieadekwatność do wymagań obrotu gospodarczego.
20.	**2.4 Cyfrowa tożsamość (str.93)** **Cel 1** b) Skuteczne umocowanie prawne środka identyfikacji elektronicznej dla osoby prawnej oraz środka identyfikacji elektronicznej dla osoby fizycznej repezentującej osobę prawną, aby mógł on służyć do automatycznego uwierzytelniania w usługach publicznych online, bez konieczności każdorazowej manualnej weryfikacji przez urzędnika prawidłowości i aktualności przedstawianych pełnomocnictw lub upoważnień do reprezentacji;	Konieczne jest ustanowienie ram tworzenia potwierdzeń atrybutów użytecznych w procesach osób prawnych, których podstawowym obszarem działania są procesy gospodarcze. Aby funkcjonowały potwierdzenia atrybutów konieczne jest ustanowienie podstawowych identyfikatorów dla firm ale także ustanowienie krajowego rejestru schematów atrybutów, które pozwoli na ustanawianie zasad tworzenia atrybutów potrzebnych biznesowo, które mogłyby powstawać przy zaangażowaniu konkretnych branż (uprawnienia, pełnomocnictwa, potwierdzenia rachunków i sald bankowych, koncesje, uprawnienia zawodowe, referencje, dostępy, kadry, księgowość, finanse, ubezpieczenia). W żadnym wypadku nie należy opierać rozwiązania o centralne repozytoria pełnomocnictw, ponieważ są one nieadekwatne do potrzeb rozwoju rynku i procesów odbywających się w przedsiębiorstwach – np. procesy inwestycyjne, które wymagają poufności związanej z zakresem pełnomocnictw. Rozwój środków identyfikacji dla podmiotów prawnych powinien jednocześnie uwzględniać automatyzm korzystania z rozwiązań w ramach posiadanych przez te organizacje systemów i struktur uprawnień osobowych.
21.	**2.4 Cyfrowa tożsamość (str.93)** **Cel 1** c) Stworzenie nowych lub zmodyfikowanie istniejących usług publicznych tak, aby akceptowały wydane środki identyfikacji elektronicznej dla osób prawnych i środki identyfikacji elektronicznej dla osób fizycznych reprezentujących osoby prawne;	Ze względu na wymaganie braku linkowalności oraz obowiązki związane z poufnością procesu identyfikacji należy zamiast budować usługi węzłowe dla akceptacji identyfikacji skupić się na udostępnieniu publicznych bibliotek i interfejsów oraz mechanizmie skutecznego i szybkiego dołączania stron ufających, tak aby uzyskać szybką akceptację środków.

22.	**2.4 Cyfrowa tożsamość (str.93)** **Cel 1** d) Utworzenie narzędzia zapewniającego możliwość łatwego i wygodnego składania podpisów elektronicznych niezależnie od ich rodzaju i formatu dokumentu w przypadku wieloosobowej reprezentacji osoby prawnej ("wielopodpis");	Tworzenie narzędzia przez podmioty publiczne dla składania podpisów wielokrotnych wydaje się powielaniem rozwiązań dostępnych na rynku, które spełniają wymagania norm technicznych. W Polsce nie opracowano zasad (polityki) tworzenia i akceptacji podpisów elektronicznych, wobec czego nie istnieje skoordynowany model pozwalający na wykorzystanie rozwiązań dostępnych na rynku. Należy się skupić na wypracowaniu krajowych zasad (polityki) i ew. opracowaniu na zasadzie otwartego kodu rozwiązań referencyjnych. Ustanowienie zasad na poziomie krajowym opartych o polskie lub europejskie normy pozwoli także na certyfikowanie rozwiązań zamiast budowy rozwiązania, które może nie sprostać wyzwaniom rynku. Takie narzędzia już istnieją od wielu lat i nie ma potrzeby wydatkować pieniędzy publicznych na ich tworzenie. Należy zacząć współpracować z rynkiem komercyjnym i ekspertami rynkowymi w tym zakresie
23.	**2.4 Cyfrowa tożsamość (str.93)** **Cel 1** e) Udostępnienie europejskiego portfela tożsamości cyfrowej do użytku osób prawnych.	Jest to bardzo ważne rozwiązanie, jednakże zwracamy uwagę, że udostępnienie portfela dla osób prawnych powinno odbywać się w szerokiej współpracy z rynkiem, być oparte o krajowe pilotaże takiego portfela i modeli jego użycia z uwzględnieniem ważnych partnerów rynkowych takich jak banki, ubezpieczenia oraz dostawcy usług zaufania. Znaczące w udostępnieniu portfela jest współpraca ministerstw odpowiedzialnych za rejestry przedsiębiorców, zabezpieczenia społecznego, ZUS i pracy oraz administracji skarbowej. Portfel osób prawnych potrzebuje szerokiej akceptacji w usługach publicznych i prywatnych, możliwość jego zasilania potwierdzeniami atrybutów związanymi z prowadzoną działalnością – np. koncesjami, referencjami, potwierdzeniami bankowymi, poświadczeniami w zakresie zabezpieczenia społecznego i podatków. Jednocześnie wymaga to otwartości i zbudowania krajowych ram pozwalających na zasilanie portfela poświadczeniami pochodzącymi z rynku prywatnego i wykorzystywanych w sektorze prywatnym. Jednocześnie wymaga to łatwości udostępniania portfela firmowego różnym stronom ufającym bez zbędnego bagażu biurokracji.
24.	**2.4 Cyfrowa tożsamość (str.94)** **Cel 2: Podpisy elektroniczne są dostępne i powszechnie używane, a ich weryfikacja jest**	Pierwszym elementem umożliwiającym realizację celu jest odbudowanie współpracy z kwalifikowanym dostawcami usług zaufania, w celu współpracy i wytworzenia krajowych polityk związanych z akceptacją podpisów elektronicznych. Realizowana w poprzednich

	prosta i niezawodna bez względu na format dokumentu i rodzaj podpisu Co umożliwi realizację celu: a) Rozwój narzędzi do podpisywania i weryfikowania dokumentów podpisem zaufanym, podpisem osobistym oraz kwalifikowanym podpisem elektronicznym;	latach polityka Państwa oparta na ignorowaniu rynku i samodzielnej budowie rozwiązań podpisu elektronicznego przez urzędy nie pozwala adresować wyzwań rynku i uniemożliwia rozwój. Cel wymaga najpierw zbudowania krajowej strategii funkcjonowania podpisów elektronicznych, tak aby nie były budowane rozwiązania, które obciążają budżet Państwa natomiast ich zastosowanie jest ograniczone. W związku z tym należy postawić na ustanowienie krajowych wymagań (polityk) tworzenia i akceptacji podpisów elektronicznych, które by powstały wraz z rynkiem dostawców usług podpisu. Rozwój narzędzi do podpisywania i weryfikacji powinien oznaczać wspieranie interoperacyjności rozwiązań opartych o uznane normy techniczne, wspieranie API dostępu do usług podpisu, certyfikację rozwiązań. Konieczne jest wspieranie testów jakościowych w zakresie weryfikacji podpisów elektronicznych i zgodność aplikacji do weryfikacji podpisów z wymaganiami norm. Powinny powstać krajowe rekomendacje w zakresie implementacji rozwiązań podpisu w usługach publicznych, uwzględniające akceptację podpisów kwalifikowanych opartych o certyfikaty pochodzące z innych krajów UE, w tym także rekomendacje w zakresie akceptacji podpisów niezawierających numeru PESEL. Nie jest rolą administracji publicznej budowanie narzędzi tylko monitorowanie poprawności działania rynku. Narzędzia są dostępne od wielu lat na rynku. Należy zbudować mechanizmy zacząć współpracować z rynkiem jak i ekspertami rynkowymi w tym zakresie. Należy podkreślić, że narzędzia te z powodzeniem mogą realizować promowany model biznesowy, w którym użytkownik nie płaci za usługę bezpośrednio (darmowa usługa publiczna dla konsumenta), a poprzez mechanizm subsydiowania przez Państwo, płaci za nią pośrednio w formie podatków (administracja państwową rozlicza się z dostawcą usługi, publicznym lub prywatnym).

25.	**2.4 Cyfrowa tożsamość (str.94)** **Cel 2:** b) Rozpowszechnienie informacji o korzyściach wynikających z korzystania z możliwości składania i weryfikowania podpisów elektronicznych w ich systemach, w tym wspierających realizację e-usług publicznych, poprzez integrację z komponentem węzła podpisu.	Nie istnieje w Polsce „węzeł podpisu" Takie plany były w 2016 roku, ale nigdy nie zostały zrealizowane, na obecnym etapie należy ustalić czy takie rozwiązanie będzie w stanie dostosować się do bieżących wyzwań rynku. Firmy korzystające z podpisów oraz dostawcy usług zaufania od lat postulują o ujednolicenie narzędzi do podpisywania i weryfikacji bazując na sprawdzonych normach i rynkowo komponentach, jednakże państwo finansuje i rozwija rozwiązania, które nie spełniają norm takich jak podpis zaufany. Edukacja w zakresie składania i weryfikacji podpisów jest wielce wskazana, jednakże powinna ona bazować na ustanowionych standardach i jednolitym „guidebook". Poddajemy pod Państwa rozwagę czy strategia powinna doprecyzowywać środki operacyjne jej realizacji, np. "komponent węzła podpisu", jednakże jej opracowanie wymaga współpracy z partnerami rynkowymi – tj. głównymi użytkownikami podpisów oraz dostawcami rozwiązań. W celach brakuje – ustanowienie ram pozwalających na akceptację podpisów niezawierających numeru PESEL, ramy dla podpisów kwalifikowanych stosowanych przez urzędników Zasady tworzenia dokumentów zawierających podpisy elektroniczne w podmiotach publicznych zostały opracowane w latach 2005-2008, od tego czasu nie uległy zmianie. Technologicznie się zmieniło bardzo dużo, a nie zostały wpracowane na poziomie krajowym rekomendacje i nowe standardy, które ułatwiłyby korzystanie z podpisów elektronicznych w usługach publicznych. Wymagany jest przegląd i ustanowienie nowych rekomendacji dla podpisywania dokumentów. Brak powszechności podpisu elektronicznego jest związany z niską dostępnością środka identyfikacji elektronicznej na poziomie wysokim jakim jest profil osobisty oraz brakiem wsparcia krajowych dostawców podpisu w zakresie potwierdzania tożsamości. Celem powinno być utworzenie jednolitych ram potwierdzenia tożsamości dla wszystkich podpisów akceptowanych przez podmioty publiczne. Pomysłem może być także utworzenie ram pozwalających na zdalne odblokowywanie profilu osobistego w dowodzie osobistym bez konieczności chodzenia do urzędu. Taki model pozwoliłby na znaczące ułatwienie w posługiwaniu się profilem osobistym w usługach publicznych.

25.	**2.4 Cyfrowa tożsamość (str.95)** **Cel 3: Środki identyfikacji elektronicznej są bezpieczne i wygodne w użyciu** Co umożliwi realizację celu: a) Budowa oraz wdrożenie modelu szerokiego wykorzystywania warstwy elektronicznej dowodu osobistego oraz certyfikatów elektronicznych związanych z wykonywanym zawodem w systemach teleinformatycznych;	Niezrozumiałe jest powiązanie w jednym punkcie certyfikatu związanego z wykonywanym zawodem z dowodem osobistym. Wydaje się, że powinny to być osobne punkty, ponieważ dowód osobisty co do zasady jest narzędziem związanym z osobą i nie powinno się łączyć codziennego używania dowodu osobistego jako narzędzia w sprawach służbowych. Certyfikat związany z wykonywanym zawodem raczej powinien być elektronicznym potwierdzeniem atrybutu, który może funkcjonować w oparciu o portfele cyfrowej tożsamości. Wykorzystanie kart kryptograficznych (lub innych dodatkowych urządzeń) nie zawsze będzie wygodne w użyciu, stosowanie dowodu osobistego jest niewielkie zarówno w warstwie identyfikacji jak i podpisu. Strategia powinna odblokować dowód, budując szerszy zakres usług z jego wykorzystaniem w warstwie elektronicznej poprzez powszechny dostęp do wykorzystania tego środka w usługach, mechanizm odblokowaniem PIN bez chodzenia do urzędu oraz szersze wykorzystanie potwierdzenia obecności. Cel może zostać zbudowany w oparciu o przygotowane z rynkiem pilotaże, publiczne interfejsy i oraz otwarte oprogramowanie integrujące.
26.	**2.4 Cyfrowa tożsamość (str.95)** **Cel 3:** b) Dodanie do węzła krajowego środka identyfikacji o wysokim poziomie bezpieczeństwa, jakim będzie europejski portfel tożsamości cyfrowej;	Należy zwrócić uwagę, że europejski portfel cyfrowej tożsamości powinien mieć możliwość funkcjonowania bez węzła, w oparciu o bezpośrednią komunikację strony ufającej z portfelem. Ten model związany jest z utworzeniem znaczących usprawnień w zakresie wydawania certyfikatów stronom ufającym i dostępności także polskiej implementacji portfela poza węzłem krajowym. Zbudowanie interfejsu technicznego dla podmiotów publicznych w celu szybkiej adaptacji europejskiego portfela z wykorzystaniem węzła krajowego wymaga uruchomienia mechanizmów chroniących prywatność i uniemożliwiających przez węzeł zbierania danych z realizowanych identyfikacji.
27.	**2.4 Cyfrowa tożsamość (str.95)** **Cel 3** c) Dodanie do węzła krajowego historii użycia środków identyfikacji elektronicznej;	Cel jest sprzeczny z założeniami funkcjonowania środków identyfikacji elektronicznej określonych rozporządzeniem eIDAS i jest sprzeczny z wymaganiami braku śledzenia użycia środka a także braku linkowalności. Historia użycia środka może jedynie być zbierana po stronie użytkownika usługi i nie może być dostępna dla stron trzecich. Środki identyfikacji elektronicznej co do zasady nie służą dostarczeniu wartości dowodowej w

		transakcji a jedynie dostarczeniem informacji, zabezpieczenie informacji dowodowej jest domeną usług zaufania. Realizacja celu w rzeczywistości jest sposobem inwigilacji użycia środka identyfikacji przez obywatela i może naruszać jego zaufanie do środków. Kwestia jest bardzo złożona w kontekście profilowania zachowań użytkownika. Jako dane statystyczne tak, jako historia działań użytkownika niekoniecznie. Należy wziąć pod uwagę Art 5a, p. 14,16. eIDAS 2
28.	**2.4 Cyfrowa tożsamość (str.95)** **Cel 3:** d) Dodanie weryfikacji, czy urządzenie, z którego następuje logowanie do systemów teleinformatycznych przyłączonych do węzła krajowego, jest na liście urządzeń zaufanych użytkownika;	W takich sytuacjach istotne jest odpowiednie wyważenie prywatności i bezpieczeństwa rozwiązań. WK powinien być pośrednikiem – przekaźnikiem danych pomiędzy systemami. To system identyfikacji powinien mieć możliwość weryfikacji z jakich urządzeń korzysta użytkownik itp. Podobnie w bankach, to aplikacja mobilna weryfikuje bezpieczne urządzenia, a nie broker tożsamości.
29.	**2.4 Cyfrowa tożsamość (str.95)** **Cel 3:** e) Realizacja działań edukacyjnych, które wspomogą użytkowników w bezpiecznym korzystaniu ze środków identyfikacji elektronicznej.	Należy wskazać na szeroki mechanizm edukacyjny z zaangażowaniem nie tylko podmiotów publicznych, ale także innych podmiotów korzystających z identyfikacji elektronicznej, w szczególności sektora bankowego, ubezpieczeniowego, telekomunikacyjnego, medycznego i przy zaangażowaniu dostawców usług zaufania.
30.	**2.4 Cyfrowa tożsamość (str.96)** **Cel 4: Obywatele i przedsiębiorcy swobodnie i bezpiecznie korzystają z transgranicznych komercyjnych i publicznych usług**	Utworzenie takiego rejestru jest obowiązkiem wynikającym z regulacji europejskiej, jednakże należy zwrócić uwagę, że procedury wpisania do tego rejestru mogą z powodów biurokratycznych uniemożliwić szybką rejestrację. Należy wprowadzić mechanizm szybkiej, automatycznej ścieżki rejestracji w tym rejestrze, bez konieczności ręcznej weryfikacji i wydawania decyzji w trybie administracyjnym.

	Co umożliwi realizację celu: a) Utworzenie obowiązkowego rejestru podmiotów, które będą chciały świadczyć swoje usługi w oparciu o europejski portfel tożsamości cyfrowej;	
31.	**2.4 Cyfrowa tożsamość (str.96)** **Cel 4:** b) Stworzenie i udostępnienie weryfikacji niektórych danych użytkowników w rejestrach państwowych, aby można było wydawać elektroniczne poświadczenia danych równoważne prawnie z zaświadczeniami tradycyjnymi i uznawane również za granicą;	Należy wskazać, że zgodnie z regulacjami europejskim proces powinien umożliwiać dostęp do szeregu danych z pośrednictwem kwalifikowanych usług elektronicznego poświadczenia atrybutu. Utworzenie tych mechanizmów wymaga szerokiej współpracy z rynkiem dostawców usług zaufania.
32.	**2.4 Cyfrowa tożsamość (str.96)** **Cel 4:** c) Udostępnienie nieodpłatnych kwalifikowanych podpisów elektronicznych w europejskim portfelu tożsamości cyfrowej dla osób fizycznych, przynajmniej do użytku nieprofesjonalnego;	Obowiązkiem portfela jest umożliwienie złożenia kwalifikowanego podpisu elektronicznego do celów nieprofesjonalnych. Zapis może sugerować naruszenie konkurencyjności poprzez szerokie udostępnienie rozwiązania finansowanego z pieniędzy publicznych, które nie będzie respektowało rozwoju usług. Wymaganej jest wprowadzenie ram, które pozwolą na możliwość składania takiego podpisu darmowego ze strony użytkownika, natomiast w sposób, który pozwoli na rozwój usług i rynku. Umożliwienie składania podpisów kwalifikowanych w portfelu powinno iść w parze z szeroką ich akceptacją w usługach publicznych, w tym zakresie jest konieczne określenie krajowej polityki podpisu elektronicznego, ustalenie jej z rynkiem i implementowanie w rozwiązaniach przyjmujących dokumenty w usługach publicznych. Jednocześnie podpisy kwalifikowane w portfelu wymagają, aby publiczne usługi w Polsce akceptowały podpisy składane zdalnie w ustanowionych na poziomie europejskim interfejsach API, bez konieczności instalacji sterowników po stronie urządzeń końcowych.

		Aktualny stan nie pozowała na korzystanie w procesach dokumentowych z podpisów zdalnych w procesach administracji publicznej. Należy w tej materii ściśle współpracować z rynkiem komercyjnym który ma bardzo duże doświadczenia w tej kwestii. Krytyczne jest tu zdefiniowanie na poziomie całej UE co oznacza „ użycie nieprofesjonalne" Definicja takiego działania została wskazana w innym punkcie uwag oraz zaproponowana przez rynek (dostawców komercyjnych i publicznych) Komisji Europejskiej przez stowarzyszenie European Signature Dialog. Poddajemy pod rozwagę Pastwa analizę strategii wdrażania pryncypium "free-signatures" przez czołowe Państwa EU np. DE, FR. Państwa te obecnie otwarcie komunikują zamrożenie lub "kontrolowane przesuniecie" wdrażania darmowych podpisów. Podyktowane jest to analizą ryzyk prawnych (np. złożony problem rozliczalności "zastosowania nieprofesjonalnego" mogący doprowadzić do incydentów niezgodnego z przeznaczeniem użycia darmowego podpisu i w konsekwencji sankcji zdefiniowanych w rozporządzeniu eIDAS lub sprzeciwu ze strony innych Państw Członkowskich o preferowanie lokalnych obywateli lub przedsiębiorców). Z drugiej strony przejęcie przez usługodawców państwowych rynku podpisu generuje ryzyka postępowań antymonopolowych (w tym opierających się na naruszeniu głównych traktatów EU dot. wolnego rynku). W tym kontekście kluczowa jest analiza zaleceń Komisji Europejskiej dotyczącej wdrażania usług zdefiniowanych w rozporządzeniu eIDAS (uzupełniających Akty Implementujące).
33.	**2.5 Chmura obliczeniowa (str.97)** „*Uznajemy, że efektywne i bezpieczne gromadzenie oraz przetwarzanie danych dotyczących obywateli, przedsiębiorców i działania państwa, ze względu przede wszystkim na skalę (wolumen tych danych), jest na dłuższą metę niemożliwe bez wykorzystania chmury obliczeniowej. Istnieje jednak konieczność dostosowania się do sytuacji, w której dominacja rynku komercyjnych usług chmurowych przez*	Z niezrozumieniem przyjmujemy fragment dotyczący 'nierównowagi na niekorzyść instytucji sektora publicznego". Naszym zdaniem, nierównowaga bierze się z zapóźnienia technologicznego administracji publicznej, która ciągle nie wdrożyła nowoczesnych narzędzi takich jak chmura obliczeniowa. Chmura jest podstawą nie tylko dla nowoczesnych i łatwo skalowalnych usług publicznych, ale też i warunkiem koniecznym dla rozwoju sztucznej inteligencji. W kategorii "Cyfrowe usługi publiczne" Polska w 2023 roku zajęła 23. miejsce. Ta kategoria obejmuje m.in. cyfryzację usług administracji publicznej, e-zdrowie i e-learning. Chociaż nie ma tu bezpośredniego odniesienia do adopcji chmury w sektorze publicznym,

	cyfrowych gigantów przekłada się na istotną nierównowagę na niekorzyść instytucji sektora publicznego występujących pojedynczo w relacjach z dużymi dostawcami. Dodatkowo, wykorzystanie technologii chmurowych musi uwzględniać wątki suwerenności danych i ich zabezpieczenia przed zagranicznymi służbami." (Strona 34): *"Silną stroną jest obecność regionów chmurowych największych globalnych dostawców chmury – a zatem ich bezpośrednie zaangażowanie w rozwijanie cyfrowej gospodarki."*	można przypuszczać, że kraje z wyższymi wynikami w tej kategorii częściej wykorzystują chmurę do świadczenia usług publicznych. W 2023 roku Polska zajęła 25. miejsce wśród krajów UE w ogólnym rankingu DESI. Pokazuje to skalę wyzwań, które stoją przed Polską. W odniesieniu do suwerenności danych, chociaż lokalizacja danych może wydawać się prostym rozwiązaniem problemów związanych ze zgodnością i bezpieczeństwem w chmurze obliczeniowej, często jest to błędne podejście. Może stwarzać fałszywe poczucie bezpieczeństwa, a nawet wprowadzać nowe wyzwania. Lekcja z Ukrainy dobitnie pokazała skalę potencjalnych zagrożeń. Zamiast wskazywać na konieczność lokalizacji danych, korzystniej skupić się na: 1. Kontroli rezydencji danych: • Rzeczywista kontrola nad lokalizacją danych: Współcześni dostawcy chmury oferują zaawansowane mechanizmy kontroli rezydencji danych, umożliwiające klientom precyzyjne określenie, gdzie ich dane są przechowywane, nawet do konkretnego regionu lub strefy dostępności. Zapewnia to zgodność z lokalnymi przepisami i regulacjami bez potrzeby ścisłej lokalizacji danych. 2. Domyślnym szyfrowaniu: • Ochrona danych na wszystkich etapach: Wiodący dostawcy chmury oferują domyślne szyfrowanie danych w spoczynku, w użyciu i w tranzycie. Oznacza to, że dane są chronione niezależnie od ich fizycznej lokalizacji, co sprawia, że argument za lokalizacją danych traci na znaczeniu. • Zaawansowane techniki szyfrowania: Dostawcy chmury inwestują znaczne środki w zaawansowane technologie szyfrowania, często przewyższające możliwości pojedynczych organizacji. Zapewnia to solidną ochronę danych przed nieautoryzowanym dostępem i cyberzagrożeniami. 3. Ograniczeniu polityk bezpieczeństwa: • Szczegółowa kontrola dostępu do danych: Ograniczenia polityki bezpieczeństwa danej organizacji pozwalają administratorom zdefiniować szczegółowe mechanizmy kontroli dostępu i polityki bezpieczeństwa dla swojego środowiska

		chmurowego. Gwarantuje to, że tylko upoważniony personel ma dostęp do poufnych danych, niezależnie od miejsca ich przechowywania. • Egzekwowanie zgodności: Te zasady można skonfigurować w celu egzekwowania zgodności z określonymi wymogami prawnymi, takimi jak RODO lub HIPAA, co dodatkowo zmniejsza potrzebę lokalizacji danych. 4. Kontroli usług VPC: • Bezpieczny obwód danych: Kontrola usług VPC tworzy bezpieczne środowisko wokół zasobów chmury, zapobiegając eksfiltracji danych i nieautoryzowanemu dostępowi. Stanowi to dodatkową warstwę bezpieczeństwa, niezależnie od lokalizacji danych. • Zarządzanie danymi i kontrola: Kontrola usług VPC umożliwia organizacjom definiowanie jasnych granic dostępu do danych i ich udostępniania, zapewniając zgodność i zmniejszając ryzyko naruszenia danych. Podsumowując: Lokalizacja danych może być kosztownym i nie efektywnym podejściem do rozwiązywania problemów związanych z zgodnością i bezpieczeństwem. Współcześni dostawcy chmury oferują szereg zabezpieczeń uwzględniających wymogi suwerennościowe, które zapewniają większą elastyczność, skalowalność i bezpieczeństwo bez ograniczeń związanych ze ścisłą lokalizacją danych.
34.	**2.4 Cyfrowa tożsamość (str.96)** **Cel 4:** d) Wprowadzenie procedur jednoznacznego transgranicznego dopasowywania tożsamości, w którym dane identyfikujące osobę są przyporządkowywane do istniejącego konta należącego do tej samej osoby w danej usłudze publicznej;	Cel łączy się z procesem akceptacji wniosków i tożsamości niezawierającej numeru PESEL, w tym zakresie warto ustanowić ramy, które będą miały zastosowanie zarówno dla funkcjonowania krajowego jak i transgranicznego.

35.	**2.4 Cyfrowa tożsamość (str.96)** **Cel 4:** e) Modyfikację krajowych systemów teleinformatycznych, w tym wspierających realizację e-usług publicznych, aby w szerszym zakresie uznawały transgraniczne środki identyfikacji elektronicznej, w tym europejskie portfele tożsamości cyfrowej wydawane przy inne państwa członkowskie oraz ułatwiały korzystanie z usług elektronicznych publicznych użytkownikom z innych państw członkowski (dostępność usługi i wsparcia w innym języku niż polski).	Nie dotyczy to tylko środków identyfikacji, ale także usług kwalifikowanych w tym podpisów elektronicznych. Obecnie poprawnie wydane zagraniczne podpisy kwalifikowane nieposiadające nr PESEL nie są prawidłowo obsługiwane w systemach administracji publicznej. Dodatkowo nawet jeśli podpis kwalifikowany jest teoretycznie możliwy do użycia to stopień skomplikowania jego użycia dla użytkownika jest zdecydowanie większy niż dla innych „państwowych" podpisów elektronicznych. Administracja publiczna de facto nie promuje podpisów kwalifikowanych na rynku które jako jedyne można uznać prawnie transgraniczne
36.	**4.1 "Cyfrowa transformacja przedsiębiorstw" (Str. 138-144)** Cel 6	Dodać Cel 6. "Cel 6: Przyspieszenie wdrażania sztucznej inteligencji wśród MŚP, co umożliwi realizację celu poprzez: a) Zapewnienie odpowiednich wytycznych i zasobów dla MŚP w celu wdrożenia rozwiązań w zakresie sztucznej inteligencji b) Stworzenie programu wdrażania sztucznej inteligencji dla MŚP wzorowanego na singapurskiej inicjatywie Go Digital c) Oferowanie zachęt finansowych lub voucherów dla MŚP w celu uzyskania dostępu do usług AI opartych na chmurze".
37.	**4.2 "Sztuczna inteligencja" (Str. 150)** **Cel 1**	Dodać punkt i) w ramach Celu 1: Nowa wersja: "i) Identyfikacja i wspieranie rozwoju sektorowych zastosowań sztucznej inteligencji w priorytetowych branżach"
38.	**4.2 "Sztuczna inteligencja" (Str. 151)** **Cel 2, punkt d)**	Proponujemy modyfikacjję tego punktu. "d) Wsparcie MŚP we wdrożeniu AI poprzez dostęp do tanich usług doradczych oraz podnoszenie zarówno podstawowych kompetencji w zakresie AI, jak i kompetencji

	"d) Wsparcie MŚP we wdrożeniu AI poprzez dostęp do tanich usług doradczych oraz podnoszenie kompetencji cyfrowych zarówno w przedsiębiorstwach, jak i w sektorze publicznym poprzez wspieranie programów pomagających realizować założenia edukacji ustawicznej, w tym szkolenia zawodowe w zakresie AI;"	cyfrowych powiązanych z AI w przedsiębiorstwach i sektorze publicznym. Powinno to obejmować wspieranie programów, które pomagają wdrażać założenia edukacji ustawicznej, w tym szkolenia zawodowe w zakresie AI i programy podnoszenia kwalifikacji dla pracowników w celu zdobycia stosowanych umiejętności w zakresie AI w ich konkretnych sektorach;"
39.	**4.2 "Sztuczna inteligencja" (Str. 151)** **Cel 2, punkt g):** "g) Wdrożenie i upowszechnienie polskiego dużego modelu językowego w modelu open-source, z typem licencji pozwalającej na jego wykorzystanie na rynku oraz dalsze udoskonalanie oraz dobrej jakości zbioru danych językowych dla polskiego rynku."	Proponujemy modyfikacjję tego punktu. “g) Wdrożenie i upowszechnienie polskiego dużego modelu językowego w modelu open-source, z typem licencji pozwalającej na jego wykorzystanie na rynku oraz dalsze udoskonalanie. Powinien on zostać opracowany w ramach podejścia wielostronnego, z udziałem środowisk akademickich, przemysłu i rządu. Należy upewnić się, że model ten można dostosować do różnych zastosowań sektorowych i że może on być precyzyjnie dostosowany przez przedsiębiorstwa i podmioty sektora publicznego do ich konkretnych potrzeb. Opracowanie wytycznych i programów wsparcia, aby pomóc organizacjom w skutecznym wykorzystaniu i dostosowaniu tego modelu. Zapewnienie, że duże modele językowe mają dostęp do wysokiej jakości zbiorów danych w celu wspierania ich ciągłego doskonalenia i adaptacji. Powinno to obejmować możliwość uczenia się ze źródeł danych online".
40.	**4.2 "Sztuczna inteligencja" (Str. 151)** **Cel 2**	Proponujemy dodać punkt h) do Celu 2: "h) Ustanowienie sektorowych programów przyjmowania AI, koncentrujących się na branżach, w których Polska ma przewagę komparatywną i w których rozwiązania AI są łatwo dostępne, ale ich wdrożenie jest niskie. Programy te powinny obejmować dostosowane wytyczne, zasoby i potencjalnie zachęty finansowe dla firm do wdrażania rozwiązań AI. i) Opracowanie i wdrożenie krajowej strategii umiejętności AI, która obejmuje zarówno podstawowe umiejętności AI, jak i szersze umiejętności związane ze sztuczną inteligencją w różnych sektorach i zawodach. Powinno to obejmować rozszerzenie modułów AI i analizy danych w programach szkolenia zawodowego i wyższych uczelni".

41.	**4.2 "Sztuczna inteligencja" (Str. 151)** **Cel 2**	Proponujmey dodać punkt i) do Celu 2: "i) Promowanie odpowiedzialnego korzystania z generatywnej sztucznej inteligencji w sektorze publicznym i prywatnym. Opracowanie przypadków zastosowania i najlepszych praktyk w celu wykorzystania generatywnej sztucznej inteligencji w kluczowych branżach i usługach publicznych. Ustanowienie krajowej grupy zadaniowej ds. generatywnej sztucznej inteligencji w celu koordynowania wysiłków, dzielenia się wiedzą i rozwiązywania wyzwań związanych z wdrażaniem rozwiązań w zakresie generatywnej sztucznej inteligencji".
42.	**4.2 "Sztuczna inteligencja" (Str. 152)** Cel 3: Zapewnienie odpowiedniej infrastruktury obliczeniowej i zasobów danych ułatwiających rozwój sztucznej inteligencji. Co umożliwi realizację celu: a) Dostarczenie ogólnodostępnej zdecentralizowanej mocy obliczeniowej na potrzeby realizacji projektów sztucznej inteligencji, w tym poprzez w tym poprzez rozszerzanie i promowanie inicjatyw takich jak PLGrid; b) Zwiększenie transparentności procesu dostępu do mocy obliczeniowych, takich jak PLGrid, dla badań naukowych i komercji; c) Ułatwienie przedsiębiorstwom i ośrodkom naukowym dostępu do zbiorów danych do testowania i rozwijania algorytmów AI; d) Określenie standardu wytwarzania danych zasilających systemy sztucznej inteligencji	Proponujemy modyfikację Celu 3: "a) Docenienie roli chmury obliczeniowej i jej wykorzystanie jako kluczowego czynnika umożliwiającego rozwój i wdrażanie sztucznej inteligencji i generatywnej sztucznej inteligencji. Co umożliwi realizację celu: b) Opracowanie krajowej strategii chmury obliczeniowej, która wspiera innowacje w zakresie sztucznej inteligencji, zapewniając, że polityka i inwestycje rządowe ułatwiają dostęp do skalowalnej, bezpiecznej i opłacalnej infrastruktury chmury obliczeniowej na potrzeby rozwoju sztucznej inteligencji. c) Wdrożenie polityk zachęcających do korzystania z usług w chmurze w sektorze publicznym i prywatnym, ze szczególnym uwzględnieniem ich zastosowania w projektach związanych ze sztuczną inteligencją i generatywną sztuczną inteligencją. d) Nawiązanie partnerstw z wiodącymi dostawcami usług w chmurze w celu zapewnienia polskim naukowcom, startupom i przedsiębiorstwom dostępu do najnowocześniejszych platform i narzędzi do rozwoju sztucznej inteligencji. e) Zapewnienie, że procesy zamówień publicznych na projekty AI uwzględniają rozwiązania oparte na chmurze, promując wydajność i skalowalność rządowych inicjatyw AI. f) Wspieranie rozwoju sektorowych zbiorów danych i ram wymiany danych w celu ułatwienia wdrożenia sztucznej inteligencji w priorytetowych branżach. Może to

	zgodnie z interoperacyjnością, zasadami etycznymi oraz prawami człowieka zgodnymi z unijnymi i międzynarodowymi standardami; e) Aktywny udział polskich reprezentantów w pracach nad międzynarodowymi standardami związanymi z AI, ICT, czy też opracowaniem struktur danych.	obejmować tworzenie "instytucji danych" we wrażliwych dziedzinach, takich jak opieka zdrowotna, aby umożliwić godny zaufania dostęp do danych na potrzeby innowacji w zakresie sztucznej inteligencji".
43.	**4.2 "Sztuczna inteligencja" (Str. 152)** Cel 4.	Proponujmey dodanie nowego Celu 4: "Cel 4: Zapewnienie zrównoważonego i sprzyjającego innowacjom otoczenia regulacyjnego dla AI. Co umożliwi realizację celu: a) Dostosowanie polskich przepisów dotyczących AI do ram UE, koncentrując się na harmonizacji w państwach członkowskich w celu zmniejszenia fragmentacji i promowania jednolitego europejskiego ekosystemu AI. b) Wdrożenie podejścia regulacyjnego, które równoważy innowacje z niezbędnymi zabezpieczeniami, unikając nadmiernej regulacji, która mogłaby stłumić rozwój i wdrożenie AI. c) Ustanowienie piaskownic regulacyjnych w kluczowych sektorach, aby umożliwić kontrolowane testowanie i rozwój aplikacji AI, promując innowacje przy jednoczesnym zapewnieniu bezpieczeństwa i względów etycznych. d) Aktywny udział w dyskusjach na szczeblu UE na temat regulacji AI, aby zapewnić reprezentację interesów Polski i potrzeb naszego ekosystemu AI. e) Regularny przegląd i aktualizacja podejść regulacyjnych, aby dotrzymać kroku postępowi technologicznemu, zapewniając, że przepisy pozostają aktualne i nie utrudniają innowacji.“
44.	**4.2 "Sztuczna inteligencja" (Str. 152)** Cel 5.	Proponujmey dodanie nowego Celu 5 "Cel 5: Monitorowanie i mierzenie wdrożenia sztucznej inteligencji w całej gospodarce. a) Prowadzenie regularnych, kompleksowych badań dotyczących wskaźników wdrożenia sztucznej inteligencji w różnych sektorach i w przedsiębiorstwach o różnej wielkości, zgodnie ze standardami OECD dotyczącymi pomiaru wykorzystania ICT.

		b) Opracowanie kluczowych wskaźników wydajności (KPI) do pomiaru wpływu gospodarczego AI i wskaźników wdrożenia w różnych sektorach. c) Publikowanie rocznych raportów na temat stanu wdrożenia sztucznej inteligencji w Polsce, identyfikujących obszary postępu i wyzwań. d) Ustanowienie mechanizmu bieżącej oceny i dostosowywania polityk w zakresie sztucznej inteligencji w oparciu o dane dotyczące wdrożenia i oceny wpływu gospodarczego.“
45.	**4.7 Cyfrowa i zielona transformacjab (str. 178)** **Cel 4: Przyjazny środowisku sektor ICT**	Strategia zachęca operatorów centrów przetwarzania danych “do uwzględnienia dobrych praktyk, o których mowa w europejskim kodeksie postępowania w sprawie efektywności energetycznej centrów danych”. Dodatkowo, Strategia promuje rozwój inteligentnych sieci jako środka do optymalizacji zużycia energii i integracji odnawialnych źródeł energii z systemem energetycznym. Kładzie nacisk na wykorzystanie inteligentnych liczników, analizy danych i sztucznej inteligencji w celu zwiększenia wydajności sieci i skuteczniejszego zarządzania przepływami energii. Brak jest jednak wyraźnej wzmianki o niestabilności i wysokich cenach energii. Koszty energii w Polsce są jednymi z najwyższych w UE i negatywnie wpływają na proces decyzyjny dotyczący lokalizacji centrów przetwarzania danych w kraju, a więc i na dostępność cenową usług cyfrowych. Dodatkowo, zwracamy uwagę, że na skomplikowany proces wpisywania centrów przetwarzania danych na listę obiektów infrastruktury krytycznej w Polsce. Obecnie, centra przetwarzania danych mogą być uznane za infrastrukturę krytyczną, jeśli spełniają określone kryteria, takie jak: • Przetwarzanie danych o znaczeniu krytycznym dla funkcjonowania państwa, gospodarki, lub kluczowych usług publicznych (np. dane dotyczące bezpieczeństwa narodowego, systemów finansowych, energetyki, transportu, służby zdrowia), np. Krajowe Centrum Przetwarzania Danych (KCPD) • Wpływ na funkcjonowanie innych systemów, które mogą zakłócić działanie innych systemów infrastruktury krytycznej, np. centra danych operatorów telekomunikacyjnych.

		• Skala działania: Duże centra danych o znaczącym zasięgu i wpływie na gospodarkę, np. centra danych banków i instytucji finansowych. Uznanie innych centrów przetwarzania danych za krytyczne ma kluczowe znaczenie dla zasilania tych obiektów w energię elektryczną. W Polsce system elektroenergetyczny działa w oparciu o tzw. stopnie zasilania. Są to poziomy ograniczeń w dostarczaniu energii elektrycznej, które wprowadza się w sytuacjach zagrożenia bezpieczeństwa energetycznego, np. gdy zapotrzebowanie na energię przewyższa możliwości jej produkcji. W chwili obecnej, możliwe jest ograniczenia dostępności energii dotyczą dużych odbiorców, którzy mają podpisane umowy na moc umowną równą lub większą niż 300 kW. Ograniczanie dostępności energii elektrycznej może to zakłócić pracę centrów przetwarzania danych, które wymagają stałego, niefluktuującego zasilania w energię elektryczną.