



Strategia Cyfryzacji Państwa

Projekt do konsultacji
społecznych



Tu tworzymy przyszłość

Spis treści

Wstęp	3
Diagnoza	9
Wyzwania i trendy	20
Analiza SWOT	25
Cele i czynniki umożliwiające ich realizację	37
Obszary horyzontalne	39
1.1. Komunikacja elektroniczna	40
1.2. Kompetencje przyszłości	46
1.3. Cyberbezpieczeństwo	57
1.4. Koordynacja cyfrowej transformacji kraju	64
Państwo	72
2.1. E-usługi publiczne	72
2.2. Cyfryzacja procesów administracyjnych i postępowań sądowych	79
2.3. Systemy i rejestry	86
2.4. Cyfrowa tożsamość	90
2.5. Chmura obliczeniowa	97
2.6. Otwarte dane i wymiana danych	102
Ludzie	109
3.1. Bezpieczna przestrzeń cyfrowa	109
3.2. Cyfrowe zdrowie	117
3.3. Branże kreatywne	126
3.4. Cyfrowa akademia	132
Biznes i technologie	136
4.1. Cyfrowa transformacja przedsiębiorstw	138
4.2. Sztuczna inteligencja	145
4.3. Inne technologie przełomowe	152
4.4. Technologie kosmiczne	160
4.5. Finansowanie i wsparcie innowacji	163
4.6. Open source	167
4.7. Cyfrowa i zielona transformacja	170
System wdrażania	181
Finansowanie	189
Słownik	190

Wstęp

Oddajemy w Państwa ręce dokument stanowiący pierwszą w historii Polski kompleksową strategię cyfryzacji kraju. W ostatnich latach cyfryzacja stopniowo i słusznie, przestaje być postrzegana jako odrębny obszar działalności państwa czy sektor gospodarki podobny do wielu innych. Coraz częściej dostrzegany jest jej horyzontalny charakter, oddziałujący na niemal wszystkie obszary funkcjonowania społeczeństwa, państwa i gospodarki. Sfera technologii cyfrowych jest kluczowym polem nasilającej się rywalizacji geopolitycznej, a inwestycje w tej dziedzinie pośrednio (za sprawą technologii podwójnego zastosowania) lub bezpośrednio przekładają się na poziom bezpieczeństwa państwa.

Przed Polską realizacja kluczowych celów na najbliższą dekadę. Cele te muszą uwzględniać między innymi zmieniający się krajobraz bezpieczeństwa państwa i środowiska międzynarodowego, aktualne trendy i wyzwania w obszarze technologii i jej regulacji, a także specyfikę polskiego społeczeństwa i gospodarki. Polskie ambicje i działania wpisują się w kontekst zauważalnego w ostatnich latach wzrostu znaczenia cyfryzacji na liście priorytetów Unii Europejskiej.

Niniejsza strategia stanowi ponadsektorowy dokument strategiczny w dziedzinie informatyzacji państwa, określający nadrzędny cel, jakim jest poprawa jakości życia obywateli poprzez cyfryzację do 2035 r. Jego realizacja możliwa jest tylko dzięki interwencji w szeregu obszarów, wykraczających poza

tradycyjnie definiowany dział administracji – informatyzacja¹. Zaplanowane do realizacji cele obejmują szerokie spektrum zagadnień, począwszy od kwestii horyzontalnych, poprzez płaszczyznę państwa i jego obywateli, na gospodarce i rozwoju technologii kończąc. Takie podejście pozwoliło na stworzenie nowoczesnej, przekrojowej i odpowiadającej na aktualne wyzwania wizji rozwoju cyfrowego, bazującej na aktualnych trendach europejskich i globalnych, wynikającej z diagnozy aktualnego stanu informatyzacji państwa oraz odpowiadającej na sformułowane oczekiwania społeczne.

W początkowych rozdziałach strategii zawarte zostały: diagnoza stanu informatyzacji opracowana na podstawie wyników międzynarodowych wskaźników i badań; wyzwania i trendy, które miały wpływ na określanie kierunków interwencji; analiza silnych i słabych stron, a także szans i zagrożeń dla cyfryzacji Polski oraz ambitna wizja transformacji cyfrowej do 2035 roku wraz prezentacją nadrzędnego celu strategii i uwarunkowań, niezbędnych do jego realizacji.

Dalsza część dokumentu obejmuje obszary horyzontalne, które ze względu na rangę i znaczenie, istotnie wpływają na efektywność działań w innych obszarach i stanowią punkt wyjścia dla transformacji cyfrowej wielu dziedzin życia społeczno-gospodarczego. Do takich obszarów zaliczono: komunikację elektroniczną, kompetencje przyszłości, cyberbezpieczeństwo oraz koordynację transformacji cyfrowej.

Pozostałe cele strategii pogrupowane zostały w 17 obszarach, podzielonych na płaszczyzny: państwo, ludzie oraz biznes i technologie. Cele w ramach płaszczyzny państwo koncentrują się na zwiększeniu i poprawy jakości świadczenia e-usług

¹ Ustawa o działach administracji rządowej z dnia z dnia 11 września 2024 r. Dz.U. z 2024 r. poz. 1370)

publicznych, cyfryzacji procesów administracyjnych i postępowań sądowych, optymalizacji funkcjonowania systemów i rejestrów, rozwoju cyfrowej tożsamości, wykorzystaniu chmury obliczeniowej czy wzmocnieniu otwartości danych i wymiany danych. Cele w ramach płaszczyzny ludzkie dotyczą nie tylko bezpieczeństwa przestrzeni cyfrowej, ale zgodnie ze zdefiniowanymi wyzwaniem i potrzebami, obejmują działania w zakresie cyfrowego zdrowia, rozwoju branż kreatywnych oraz rozwoju akademii i nauki w odniesieniu do sektora cyfrowego. Cele w ramach najbardziej przekrojowej płaszczyzny dotyczącej biznesu i technologii koncentrują się na: zagadnieniach cyfrowej transformacji przedsiębiorstw, w tym działaniach wspierających ten proces oraz dotyczących rozwoju e-usług dla przedsiębiorców; priorytetach w zakresie rozwoju sztucznej inteligencji i innych technologii przełomowych, rozwoju technologii kosmicznych, a także finansowaniu i wsparciu innowacji oraz open source. W tej części również zaadresowane zostały wyzwania i adresujące je cele i działania w obszarach cyfrowej i zielonej transformacji.

Struktura wszystkich obszarów została ujednolicona i zawiera pogłębioną, szczegółową diagnozę (→ jak jest), cele odpowiadające sformułowanym problemom i deficytom (→ jak powinno być) oraz konkretne środki i działania, które pozwolą na osiągnięcie pożądanego stanu (→ co umożliwi realizację celu). W dokumencie znaleźć można również odnotowane wymierne i realne korzyści, jakie obywatel czy przedsiębiorca odczuje po skutecznym wdrożeniu zaplanowanych działań i realizacji zamierzonych celów. Stanowią one przykłady, w jaki sposób

podniesie się jakość życia, tj. nadrzędny cel strategii.

W ostatnim rozdziale opisany został system wdrażania strategii, odnoszący się do sposobu i zasad współpracy podmiotów, których dotyczy proces informatyzacji oraz jej koordynacji, jak również możliwości finansowania działań. Szczególna rola w tym zakresie została przypisana pełnomocnikom ds. informatyzacji oraz Komitetowi do Spraw Cyfryzacji, który zastąpi obecnie działający Komitet Rady Ministrów do Spraw Cyfryzacji², Realizacja ambitnej wizji strategii wymaga wdrożenia spójnych, zharmonizowanych i konsekwentnych działań, przy ścisłej współpracy interesariuszy. Monitorowanie strategii będzie obejmowało mierzenie postępów w realizacji określonych celów, w całym cyklu życia strategii, oraz z wykorzystaniem wskaźników efektywności ujętych w tabeli na końcu dokumentu. Zadanie to powierzone zostanie ministrowi właściwemu do spraw informatyzacji, przy zaangażowaniu pozostałych członków Rady Ministrów. Biorąc pod uwagę zasady zarządzania strategicznego oraz tempo rozwoju technologicznego, planowana jest również regularna ewaluacja i aktualizacja dokumentu.

Wdrażanie strategii nie może się odbywać w oderwaniu od otoczenia strategicznego, zarówno krajowego, jak i unijnego. Sformułowane w strategii cele znajdują odzwierciedlenie i są uszczegółowione w szeregu już obowiązujących dokumentów lub będą spójne z nowymi wersjami dokumentów będących aktualnie w opracowaniu, tj. Strategia Cyberbezpieczeństwa RP (Obecnie obowiązująca na lata 2019-2024, nowy dokument od 2025), Narodowy Plan Szerokopasmowy (aktualizacja w 2026 r.), Program Rozwoju Kompetencji Cyfrowych,

² Na podstawie nowelizacji ustawy o informatyzacji działalności realizujących zadania publiczne z dnia

20 lutego 2024 r. (Dz.U. z 2024 r. poz. 307) (UC

44)

Program Otwierania Danych (Obecnie obowiązujący na lata 2021-27), Polityka Rozwoju Sztucznej Inteligencji (obecnie obowiązująca od 2020 r., planowana aktualizacja w 2025 r.). Niemniej, z uwagi na przekrojowy i ponadsektorowy charakter strategii, zawarte w niej kierunki transformacji należy rozpatrywać w kontekście innych sektorowych dokumentów strategicznych, w tym np. Polityki Cyfrowej Transformacji Edukacji do 2035, Strategii Produktywności do 2030, Polityki Energetycznej Polski do 2040 czy strategii migracyjnej na lata 2025-30. Odnosząc się do europejskich ram strategicznych transformacji cyfrowej, dokument uwzględnia i poszerza cele zarysowane w ramach programu polityki „Droga ku cyfrowej dekadzie do 2030 r.”. Obejmuje ona obszary nieuwzględnione w unijnych celach, ma też bardziej odległy, sięgający 2035 r., horyzont czasowy.

Dokument powstał w Ministerstwie Cyfryzacji we współpracy z innymi urzędami administracji rządowej oraz z uwzględnieniem postulatów interesariuszy społecznych i środowisk biznesowych.

Zastąpi on Program Zintegrowanej Informatyzacji Państwa i będzie stanowić podstawę strategiczną dla wydatkowania europejskich funduszy przeznaczonych na cyfryzację, a tym samym będzie wyznaczał kierunek negocjacji obejmujących nadchodzącą perspektywę finansową.

Wyzwania stojące przed Polską w obszarach konkurencyjności gospodarki, demografii, bezpieczeństwa państwa i jego obywateli czy zdrowia sprawiają, że intensywne inwestowanie w cyfryzację w wielu obszarach przestaje być kwestią wyboru. Staje się koniecznością, bez której pozycja naszego kraju wyraźnie osłabnie. Jeśli jednak cyfryzacji zostanie nadany odpowiadający jej znaczeniu priorytet, zyskają nie tylko poszczególni obywatele i obywatelki – których jakość życia się poprawi – ale i Polska jako całość.



Krzysztof Gawkowski
wicepremier, minister cyfryzacji

Wizja

Nieustannie przyspieszający rozwój technologiczny sprawia, że planowanie działań w obszarze cyfryzacji w perspektywie kolejnej dekady jest zadaniem niezwykle trudnym. Tym trudniejszym, że technologie cyfrowe przenikają każdy niemal aspekt ludzkiego życia, a co za tym idzie – wymagają bliskiej współpracy całej administracji. Ta współpraca jest możliwa, gdy kieruje nią wspólna wizja. Niniejszy dokument zarysowuje taką wizję dla całego państwa, a także działania prowadzące do jej realizacji.

Nasza wizja na 2035 r. koncentruje się na człowieku i tym, jak najskuteczniej poprawić jakość życia obywateli. Za dziesięć lat wizyta w urzędzie będzie czymś wyjątkowym – wszystkie kluczowe usługi będą dostępne przez telefon, z każdego miejsca w kraju. Państwowe systemy same wykryją, że jakieś działanie powinno być podjęte i zaproponują rozwiązanie. Obywatel czy przedsiębiorca nigdy nie będzie musiał dwa razy podawać tych samych danych – urzędy same się nimi wymieniają dzięki pełnej interoperacyjności systemów i rejestrów. Dzięki planowanej poprawie koordynacji między różnymi częściami administracji unikniemy dublowania rozwiązań i niespójności, a tym samym marnowania publicznych pieniędzy.

Intensywny rozwój cyfrowej administracji wymaga inwestycji – w infrastrukturę, w kompetencje urzędników, i w zapewnienie najwyższego poziomu bezpieczeństwa systemom państwowym i tym, które dla państwa mają istotne znaczenie. To szczególnie istotne wobec poważnego pogorszenia międzynarodowej sytuacji

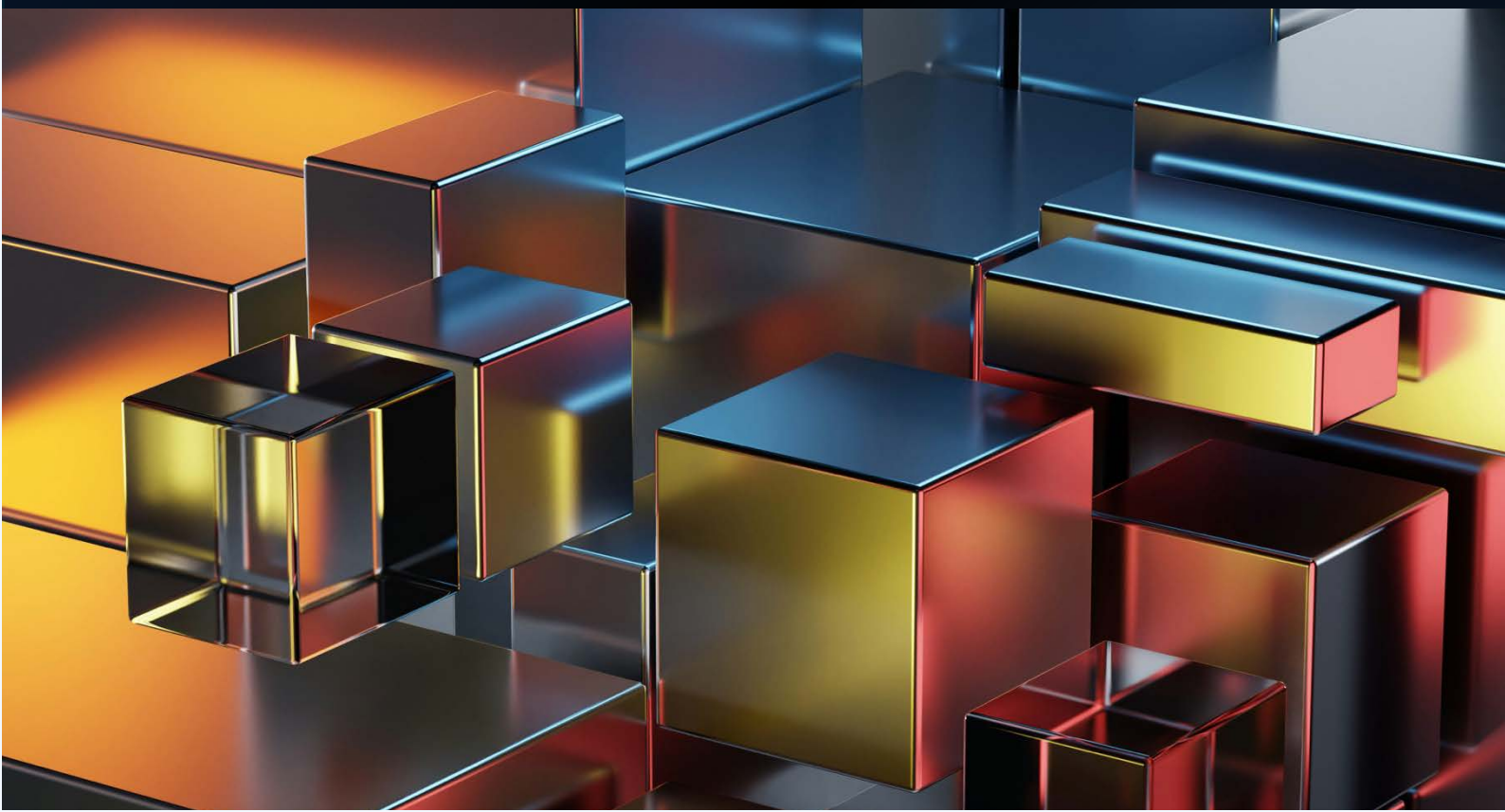
bezpieczeństwa i wzrostu cyberprzestępczości. Ale bezpieczeństwo postrzegamy znacznie szerzej – również w kontekście zdrowia psychicznego czy ochrony obywateli przed szkodliwymi treściami. Dlatego wiemy, że w 2035 r. polscy obywatele muszą mieć nie tylko wysokie kompetencje w korzystaniu z technologii cyfrowych, ale też świadomość, jak korzystać z nich w zdrowy sposób, a czasem – kiedy warto się po prostu odłączyć. Rozwój sfery cyfrowej musi być zrównoważony – z perspektywy psychologicznej, pracowniczej i klimatycznej.

Z tak postrzeganym upowszechnianiem technologii wiąże się ogrom szans na poprawę jakości życia, wzmocnienie polskiej gospodarki i pozycji międzynarodowej. Żeby to się udało, będziemy stymulować adopcję technologii – przede wszystkim sztucznej inteligencji – w administracji i wśród przedsiębiorstw z różnych branż. Zapewnimy lepsze ramy do rozwoju technologii na uczelniach i w gospodarce, będziemy stymulować procesy wymiany wiedzy i kadr między biznesem a nauką. Poprawimy jakość pracy w akademii i rozwiniemy infrastrukturę dla polskiej nauki.

Polska cyfryzacja ma wiele obszarów, z których możemy być dumni, ale nie jesteśmy jeszcze liderem Europy ani tym bardziej świata. Uspójnienie wizji, realizacja przewidzianych w niej działań i znaczne zwiększenie przeznaczanych na cyfryzację środków pozwoli zmienić ten stan rzeczy. Za dziesięć lat Polska będzie prawdziwym cyfrowym liderem.

Wybrane cele na 2035 r.

- Wszystkie kluczowe usługi dostępne są przez aplikację mobilną.
- Państwowe systemy i rejestry są w pełni interoperacyjne.
- 20 mln Polek i Polaków aktywowało portfel tożsamości cyfrowej.
- Płatności elektroniczne są dostępne w całej administracji.
- 50% firm i 80% urzędów wykorzystuje technologie sztucznej inteligencji.
- Wszystkie istotne incydenty cyberbezpieczeństwa są zgłaszane terminowo.
- W każdym zakątku kraju jest zasięg szybkiego internetu.
- 85% Polek i Polaków posiada przynajmniej podstawowe kompetencje cyfrowe.
- Moc obliczeniowa dostępna dla naukowców jest przynajmniej dziesięciokrotnie większa niż dziś.
- Wszystkie placówki ochrony zdrowia wymieniają się dokumentacją medyczną w formie elektronicznej.



Diagnoza



Ministerstwo
Cyfryzacji

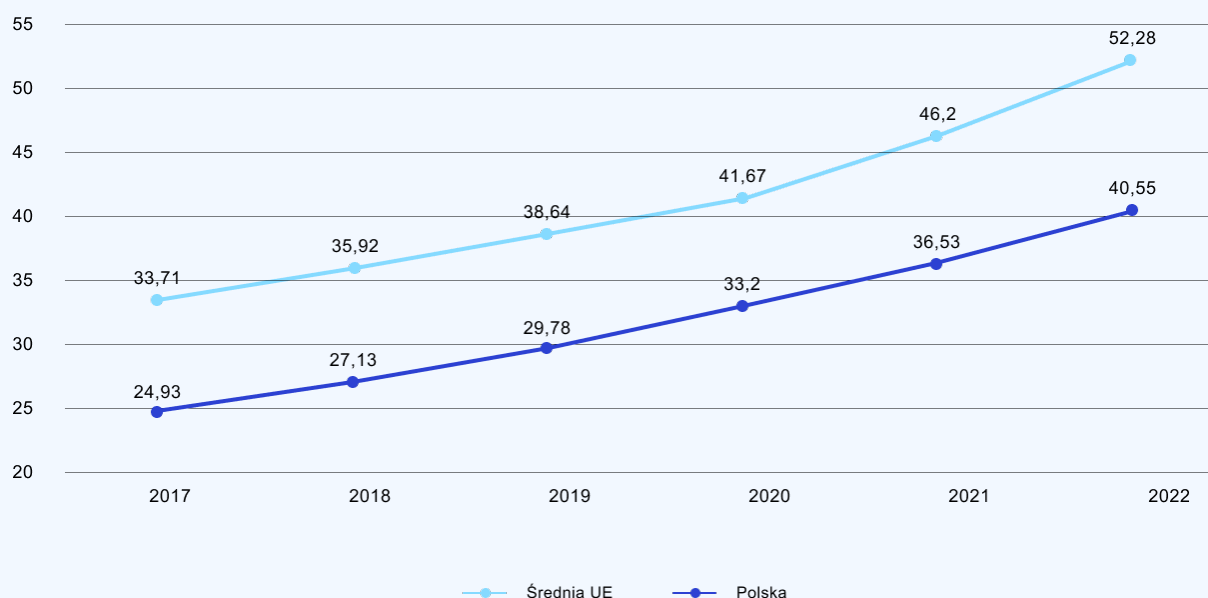
Tu tworzymy przyszłość

Diagnoza

Indeks gospodarki cyfrowej i społeczeństwa cyfrowego (DESI)

Wyniki indeksu DESI (ang. Digital Economy and Society Index) z lat 2017-2022 wskazują, że każdego roku Polska zajmowała 24. miejsce wśród 27 państw członkowskich UE. Luka cyfrowa jest widoczna we wszystkich badanych obszarach, takich jak kompetencje cyfrowe, telekomunikacja, transformacja cyfrowa przedsiębiorstw i cyfrowe usługi publiczne. Jednak postęp w dziedzinie cyfryzacji staje się coraz bardziej widoczny. **Na przestrzeni 5 lat Polska poprawiła swój wynik z 24,9 pkt. w 2017 r. do 40,6 pkt. w 2022 r., tym samym będąc w czołówce państw najintensywniej nadrabiających dystans do liderów.** Zgodnie z analizą Polskiego Instytutu Ekonomicznego³ punktacja Polski w indeksie DESI w tym okresie wzrosła z 52,1% do 58,3% punktacji lidera.

DESI 2017-2022



Wykres 1 DESI 2017-2022, źródło: opracowanie własne na podstawie raportów DESI 2017-2022

Od 2023 r., zgodnie z założeniami unijnego programu polityki „Droga ku cyfrowej dekadzie” do 2030 r., DESI jest włączany do sprawozdania na temat stanu realizacji programu⁴. Komisja Europejska zrezygnowała z tworzenia rankingu państw członkowskich,

3 <https://pie.net.pl/polska-wsrod-unijnych-liderow-postepu-w-rozwoju-cyfryzacji/>

4 <https://digital-strategy.ec.europa.eu/en/library/digital-decade-2024-country-reports>

udostępniając jednocześnie narzędzie⁵ do porównywania wyników państw względem siebie i średniej UE w poszczególnych wskaźnikach.

W 2024 r. Polska osiągnęła wyższe wyniki niż średnia UE w 6 na 36 wskaźników: łączność szerokopasmowa, zasięg stałych sieci o bardzo dużej przepływności, zasięg technologii „światłowod do lokalu” (FTTP, ang. Fibre to the premises), chmura, wstępnie wypełnione formularze oraz dostęp do e-dokumentacji medycznej.

W ostatnim sprawozdaniu z realizacji programu polityki „Droga ku cyfrowej dekadzie” do 2030 r.⁶ odnotowano znaczne postępy w obszarze łączności gigabitowej i cyfryzacji MŚP. W przypadku wskaźnika zasięgu sieci o bardzo wysokiej przepustowości **Polska z wynikiem 81,1% objętych gospodarstw domowych przekracza średnią UE (wynoszącą 78,8%)** i jest na dobrej drodze do osiągnięcia 100% zasięgu do 2030 r. Chociaż wskaźniki KPI dotyczące cyfryzacji przedsiębiorstw są poniżej unijnej średniej, **tempo wzrostu poziomu cyfryzacji polskich MŚP pomiędzy rokiem 2021 a 2023 było 5 razy wyższe niż w UE.** Według raportu o stanie cyfrowej dekady, polskie MŚP mają duży potencjał wzrostowy; autorzy zwracają też uwagę, że 14 proc. z nich angażuje się w handel internetowy. Utrzymywanie się wyzwań w obszarze transformacji cyfrowej przedsiębiorstw spowodowane jest niedoborem specjalistów, wysokimi kosztami i brakiem odpowiedniego finansowania. Ponadto w sprawozdaniu zauważono, że **znaczne środki zostaną przeznaczone na poprawę jakości telekomunikacji, zwiększenie wykorzystania technologii cyfrowych przez przedsiębiorstwa oraz rozwój cyfrowych usług publicznych**, które powinny poprawić konkurencyjność polskiej gospodarki i zwiększyć wykorzystanie technologii cyfrowych przez całe społeczeństwo. Komisja Europejska odnotowała również polskie deklaracje w zakresie inwestycji w produkcję półprzewodników i uczestnictwa w projektach budowy komputerów kwantowych.

Mimo pozytywnych trendów, Polska osiąga wciąż niezadowalające wyniki w zakresie umiejętności cyfrowych i wdrażania zaawansowanych technologii. Rezultat Polski we wskaźniku *co najmniej podstawowe umiejętności cyfrowe* wynosi 44%, co jest poniżej średniej UE, równej 55,6%. Polska osiąga wartość poniżej średniej UE także we wskaźnikach takich jak *ponadpodstawowe umiejętności cyfrowe* (PL 20%, UE 27%) i *co najmniej podstawowe umiejętności tworzenia treści cyfrowych* (PL 60%, UE 68%).

Analiza krajowych planów działania przeprowadzona przez Komisję Europejską wskazuje, że w obecnym scenariuszu wspólne wysiłki nie osiągają poziomu ambicji UE. Zidentyfikowane luki obejmują potrzebę dodatkowych inwestycji, zarówno na szczeblu unijnym, jak i krajowym w wielu obszarach. Polska powinna rozważyć dostosowanie do celów UE poziomu ambicji celów dotyczących liczby specjalistów ICT oraz wykorzystania sztucznej inteligencji i analizy danych przez przedsiębiorstwa.

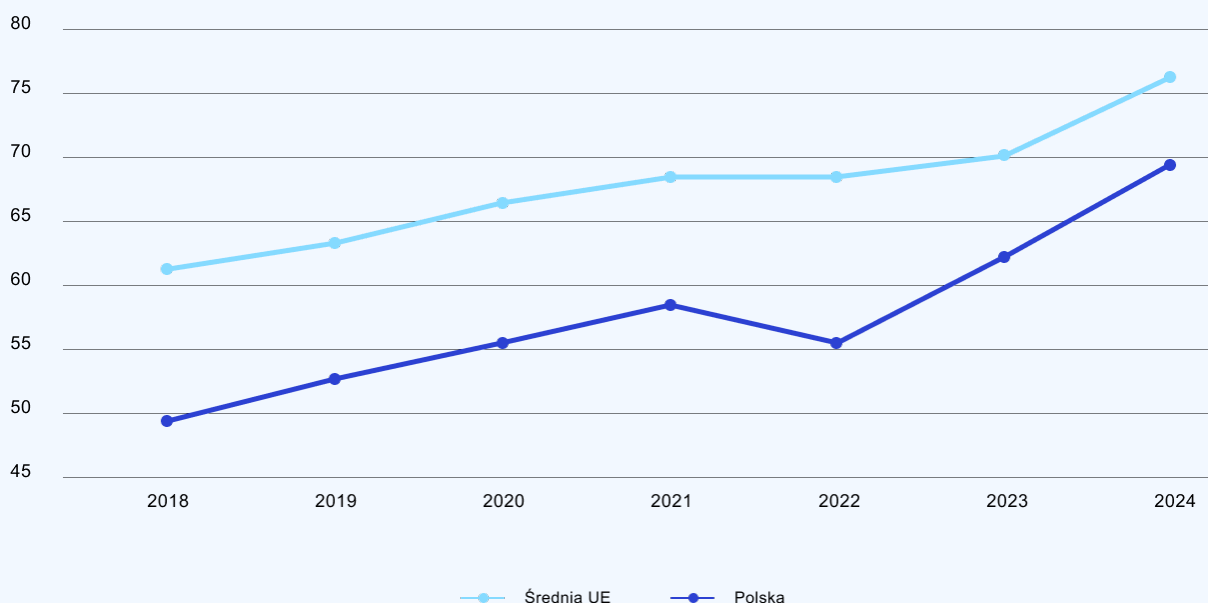
5 https://digital-decade-desi.digital-strategy.ec.europa.eu/datasets/desi/charts/desi-indicators?period=desi_2024&indicator=desi_dsk_dcc_bab&breakdown=ind_total&unit=pc_ind&country=AT,BE,BG,HR,CY,CZ,DK,EE,EU,FI,FR,DE,EL,HU,IE,IT,LV,LT,LU,MT,NL,PL,PT,RO,SK

6 <https://digital-strategy.ec.europa.eu/en/factpages/poland-2024-digital-decade-country-report>

eGovernment Benchmark

eGovernment Benchmark⁷ jest corocznym badaniem, monitorującym wdrożenie cyfrowych usług publicznych we wszystkich krajach europejskich. W 2024 r. polski wynik wzrósł do 69 pkt.; zbliżone osiągają państwa takie jak Czechy, Bułgaria, Grecja czy Chorwacja. Dystans do średniej UE wynosi 7 pkt. Ponadto, **Polska znalazła się w gronie państw, które osiągnęły największy wzrost wyników ogólnych w ujęciu czteroletnim: +14 pkt**

eGovernment Benchmark 2018-2024



Wykres 2 Wyniki eGovernment Benchmark 2018-2024, źródło: opracowanie własne na podstawie wyników badania 2018-2024

Wskaźniki e-administracji zogniskowane są wokół czterech wymiarów: orientowanie na użytkownika, przejrzystość świadczenia usług, kluczowe czynniki wspomagające oraz usługi transgraniczne. W raporcie z 2024 r. Polska odnotowuje wyniki na poziomie średniej europejskiej lub powyżej niej w zakresie 5 wskaźników: *wsparcie użytkownika, przejrzystość projektowania usług, eID, eDokumenty i predefiniowane formularze*. **Największy wzrost odnotowano we wskaźnikach *przejrzystość danych osobowych, e-dokumenty, oraz poczta cyfrowa***. Stosunkowo najwyższe wyniki Polska osiągnęła w całej kategorii dot. usług transgranicznych, a także we wskaźnikach *przejrzystość świadczenia usług elektronicznych, przejrzystość danych osobowych oraz poczta elektroniczna*. Pod względem klasyfikacji w odniesieniu do tzw. zdarzeń życiowych, największy wzrost punktowy w 2024 r. odnotowano w zdarzeniu życiowym *sprawiedliwość* (wzrost o 27 pkt) i *zdrowie* (wzrost o 12 p.p.). Mimo rosnących wyników Polski w każdym zdarzeniu życiowym, nadal pozostaje przestrzeń do poprawy, szczególnie w zdarzeniach życiowych *sprawiedliwość* i *transport*, gdzie wyniki są poniżej średniej unijnej.

⁷ <https://digital-strategy.ec.europa.eu/en/library/digital-decade-2024-egovernment-benchmark>

Wnioski z raportu sugerują, że kluczowe w osiągnięciu celów transformacji cyfrowej UE jest **działanie na rzecz wyrównania dysproporcji** pomiędzy krajami, grupami użytkowników i szczeblami rządowymi **w zakresie integracji i wydajności świadczenia usług cyfrowych**. Ponadto, państwa europejskie powinny dążyć do ich **proaktywnego świadczenia**, co oznacza, że obywatel uzyskuje efekt usługi w wyniku automatycznego działania administracji.

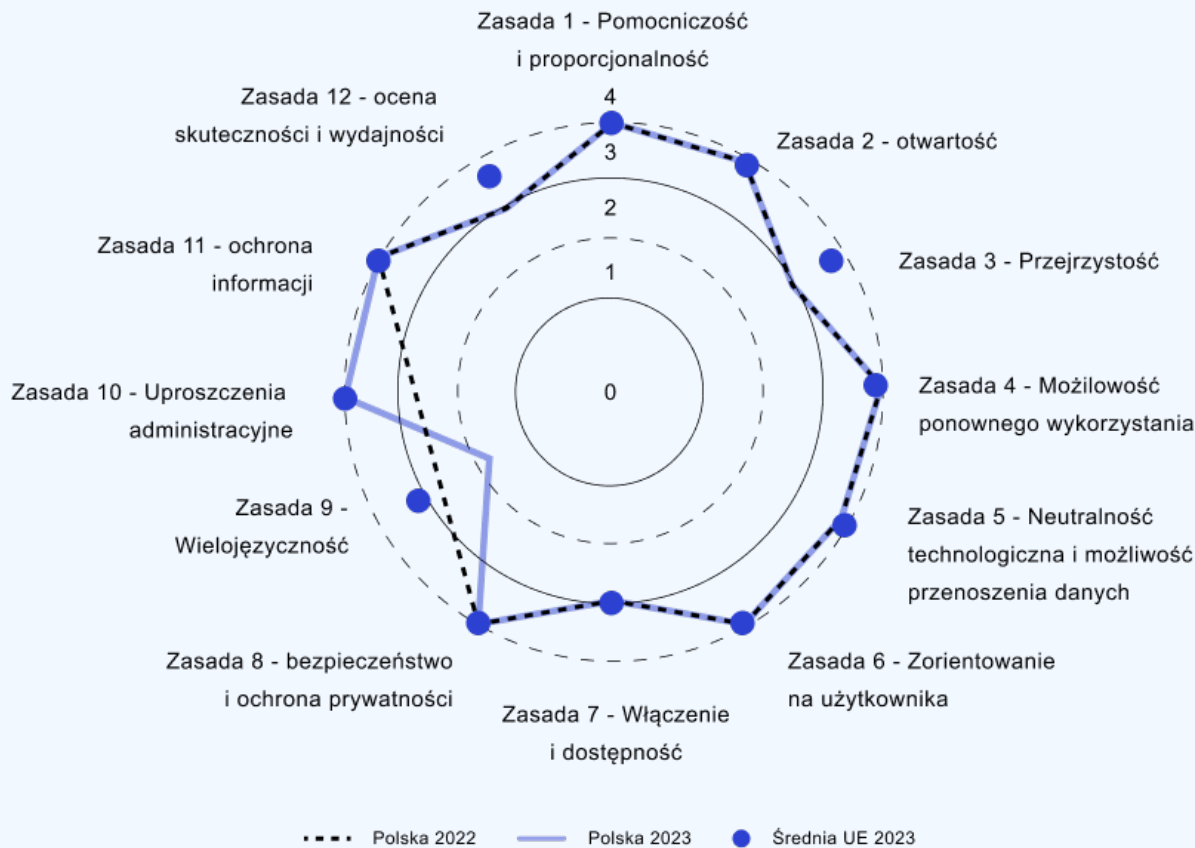
Digital Public Administration Factsheet (DPA)

Digital Public Administration Factsheet⁸ to unijny raport przedstawiający stan transformacji cyfrowej administracji publicznej ze szczególnym uwzględnieniem aspektów interoperacyjności. Raport jest publikowany corocznie i bazuje na danych przekazanych przez państwa UE, wskaźnikach Eurostatu, eGovernment Benchmark oraz wynikach uzyskanych w ramach mechanizmu monitorowania Europejskich Ram Interoperacyjności (EIF, ang. European Interoperability Framework).

Na przestrzeni lat 2018-2022 nastąpił stopniowy wzrost we wszystkich wskaźnikach dotyczących cyfrowej administracji publicznej w Polsce. Największy, blisko dwukrotny wzrost (z 21% w 2018 r. do 40% w 2022 r.) dotyczył odsetka osób korzystających z internetu do wysyłania wypełnionych formularzy w kontaktach z administracją publiczną. Zarazem, najniższy poziom osiągnął wskaźnik odsetka osób korzystających z Internetu w celu pobierania oficjalnych formularzy od administracji publicznej. W 2022 r. zanotowano wzrost o jedyne 7 pkt w stosunku do 2018 r., kiedy odsetek ten wynosił 20%.

⁸ https://joinup.ec.europa.eu/sites/default/files/inline-files/NIFO_2024%20Supporting%20Document_Poland_vFinal_rev.pdf

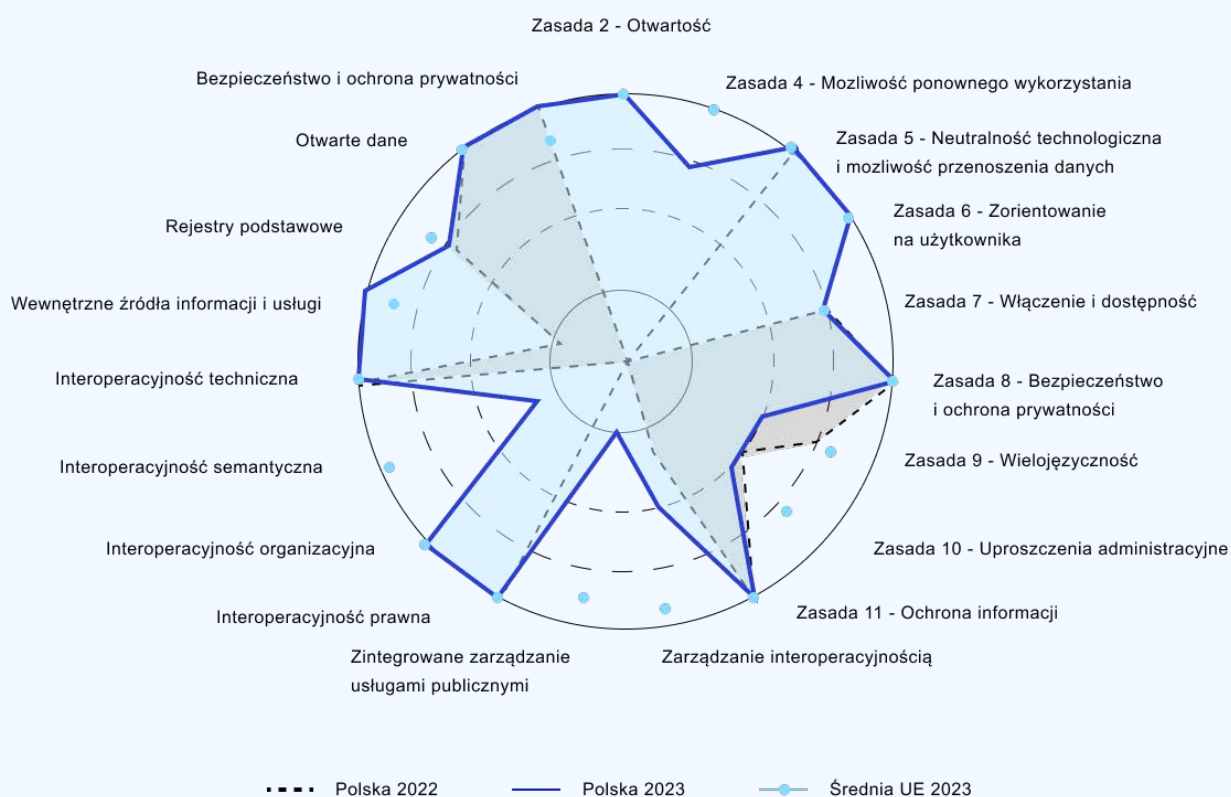
Zasady interoperacyjności



Wykres 3 Europejskie Ramy Interoperacyjności, Tablica wyników 1 - Zasady interoperacyjności, źródło: opracowanie własne na podstawie Digital Public Administration Factsheet 2024

Według raportu Digital Public Administration Factsheet 2024, Polska poczyniła znaczne postępy w zakresie cyfrowej transformacji administracji publicznej. Wzrost widoczny jest we wszystkich badanych obszarach. W zakresie zasad interoperacyjności, Polska osiągnęła wyniki na poziomie średniej unijnej za wyjątkiem zasady 3 *przejrzystość*, zasady 9 *wielojęzyczność*, oraz zasady 12 *ocena skuteczności i wydajności*. Zawarte w raporcie rekomendacje wskazują, że Polska powinna przeznaczyć więcej wysiłków na interoperacyjność systemów teleinformatycznych i techniczną infrastrukturę oraz uwzględnić wielojęzyczność przy ustanawianiu europejskich usług użyteczności publicznej. Należy zauważyć, że w 2023 r. zarekomendowano Polsce implementację nowych rozwiązań cyfrowych i optymalizację procesów administracyjnych, a w 2024 r. wynik Polski we wskaźniku *uproszczenia administracyjne* (zasada 10) wzrósł do maksymalnego możliwego poziomu.

Introperacyjność transgraniczna



Wykres 4 Europejskie Ramy Interoperacyjności, Tablica wyników 4 - Interoperacyjność transgraniczna, źródło: opracowanie własne na podstawie Digital Public Administration Factsheet 2024

W zakresie interoperacyjności transgranicznej Polska powinna poprawić wyniki we wskaźnikach związanych ze zintegrowanym zarządzaniem usługami publicznymi, a także interoperacyjnością semantyczną, które w obu przypadkach uzyskały wyniki poniżej średniej UE.

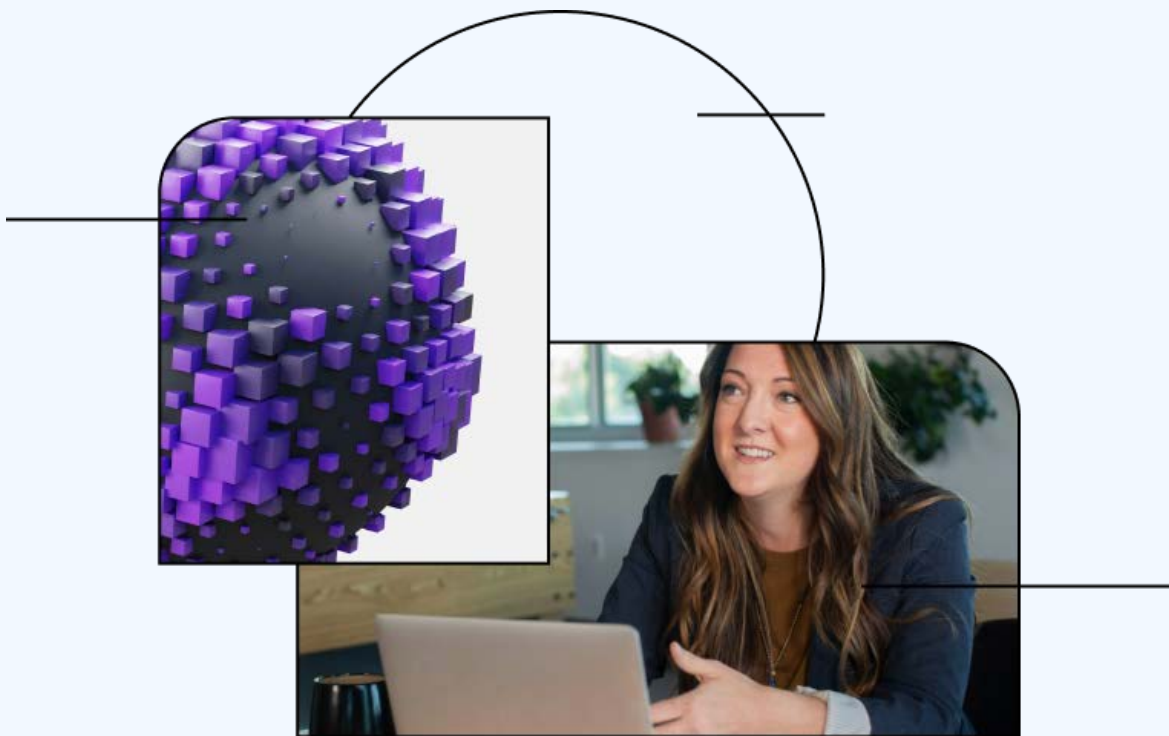
Digital Government Index (DGI)

W raporcie OECD (Organizacji Współpracy Gospodarczej i Rozwoju, ang. Organisation for Economic Cooperation and Development) Digital Government Index z 2023 r.⁹, oceniającym postępy transformacji cyfrowej sektora publicznego za lata 2020-2022, Polska uplasowała się na 20. miejscu wśród 33 państw członkowskich Organizacji. Wynik wyniósł 57,1%, przy średniej OECD na poziomie 60,5%. Najlepszy wynik tj. 11 pozycję Polska osiągnęła w kategorii *rząd jako platforma*, w której mierzone jest funkcjonowanie wspólnych elementów tj. wytyczne, narzędzia, dane, tożsamość cyfrowa i oprogramowanie, które umożliwią transformację procesów i usług publicznych. Obszarem, w którym Polska osiągnęła najniższy wynik, tj. 29. miejsce, jest *proaktywność*, definiowana jako *zdolność rządów do przewidywania potrzeb użytkowników i dostawców w celu świadczenia usług publicznych*.

9 https://www.oecd.org/en/publications/2023-oecd-digital-government-index_1a89ed5e-en.html

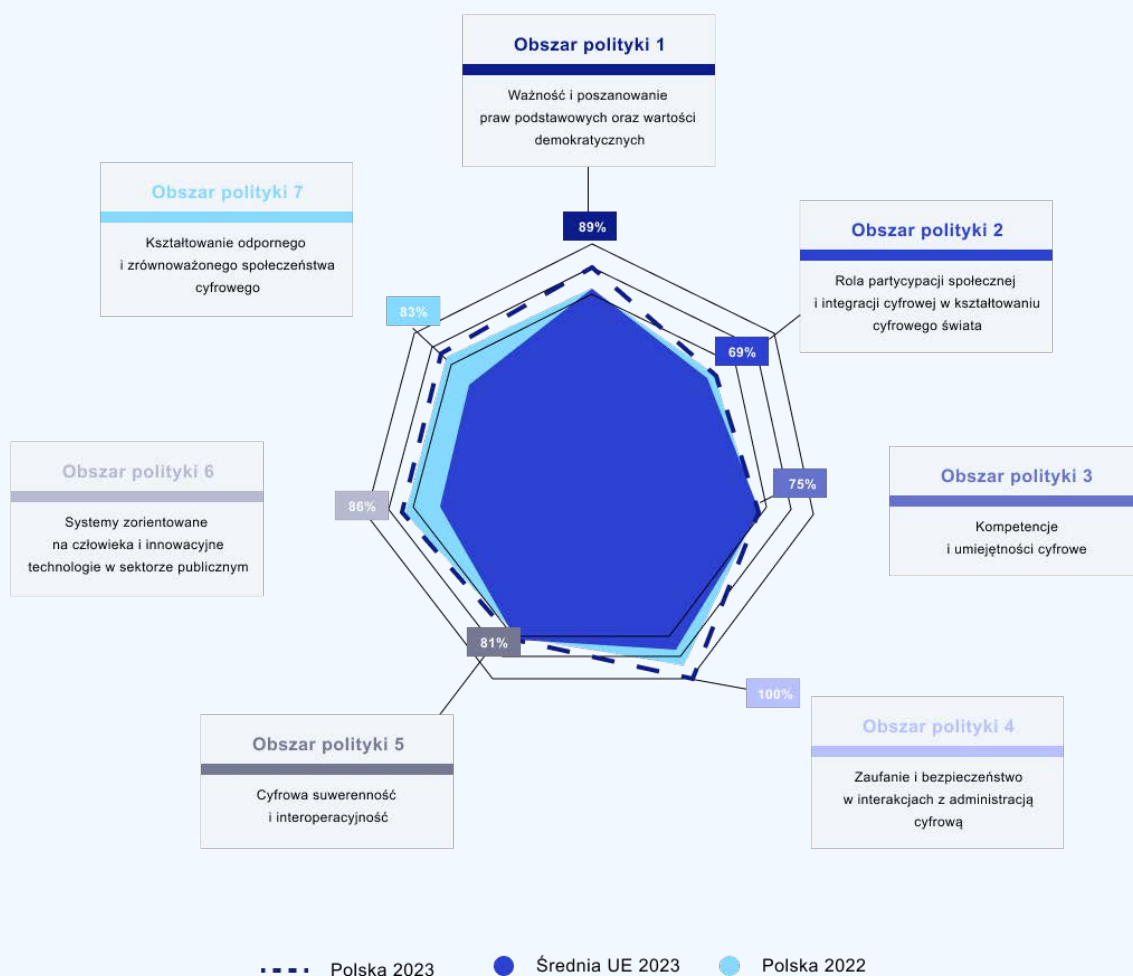
Deklaracja Berlińska

Deklaracja Berlińska w sprawie społeczeństwa cyfrowego i administracji cyfrowej opartej na wartościach określa szereg kluczowych zasad i towarzyszących im obszarów polityki wskazanych, aby zapewnić zgodność transformacji cyfrowej ze wspólnymi europejskimi prawami podstawowymi oraz wartościami. Raport z monitoringu Deklaracji Berlińskiej¹⁰ to narzędzie dokumentujące postępy w realizacji działań w ramach deklaracji dla państw sygnatariuszy. Mechanizm monitorowania opiera się na kluczowych wskaźnikach efektywności, do których ewaluacji wykorzystano dane zapewnione przez państwa członkowskie, eGovernment Benchmark, EIF, oraz DESI.



¹⁰ https://joinup.ec.europa.eu/sites/default/files/inline-files/BDM_Report_2023_vFinal_rev.pdf

Poziom realizacji obszarów polityki



Wykres 5 Monitoring Deklaracji Berlińskiej 2023, Poziom realizacji obszarów polityki - Polska w porównaniu ze średnią UE, źródło: opracowanie własne na podstawie Raportu z monitorowania Deklaracji Berlińskiej 2024

W raporcie wydanym w 2024 roku zauważono, że na ogół wyniki Polski wykazały stabilność i niewielkie wahania względem ubiegłorocznego podsumowania. **Największy wzrost, o 9 pkt, odnotowano w obszarze pierwszym ważność i poszanowanie praw podstawowych oraz wartości demokratycznych.** Na kolejnym miejscu usytuował się obszar czwarty, **zaufanie i bezpieczeństwo w interakcjach z administracją cyfrową, w którym wynik wzrósł o 4 pkt.** Niewielki spadek, o 2 pkt odnotowano w obszarze drugim *rola partycypacji społecznej i integracji cyfrowej w kształtowaniu cyfrowego świata*. Polska uzyskała wynik wyższy od średniej UE w czterech z siedmiu obszarów. **Największą różnicę, o 13 pkt, odnotowano w obszarze szóstym systemy zorientowane na człowieka i innowacyjne technologie w sektorze publicznym.** Następnie o 10 i 9 pkt w obszarze czwartym i obszarze siódmym *kształtowanie odpornego i zrównoważonego społeczeństwa cyfrowego*. Obszarami, w których Polska wypada poniżej średniej UE jest obszar trzeci *kompetencje i umiejętności cyfrowe*, w którym różnica wynosi 6 pkt, a także obszar piąty *cyfrowa suwerenność i interoperacyjność* z różnicą wynoszącą 4 pkt.

Polska została wyróżniona na tle Unii Europejskiej w obszarze siódmym *odporność i zrównoważony rozwój* za inicjatywy na rzecz rozwoju cyfrowych usług zdrowotnych, takich

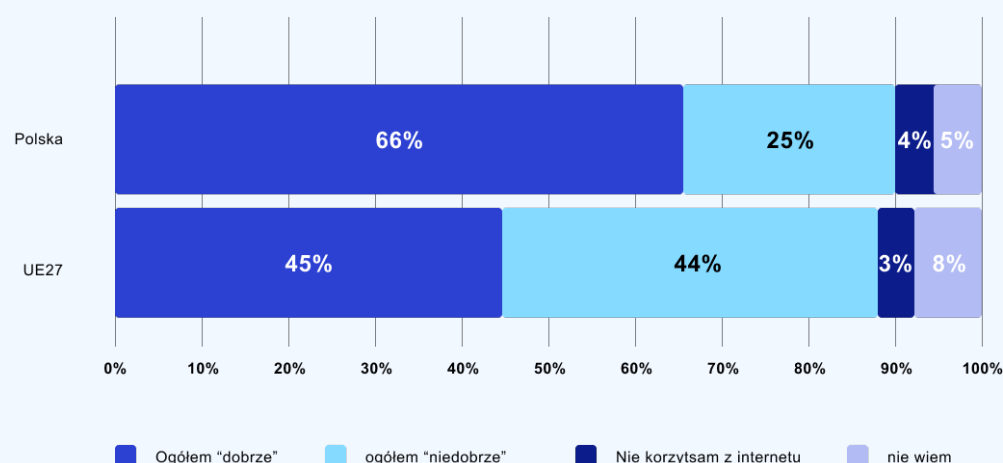
jak Internetowe Konto Pacjenta, aplikacja mojejKp, e-recepta czy uruchomienie na portalu pacjent.gov.pl chatbota informującego pacjentów o e-usługach w systemie ochrony zdrowia. **W obszarze czwartym zaufanie poprzez bezpieczeństwo w sferze cyfrowej dobrze oceniono rozwój mobilnej aplikacji mObywatel, a w obszarze szóstym systemy sztucznej inteligencji oparte na wartościach i zorientowane na człowieka efektywną koordynację działań związanych z rozwojem polskiego ekosystemu AI (m.in. strategicznie działania w Komitecie Rady Ministrów ds. Cyfryzacji).**

Specjalne badanie Eurobarometru: obywatele europejscy i cyfrowa dekada

Na potrzeby wsparcia monitoringu programu polityki „Droga ku cyfrowej dekadzie” do 2030 r. oraz założeń Europejskiej Deklaracji Praw i Zasad Cyfrowych na zlecenie Komisji Europejskiej przeprowadzono badanie sprawdzające, czy i w jakim stopniu ewoluują postawy obywateli Unii Europejskiej wobec technologii cyfrowych. Wnioski z wydanego w 2024 r. raportu¹¹ wskazują na to, że prawie trzy czwarte Europejczyków (73%) uważa, że cyfryzacja codziennych usług publicznych i prywatnych ułatwia im życie, w tym 19% twierdzi, że „znacznie ułatwia”. Nieco mniej niż jedna czwarta (23%) twierdzi, że cyfryzacja codziennych usług publicznych i prywatnych utrudnia im życie.

Przedstawione wyniki wskazują na to, iż **na ogół postawy i postrzeganie technologii cyfrowych przez Polaków jest pozytywne i oceniane na tym samym poziomie lub wyższym niż średnio wśród obywateli Unii**. W zakresie wyobrażeń dotyczących przyszłości technologii cyfrowych aż 80% (+3 pkt względem 2023 r.) Polaków myśli, że do 2030 r. technologie cyfrowe będą istotne w dostępie do usług opieki zdrowotnej lub korzystania z nich, tego samego zdania jest 79% obywateli UE. W porównaniu do 73% Europejczyków, **aż 81% Polaków uważa, że cyfryzacja codziennych usług publicznych i prywatnych ułatwia im życie.**

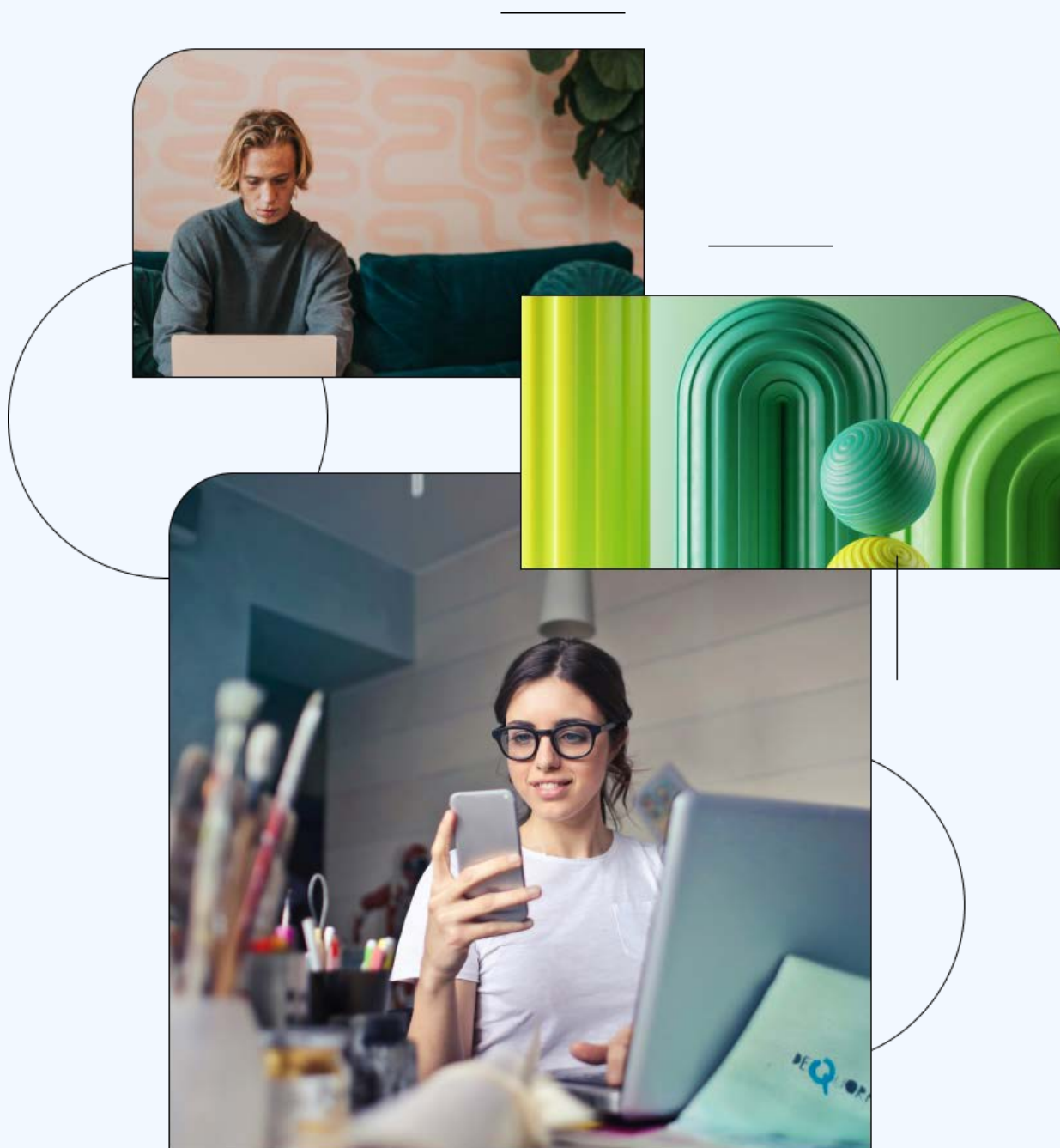
Jak dobrze Twoim zdaniem UE chroni Twoje prawa w środowisku cyfrowym?



11 <https://europa.eu/eurobarometer/api/deliverable/download/file?deliverableId=92894>

Wykres 6 Specjalne badanie Eurobarometru 551, pytanie QC7, źródło: opracowanie własne na podstawie Arkusza informacyjnego dla Polski

Jedynie 45% obywateli UE sądzi, że Unia dobrze chroni ich prawa w środowisku cyfrowym, podczas gdy tego samego zdania jest 66% obywateli Polski. W zakresie postrzegania stosowania zasad cyfrowych w kraju **najniższy wynik dotyczy zapewnienia bezpiecznego środowiska cyfrowego i treści dla dzieci i młodzieży. 59% Polaków sądzi, że zapewniane są one ogółem dobrze, natomiast 33%, że ogółem niezbyt dobrze** (średnia UE 39% - ogółem dobrze, 53% - ogółem niezbyt dobrze).



Wyzwania i trendy



Ministerstwo
Cyfryzacji

Tu tworzymy przyszłość

Wyzwania i trendy

W ostatnich kilkunastu latach – częściowo ze względu na pandemię – Polska zanotowała wyraźny rozwój w dziedzinie cyfryzacji, szybko nadrabiając dystans dzielący ją od unijnych liderów. Szczególnie widoczne były postępy w obszarach cyfrowych usług publicznych i otwartych danych. Z drugiej strony, w wielu dziedzinach dystans do liderów wciąż pozostaje znaczący; zwłaszcza w odniesieniu do kompetencji cyfrowych obywateli i wykorzystania technologii cyfrowych w przedsiębiorstwach.

Projektując cyfrowy rozwój kraju na kolejne lata, nie można jednak poprzestawać na analizie pozycji Polski w międzynarodowych wskaźnikach. Konieczna jest analiza i przygotowanie odpowiedzi na kluczowe trendy i wyzwania, wśród których wymienić warto:

Multipolaryzację świata.

Narastająca rywalizacja między mocarstwami przekłada się na obszar technologii. Przedmiotem współczesnej rywalizacji stały się kluczowe technologie tj. półprzewodniki, 5G, AI, czy technologie kwantowe. Ponadto, mocarstwa rywalizują ze sobą o zasoby służące do ich rozwoju – dane i surowce krytyczne. Z powodu pandemii, kurczących się zasobów i niestabilności gospodarczej dotychczasowe globalne łańcuchy dostaw ulegają znaczącemu skróceniu, co stanowi zarówno wyzwanie, jak i szansę dla Polski.

Nacisk na suwerenność technologiczną.

Postępująca rywalizacja przekłada się na dążenie do przywracania unijnej i krajowej produkcji kluczowych komponentów technologicznych i upraszczania łańcuchów dostaw. Suwerenność technologiczna jest istotna dla dalszego rozwoju, w tym utrzymania zdolności produkcyjnych w UE. Niemniej suwerenności technologicznej UE równolegle towarzyszy pogłębiająca się współpraca UE z państwami pozaeuropejskimi o zbliżonych wartościach i filozofii rozwoju cyfrowego (tzw. like-minded). Zauważalna jest konwergencja technologiczna i regulacyjna między tymi ośrodkami na świecie.

Splinternet.

Powyższym zjawiskom towarzyszy zjawisko splinternetu, tj. fragmentaryzacji otwartego internetu na rozdrobnione sieci pod kontrolą rządów czy korporacji. Takie zjawiska mają charakter negatywny i podważają fundamenty społeczne i gospodarcze internetu. Z perspektywy globalnej, istotnym czynnikiem jest zróżnicowane podejście do regulacji cyfrowych, biorące pod uwagę różne wrażliwości, niemniej bez naruszania fundamentalnych praw i wolności.

Wzrost znaczenia cyberbezpieczeństwa.

Nasilenie się rywalizacji międzynarodowej (w tym w obszarze technologii) przekłada się na konieczność zwrócenia większej uwagi na problem cyberbezpieczeństwa, zwłaszcza w odniesieniu do sektorów krytycznych. Kwestia ta ma jednocześnie rosnące znaczenie dla obywateli czy instytucji, coraz częściej narażonych na cyberataki i padających ofiarą profesjonalizacji grup cyberprzestępczych.

Hiperłączność,

zarówno w odniesieniu do interakcji międzyludzkiej za pośrednictwem technologii informacyjno-komunikacyjnych (ICT), jak i interakcji człowiek-maszyna i maszyna-maszyna (internet rzeczy). Trend ten bezpośrednio przekłada się na rosnące znaczenie danych i obciążenie sieci telekomunikacyjnych.

Zaburzenia konkurencji

wobec dominacji dużych platform technologicznych, których pozycja rynkowa zmniejsza zasięg kontroli rządów i stanowi istotne wyzwanie z perspektywy regulacyjnej. Jest ono tym większe, że wiele z najistotniejszych platform (społecznościowych czy handlowych) ma pochodzenie pozaunijne. Państwo musi angażować się w działania na rzecz zapewniania równego pola gry dla wszystkich uczestników rynku.

Rosnące koszty psychospołeczne związane ze sferą cyfrową.

Modele biznesowe oparte na uzależnianiu użytkowników od treści i algorytmach śledzących, upowszechnianie nierealistycznych standardów urody, dostęp nieletnich do szkodliwych treści, hejt, szerząca się dezinformacja – wszystkie te czynniki mają negatywny wpływ na zdrowie psychiczne dzieci i dorosłych, osłabienie więzi społecznych czy polaryzację debaty publicznej i wymagają kompleksowej odpowiedzi.

„Bliźniaczą przemianę”,

czyli bezpośrednie powiązanie transformacji cyfrowej z transformacją energetyczną, również w zakresie decyzji inwestycyjnych. Rośnie świadomość konieczności poszukiwania synergii między tymi procesami – wykorzystania zielonej energii do zaspokajania rosnących potrzeb związanych z tworzeniem i wykorzystywaniem ICT, a jednocześnie oparcia ekologicznej energetyki na technologiach cyfrowych.

Rozpowszechnianie się i szybki rozwój sztucznej inteligencji (AI),

która może stać się fundamentem przemian w sektorze cyfrowym w najbliższych latach. Wdrażanie AI oznacza nowe możliwości m.in. w obszarze badań, tworzenia treści czy usług, ale wiąże się też z zagrożeniami, które wymagają skoordynowanej odpowiedzi instytucji państwa.

Oddalenie infrastruktury i usług cyfrowych od użytkownika.

Elastyczność i skalowalność rozwiązań chmurowych sprawia, że coraz częściej przechowywanie i prowadzenie operacji na danych odbywa się nie przy wykorzystaniu lokalnej infrastruktury, a właśnie w chmurze. Rośnie popularność rozwiązań dostarczanych w modelu subskrypcyjnym – infrastruktury, platform czy usług.

Automatyzację i robotyzację gospodarki,

będąca owocem dążenia do zwiększenia efektywności przedsiębiorstw i wynikiem trudności w znalezieniu odpowiednio wykwalifikowanych pracowników.

Szybkie starzenie się polskiego społeczeństwa,

które jest obciążeniem dla systemu świadczeń społecznych i wyzwaniem z perspektywy konieczności rozwoju srebrnej gospodarki. Przełoży się na konieczność zwiększenia zastosowania technologii w gospodarce i dostosowania systemu rozwoju kompetencji przyszłości do zmienionej struktury demograficznej.

Niezakończony proces tworzenia jednolitego unijnego rynku cyfrowego

oraz trudności z dostępem do kapitału (w tym kapitału wysokiego ryzyka), utrudniające skalowanie przedsiębiorstw działających w obszarze ICT.



Większość z wymienionych trendów i wyzwań ma wymiar globalny lub przynajmniej unijny. Jednak efektywne projektowanie cyfrowego rozwoju Polski musi uwzględniać także krajowe oraz regionalne wyzwania i specyfiki. Tempo rozwoju technologicznego wymaga też, by analiza ta nie odbywała się incydentalnie, przy okazji tworzenia kolejnych strategii, lecz na bieżąco. Tym samym konieczne jest systemowe pogłębienie wiedzy i jej międzyinstytucjonalna wymiana, bez których znacząco utrudniona będzie właściwa alokacja ograniczonych zasobów i osiągnięcie efektu mnożnikowego czy wprowadzanie rozwiązań technicznych i legislacyjnych umożliwiających pogłębienie współpracy w ramach administracji.

Polska administracja musi posiadać też możliwość samodzielnej analizy trendów rynkowych i technologicznych, w celu odróżnienia tych, które mają realny wpływ na gospodarkę i społeczeństwo od tych, które są przede wszystkim tymczasowym medialnym trendem.

Efektywna implementacja wniosków z takich analiz będzie wymagała zaś wzmocnienia kompetencji cyfrowych urzędników i szkolenia kadr w zakresie polityk publicznych odnoszących się do cyfryzacji. Nie uda się też bez uspojnienia procesów polskiego rozwoju cyfrowego. Ze względu na horyzontalność cyfryzacji, trapiąca wciąż administrację silosowość jest bowiem w tym obszarze szczególnie szkodliwa. Należy budować świadomość konieczności bliskiej współpracy między instytucjami odpowiedzialnymi za budowę cyfrowego państwa, również z sektorów dzielących „wspólną granicę” z cyfryzacją w sensie ścisłym.



Analiza SWOT



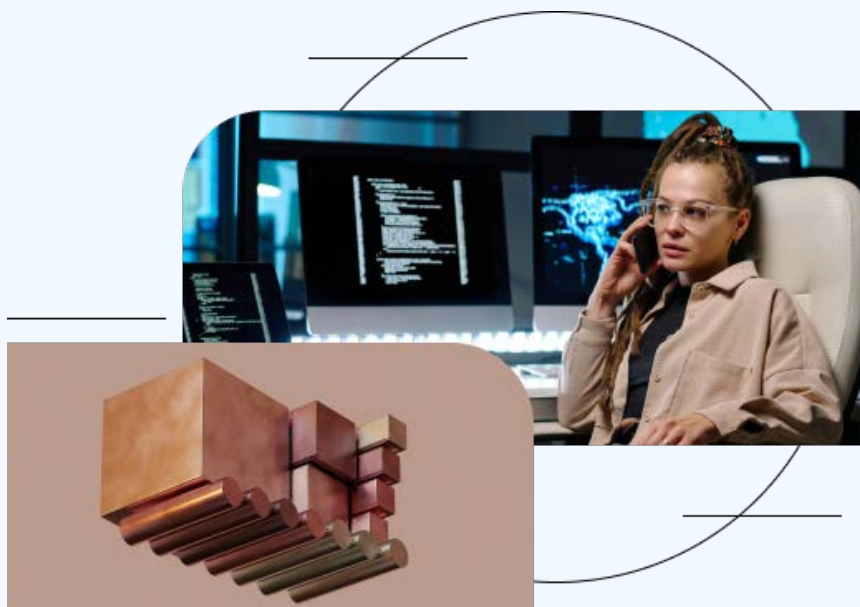
Ministerstwo
Cyfryzacji

Tu tworzymy przyszłość

Analiza SWOT

By wyznaczyć priorytety w obszarze cyfryzacji państwa na kolejną dekadę, konieczne było dokonanie dogłębnej analizy sytuacji w zakresach właściwości poszczególnych ministerstw, a także państwa jako całości. Uzyskane z ministerstw materiały diagnostyczne zostały uzupełnione przez analizę silnych i słabych stron, a także szans i zagrożeń dla cyfryzacji Polski, wykonaną przez Polski Instytut Ekonomiczny (PIE) na zlecenie Ministerstwa Cyfryzacji (MC). PIE przeprowadził analizę SWOT dla pięciu obszarów, blisko związanych z działaniami MC:

cyfrowego państwa;
kompetencji przyszłości;
infrastruktury;
gospodarki cyfrowej;
cyberbezpieczeństwa.



Cyfrowe państwo

W zakresie rozwoju cyfrowych usług publicznych (i prywatnych), Polska radzi sobie relatywnie dobrze. Wbrew dalekiemu miejscu w zestawieniach DESI, dystans do liderów jest mniejszy niż w innych obszarach, a niektóre krajowe rozwiązania (np. mObywatel) są dobrym przykładem dla innych państw. Ponieważ dla rozwoju usług cyfrowych kluczowe jest zaufanie społeczne do zastosowanych technologii, należy podkreślić, że w ostatnich latach nie było większych incydentów naruszających takie zaufanie. Według badań PIE, Polki i Polacy mają pozytywne nastawienie do e-usług, w tym do wykorzystania AI w usługach publicznych. 92,5 proc. respondentów deklaruje, że cyfrowe usługi publiczne ułatwiają im załatwianie spraw urzędowych. 66,7 proc. badanych jest zdania, że państwo powinno inwestować więcej w cyfrowe usługi publiczne, jednak tylko 27,2 proc. jest gotowych sfinansować te inwestycje przez podwyżkę podatków.

Istotną trudnością jest znaczne rozproszenie tworzonych usług, w tym dublowanie się zamawianych rozwiązań na poziomie lokalnym. Sugeruje to słabą koordynację działań w tym zakresie. Jednocześnie wiele usług ma braki na poziomie UX (doświadczenie użytkownika, ang. user experience), podczas gdy w innych ośrodkach na ten aspekt stawia się duży nacisk – brakuje wypracowanych standardów czy przepływu najlepszych praktyk. Ważnym wyzwaniem jest też cyfryzacja prowadzona przez samorządy. Na tym poziomie często bowiem brak kompetencji do wprowadzania cyfrowych usług, pojawiają się trudności z zapewnieniem utrzymania systemów (ze względu na jeszcze bardziej dojmujący niż na poziomie centralnym niedostatek specjalistów ICT); pojawiają się też obawy przed trwałą utratą pracy wskutek automatyzacji.



Silne strony	Słabe strony
<ul style="list-style-type: none"> • Szeroki wachlarz cyfrowych usług publicznych; • Dostęp do funduszy strukturalnych; • Istniejące, dobrze funkcjonujące rozwiązania (mObywatel, e-PIT); • Otwartość na zmiany i aplikowanie nowych rozwiązań. 	<ul style="list-style-type: none"> • Dług technologiczny (utrzymujące się stare systemy w administracji); • Braki kompetencyjne i obawy w administracji, zwłaszcza po stronie samorządów; • Niski poziom zaufania do państwa; • Niekonkurencyjne wynagrodzenia dla specjalistów ICT w administracji publicznej. • Brak pełnej interoperacyjności systemów i rejestrów wykorzystywanych w administracji publicznej.
Szanse	Zagrożenia
<ul style="list-style-type: none"> • Pozytywne nastawienie społeczne do cyfrowych usług publicznych oraz stosowania AI w administracji; • Partnerstwo z biznesem i korzystanie z najlepszych rozwiązań rynkowych; • Rozwój lokalnego rynku ICT. 	<ul style="list-style-type: none"> • Uzależnienie od rozwiązań dostarczanych przez zewnętrznych dostawców; • Nakładanie się różnych mechanizmów i perspektyw czasowych w dokumentach strategicznych; • Silosowość w administracji publicznej – brak koordynacji działań i wspólnych standardów. • Rywalizacja geopolityczna i zagrożenie uderzeniem w czułe punkty cyfrowej infrastruktury kraju; • Szybko zmieniające się otoczenie technologiczne; oddalanie się sektora prywatnego od publicznego w zakresie stosowanych technologii.

Kompetencje przyszłości

W dzisiejszych czasach posiadanie kompetencji cyfrowych jest potrzebne zarówno do rozwoju osobistego, aktywności społecznej i obywatelskiej, jak i funkcjonowania na rynku pracy. Choć ich rozwój był w ostatnich latach przedmiotem wsparcia w ramach wielu inicjatyw, dystans do poziomu średniej unijnej pozostaje znaczący – zaledwie 44 proc. polskich obywateli posiada przynajmniej podstawowe umiejętności cyfrowe przy średniej UE wynoszącej 56%. Silne strony są ograniczone, a część ekspertów wskazuje na utrzymywanie się tych samych barier i wyzwań w dziedzinie kompetencji cyfrowych od wielu lat. Odpowiedź na problemy zdiagnozowane w tym zakresie miał stanowić Program Rozwoju Kompetencji Cyfrowych, którego opracowanie i uchwalenie zajęło ponad 4 lata, w związku z czym na jego efekty przyjdzie jeszcze poczekać.

W perspektywie kolejnych lat rysują się bardzo istotne wyzwania z obszaru demografii, a także niepokojący trend spadającego odsetka absolwentów kierunków STEM (nauka, technologia, inżynieria, matematyka, ang. science, technology, engineering, mathematics) (z drugiej strony, absolwentów kierunków ICT jest coraz więcej). Niekorzystny wpływ mają również inne czynniki np. niski poziom cyfryzacji firm. Z drugiej strony, jako niewątpliwą szansę należy traktować łatwą dostępność przykładów dobrych praktyk stosowanych przez inne kraje oraz wysoki poziom wiedzy eksperckiej zgromadzony m.in. w organizacjach społecznych zaangażowanych w rozwijanie kompetencji cyfrowych w Polsce.

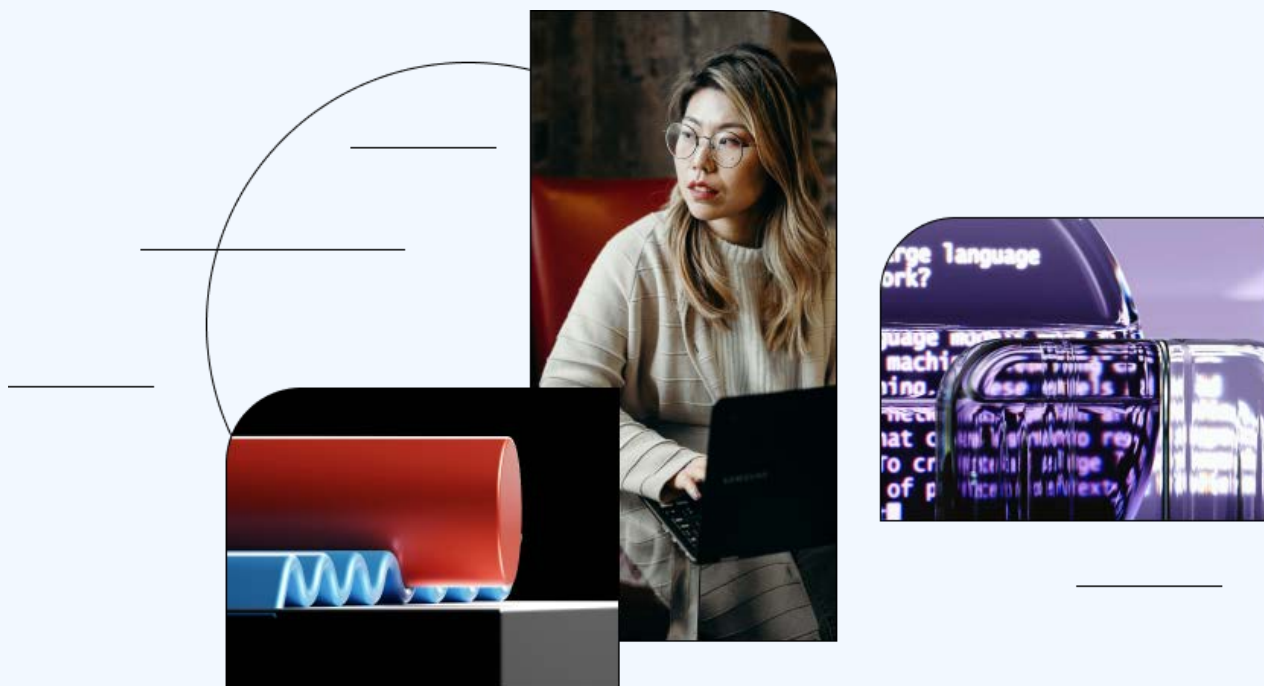


Silne strony	Słabe strony
<ul style="list-style-type: none"> • Wysoki poziom kształcenia technicznego na uczelniach; • Relatywnie wysoki (na tle Europy Środkowo-Wschodniej) poziom cyfryzacji w szkołach, w tym wyposażenie ich w szerokopasmowy dostęp do internetu; • Wysoki poziom wiedzy eksperckiej zgromadzony m.in. w instytucjach zaangażowanych w rozwijanie kompetencji cyfrowych w Polsce. 	<ul style="list-style-type: none"> • Niski poziom umiejętności cyfrowych obywateli we wszystkich kategoriach wiekowych, nawet wśród tzw. cyfrowych tubylców - osób młodych w wieku 16-19 lat; • Stosunkowo mały zasób specjalistów ICT i udział kobiet w zawodach ICT; • Niewystarczająca jakość edukacji cyfrowej. • Odsetek absolwentów kierunków STEM poniżej średniej unijnej; • Niska w porównaniu z innymi krajami UE aktywność edukacyjna osób dorosłych w Polsce; • Zbyt mały nacisk na rozwój miękkich kompetencji przyszłości.
Szanse	Zagrożenia
<ul style="list-style-type: none"> • Wzrost świadomości wśród decydentów oraz w społeczeństwie znaczenia kompetencji cyfrowych dla jakości życia obywateli i kondycji gospodarki; • Dostępność przykładów dobrych praktyk stosowanych przez inne kraje. 	<ul style="list-style-type: none"> • Szybko zmieniający się zakres kompetencji cyfrowych wymagających uzupełniania przez całe życie; • Starzenie się społeczeństwa i wykluczenie cyfrowe seniorów; • Drenaż talentów; • Brak stabilności wsparcia rozwoju kompetencji cyfrowych; • Kryzys zdrowia psychicznego i inne ryzyka związane z ekspozycją na media elektroniczne.

Infrastruktura

Infrastruktura telekomunikacyjna jest przykładem sukcesu wydatkowania środków unijnych oraz regulacji. Polska ma szeroki dostęp do nowoczesnych sieci oraz niezwykle konkurencyjny rynek, dający bardzo dobre warunki konsumentom. Pojawiają się jednak nowe wyzwania – potencjalne wykorzystanie alternatywnych technologii dostępowych (ze względu na bardzo wysokie koszty pokrycia całego kraju światłowodem); konieczność stymulacji popytu na dostęp do internetu i zapewnianie utrzymania sieci wobec rosnących kosztów; tworzenie nowych „infrastruktur” – chmury, komputerów kwantowych czy sieci prywatnych w przedsiębiorstwach.

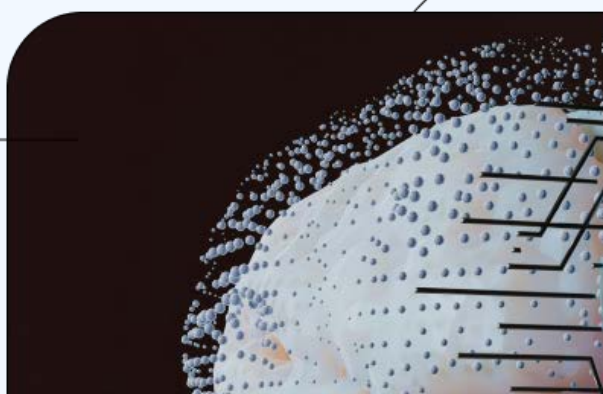
Szansą na zwiększenie środków na inwestycje oraz na poszerzenie pola działalności operatorów telekomunikacyjnych (skarżących się od lat na malejące przychody) jest trend oddzielania infrastruktury od usług (w Polsce widoczny zarówno w sieciach ruchomych jak i stacjonarnych). Telekomy mają jednak ograniczone umiejętności wchodzenia w nowe obszary biznesowe, a niski poziom cyfryzacji firm nie sprzyja ekspansji w tym kierunku. Ryzyko płynie również z zyskującej na popularności tezie o konieczności zgody na konsolidację operatorów telekomunikacyjnych w UE – dla polskiego rynku mogłoby to raczej oznaczać wzrost cen, przy wątpliwym pozytywnym wpływie na jakość dostępnej infrastruktury.



Silne strony	Słabe strony
<ul style="list-style-type: none"> • Duża konkurencja i dobra oferta dla konsumentów; • Relatywnie szeroki dostęp do światłowodów oraz dobry zasięg usług mobilnych; • Znaczące środki publiczne i duże doświadczenie w zakresie dysponowania nimi. 	<ul style="list-style-type: none"> • Ograniczona innowacyjność telekomów; • Opóźnione postępowania na częstotliwości dla sieci 5G.
Szanse	Zagrożenia
<ul style="list-style-type: none"> • Trend rozdzielania infrastruktury od usług; • Dostęp satelitarny o coraz wyższej przepływności; • Rozwijanie przez telekomy nowych modeli biznesowych; • Planowane działania stymulujące popyt na łącza o wysokich przepływnościach. 	<ul style="list-style-type: none"> • Nierównomierny dostęp do infrastruktury; • Brak uwzględnienia alternatywnych technologii przy zapewnianiu dostępu; • Niewielki popyt na łącza o najwyższych przepływnościach; • Brak udziału w międzynarodowych projektach wdrażania 5G; • Przebijająca się narracja o konieczności konsolidacji rynku telekomunikacyjnego.

Cyberbezpieczeństwo

Obszar cyberbezpieczeństwa jest powiązany ze wszystkim innymi obszarami, a silne i słabe strony, szanse i zagrożenia współgrają z tymi wskazanymi w innych częściach. Polska dysponuje istotnym zasobem kapitału ludzkiego – ekspertów w instytucjach zapewniających cyberbezpieczeństwo na poziomie krajowym czy startupów zajmujących się cyberbezpieczeństwem. Jednocześnie jednak, niski poziom kompetencji cyfrowych (w tym wśród przedsiębiorstw) może przekładać się na narastające ryzyka i dużą liczbę „słabych ogniw”. W wielu aspektach kluczowy dla cyberbezpieczeństwa jest wymiar międzynarodowy. Bliskość pełnoskalowej wojny w Ukrainie oraz agresywna postawa Rosji i innych aktorów międzynarodowych zwiększa liczbę cyberataków, ale zarazem pozwala rozwijać kompetencje w konfrontacji z realnym zagrożeniem. Korzystnym czynnikiem dla zwiększenia poziomu cyberbezpieczeństwa jest także rozwijający się rynek – zarówno rodzimych firm, jak i obecność światowych potentatów, która pozwala na korzystanie z ich wiedzy, doświadczeń i infrastruktury. Koordynację działań w obszarze cyberbezpieczeństwa może utrudniać rozproszenie odpowiedzialnych za niego instytucji oraz brak „jednego okienka” dla podmiotów krajowego systemu cyberbezpieczeństwa (KSC) i obywateli. Kwestie prawne natomiast są zarówno problemem, jak i szansą – z jednej strony niekorzystne są bowiem opóźnienia w tworzeniu niektórych aktów prawnych oraz ich coraz większa ilość komplikująca system prawny, z drugiej jednak wciąż istnieje możliwość przyjęcia dobrych przepisów oraz poszerzenie debaty na poziomie europejskim.



Silne strony	Słabe strony
<ul style="list-style-type: none"> • Zespoły CSIRT (Zespoły Reagowania na Incydenty Bezpieczeństwa, ang. Computer Security Incident Response Team) poziomu krajowego i inne instytucje odpowiedzialne za zapewnianie cyberbezpieczeństwa na poziomie krajowym; • Duży zasób specjalistów w sektorze publicznym i prywatnym; • Inicjatywy zwiększające cyberbezpieczeństwa na poziomie krajowym (w tym AntyDDoS, ARAKIS-GOV, ARTEMIS, SKR-Z, S46, CTI); • Duża liczba kierunków studiów związanych z cyberbezpieczeństwem; • Członkostwo w NATO (współpraca sojusznicza i kolektywna obrona) oraz członkostwo w UE (mechanizmy współpracy i regulacje). 	<ul style="list-style-type: none"> • Niskie wykorzystanie chmury obliczeniowej; • Niski poziom umiejętności cyfrowych, braki kompetencyjne w administracji publicznej; • Niska świadomość dotycząca zagrożeń w społeczeństwie i administracji; • Rozproszenie instytucji odpowiedzialnych za cyberbezpieczeństwo; • Bliskość pełnoskalowej wojny w Ukrainie, narażenie na cyberataki ze strony Federacji Rosyjskiej; • Braki kadrowe w IT wśród MŚP.
Szanse	Zagrożenia
<ul style="list-style-type: none"> • Rosnąca świadomość dotycząca ochrony danych i prywatności; • Wzrost znaczenia bezpieczeństwa w dyskusjach o kierunku rozwoju, przekładająca się na szanse wzrostu finansowania. 	<ul style="list-style-type: none"> • Popularyzacja smart-urządzeń (IoT – internet rzeczy, ang. Internet of Things) i rozwój przemysłu 4.0; • Popularyzacja pracy zdalnej; • Wykorzystanie generatywnej AI przy szkodliwej działalności w cyberprzestrzeni; • Rozwój technologii kwantowych jako zagrożenie dla bezpieczeństwa informacji; • Nasilająca się rywalizacja geopolityczna; • Wzrost liczby cyberataków; • Trudności w utrzymaniu specjalistów w sektorze publicznym; • Niski priorytet cyberbezpieczeństwa w polskich firmach oraz w administracji.

Gospodarka cyfrowa

W Polsce istnieje wciąż znaczna przestrzeń do cyfryzacji firm, automatyzacji i robotyzacji produkcji. Robotyzacja jest na niskim poziomie w stosunku do krajów regionu, a tym bardziej w odniesieniu do europejskich liderów. Wydaje się jednak, że trendy demograficzne, regulacyjne (m.in. wzrost płacy minimalnej) i rynkowe mogą przyspieszyć zmiany w tym obszarze w Polsce. Silną stroną jest obecność regionów chmurowych największych globalnych dostawców chmury – a zatem ich bezpośrednie zaangażowanie w rozwijanie cyfrowej gospodarki. Trudnością z kolei bariery mentalne (tj. brak motywacji przedsiębiorców do wdrażania nowych rozwiązań – zdecydowanie trudniejsze do przezwyciężenia niż np. bariery finansowe), „pułapka kraju średniej wielkości” (rynek krajowy wystarczająco duży do utrzymania firmy, brak zewnętrznych bodźców do rozwoju) czy wreszcie niewystarczająca dostępność krajowego kapitału (bariera wykraczająca poza sferę cyfrową). Innym ryzykiem, również wykraczającym poza tylko sferę cyfrową, jest struktura gospodarki, z dużą nadwyżką firm mikro- i małych (najprawdopodobniej niezależnie od dużego odsetka pozornie samozatrudnionych).

W rezultacie może powstać dualna gospodarka, w której firmy z kapitałem zagranicznym, włączone w globalne łańcuchy dostaw czy eksportujące stosują nowoczesne rozwiązania technologiczne i cyfrowe, a druga część pozostaje w tyle. Takie zagrożenie sugerują wskaźniki rozwoju sektora ICT, w tym w odniesieniu do flagowego polskiego obszaru eksportowego – branży gamedev (tworzenie gier komputerowych, ang. game development). Ukazują one bardzo niską liczbą specjalistów ICT w całej gospodarce, wskazującą na niski priorytet cyfryzacji w większości firm.

Istotnym kontekstem dla przyszłości polskiej gospodarki cyfrowej są też trendy demograficzne. Już w 2023 r. 25 proc osób pracujących (w wieku 18-64 lata) stanowiły osoby w wieku 50 lat lub wyższym¹². Jak wynika z analizy PIE, do 2035 r. polski rynek pracy skurczy się o 2,1 mln pracowników, czyli 12,6 proc. obecnego zatrudnienia. Najpoważniejsze skutki zmian demograficznych dotkną sektor edukacji (zmniejszenie bazy pracowników o nawet 29 proc.) oraz opieki zdrowotnej (spadek o nawet 23 proc.). Sektory przemysłowe (sekcje B-E) mogą do 2035 utracić nawet 400 tys. pracowników (spadek o 11 proc.).

Jednym z potencjalnych rozwiązań niwelujących negatywne skutki spadku podaży pracy jest wykorzystanie nowoczesnych technologii. Automatyzacja, wykorzystanie robotów przemysłowych, systemów RPA (Robotic Process Automation) oraz sztucznej inteligencji mogą wspomagać ludzką pracę, zwiększać jej efektywność lub nawet całkowicie ją zastępować¹³. Dzięki takim rozwiązaniom można zautomatyzować część etatów lub zmniejszyć zapotrzebowanie na pracę w sektorach zmagających się z niedoborami siły roboczej – tych, w których nie przyniesie to nadmiernych negatywnych kosztów społecznych.

Pomimo obecnie obserwowanego w Polsce niskiego poziomu adaptacji nowych technologii, można zakładać, że spadająca podaż pracowników, a co za tym idzie wzrost kosztów pracy, przełożą się na potrzebę innowacyjnych inwestycji na rzecz automatyzacji w polskich

12 <https://pie.net.pl/wp-content/uploads/2024/10/Podaz-pracy.pdf>

13 <https://pie.net.pl/wp-content/uploads/2024/10/Podaz-pracy.pdf>

przedsiębiorstwach¹⁴. W polskim przemyśle istnieje nadal duży potencjał automatyzacji, ponieważ obecna gęstość robotyzacji należy do najniższych w Unii Europejskiej¹⁵. Również sztuczna inteligencja jako technologia, która jest jednocześnie komplementarna oraz substytucyjna wobec pracowników wysoko wykwalifikowanych, daje duży potencjał na przejmowanie niektórych zadań od ludzi, a jednocześnie zwiększenie efektywności wykonywania pozostałych zadań, co może pomóc zniwelować negatywne skutki zmian demograficznych¹⁶.



14 <https://pie.net.pl/wp-content/uploads/2024/10/Podaz-pracy.pdf>

15 <https://pie.net.pl/wp-content/uploads/2024/07/Robotyzacja-w-Polsce-w-2023.pdf>

16 <https://www.whitehouse.gov/wp-content/uploads/2024/03/ERP-2024.pdf>

Silne strony	Słabe strony
<ul style="list-style-type: none"> • Dostępność technologii największych globalnych graczy; • Wysoki eksport ICT (szczególnie usług); • Relatywnie wysokie nakłady polskich dużych firm na RD. 	<ul style="list-style-type: none"> • Relatywnie niski poziom robotyzacji; • Brak strategii przemysłowej; • Niski poziom kompetencji cyfrowych; • Niska motywacja pracodawców do wdrażania innowacyjnych / cyfrowych rozwiązań; • Niski odsetek specjalistów ICT zatrudnionych w gospodarce; • Niska dostępność krajowego kapitału; • Niska innowacyjność gospodarki.
Szanse	Zagrożenia
<ul style="list-style-type: none"> • Podnoszenie płacy minimalnej jako potencjalny impuls do automatyzacji/cyfryzacji; • Szybkie tempo rozwoju gospodarki. 	<ul style="list-style-type: none"> • Brak silnego ekosystemu inwestycji w startupy; • Mały w stosunku do potrzeb dopływ specjalistów ICT; • Wysokie koszty zatrudnienia specjalistów ICT; • "Luka cyfrowa" wśród przedsiębiorców - grupa zautomatyzowanych firm, przeważnie dużych, eksportujących, będących w posiadaniu zagranicznego

Cele i czynniki umożliwiające ich realizację

Powyżej zarysowane uwarunkowania – obok doświadczeń z dotychczasowego funkcjonowania Ministerstwa Cyfryzacji, rekomendacji z licznych raportów z administracji i rynku oraz ciał doradczych, a także ewaluacji realizacji dotychczas obowiązujących dokumentów strategicznych – były dla nas drogowskazem w opracowaniu założeń poniższej strategii.

Biorąc pod uwagę horyzontalność procesów cyfryzacji i jej silny wpływ na wiele aspektów ludzkiego życia, uznajemy za główny cel niniejszej strategii podnoszenie jakości życia dzięki cyfryzacji.

Do realizacji tego celu konieczne jest spełnienie szeregu warunków, poczynając od zapewnienia właściwego prawodawstwa i **bezpieczeństwa w sferze cyfrowej, wsparcie obywateli w rozwijaniu kompetencji** koniecznych do poruszania się w świecie cyfrowym oraz **zagwarantowanie odpowiedniej jakości dostępu do sieci oraz usług**. Zapewnienie bezpieczeństwa oraz rozwój kompetencji i łączności należy uznać jednocześnie za istotne cele strategii, jak i fundamentalne czynniki umożliwiające społeczeństwu korzystanie z rozwijających się technologii cyfrowych.

Za kluczowe priorytety uznajemy również **rozwój polskiej gospodarki cyfrowej** (a także wykorzystanie technologii cyfrowych do rozwoju innych branż) i jej konkurencyjności, **budowanie sprawności administracji w oparciu o technologie** oraz **zabezpieczenie praw polskich obywateli w domenie cyfrowej**.

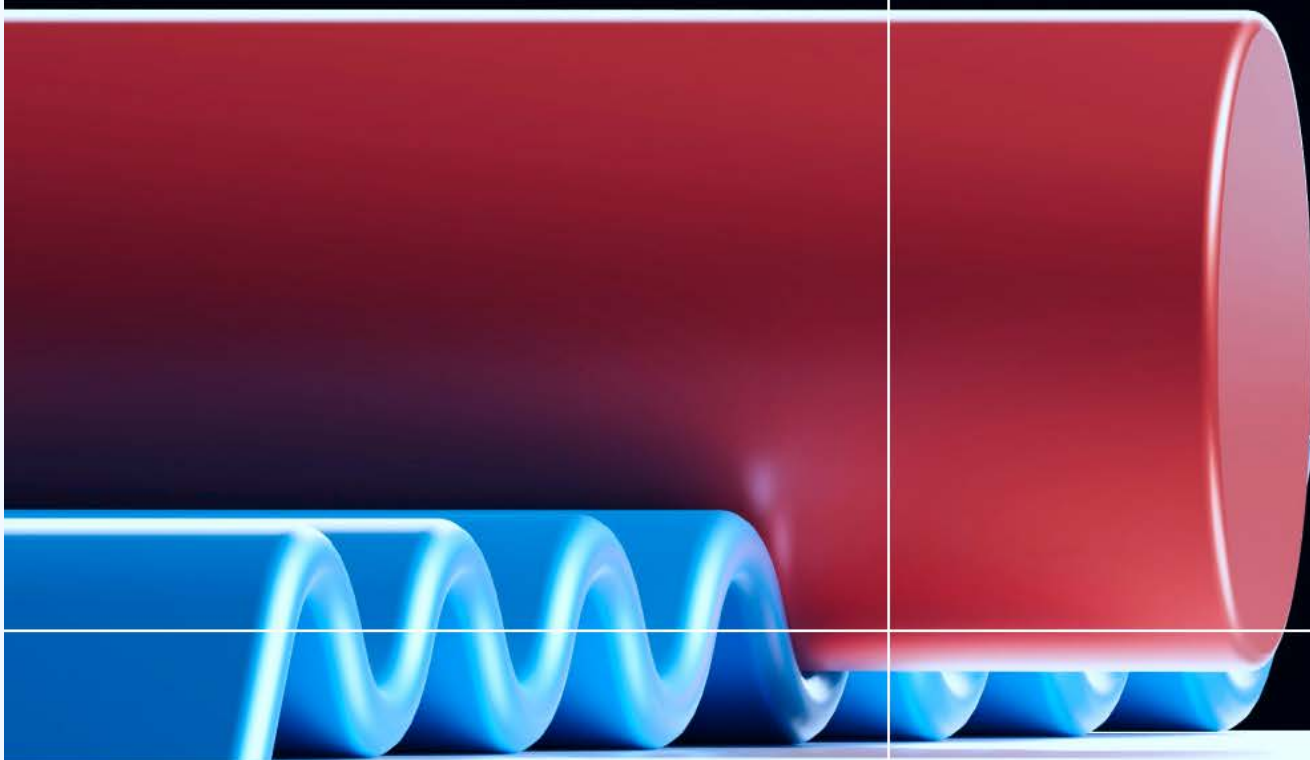
By powyższe cele i warunki mogły być skutecznie realizowane, konieczne jest:

- a) **Zwiększenie koordynacji prac między podmiotami administracji publicznej** – zarówno centralnej, jak i samorządowej – a także wsparcia innych instytucji publicznych. Brak jednego ośrodka odpowiedzialnego za cyfryzację kraju we wszystkich obszarach wymaga poprawy mechanizmów koordynacji między różnymi podmiotami działającymi w tym zakresie. Poruszanie się w szybko zmieniającej się sferze technologii wymaga też zwiększenia elastyczności funkcjonowania państwa w tym obszarze.
- b) **Przeznaczenie wystarczających zasobów finansowych, kadrowych i organizacyjnych** na rozwój cyfrowego państwa, społeczeństwa i gospodarki opartej

na danych. Inwestycje w obszar cyfrowy – zapewnianie cyberbezpieczeństwa, unowocześnianie procesów w administracji, usprawnianie e-usług, podniesienie liczby wdrożeń opartych o sztuczną inteligencję czy wsparcie tworzenia innowacji – są kluczowe, ale kosztują i wymagają zaangażowania odpowiednio wynagradzanych i kompetentnych kadr.

- c) **Długofalowe projektowanie cyfrowego rozwoju kraju.** Choć precyzyjne przewidzenie kierunków rozwoju technologii jest często niemożliwe, za istotne należy uznać zwiększenie kompetencji analitycznych ośrodków odpowiedzialnych za tworzenie polityki cyfrowej w Polsce – pozwoli to bowiem na wczesnym etapie identyfikować trendy, których uwzględnienie może być korzystne dla kraju. Należy mieć także na względzie zapewnianie neutralności technologicznej rozwiązań stosowanych przez państwo, co umożliwi uniknięcie długofalowego uzależnienia od jednego dostawcy.
- d) **Wsparcie sprawiedliwej transformacji cyfrowej,** w ramach której zagwarantowany zostanie zrównoważony rozwój oraz zwiększenie konkurencyjności gospodarki (w tym w powiązaniu z transformacją energetyczną oraz prawami pracowniczymi), włączenie społeczne, dostępność cyfrowa dla osób z niepełnosprawnościami oraz realizacja praw i zasad cyfrowych, zawartych m.in. w Europejskiej Deklaracji Praw i Zasad Cyfrowych w Cyfrowej Dekadzie. Odpowiednio zaprojektowana transformacja cyfrowa musi uwzględniać m.in. powiązania z transformacją energetyczną, zagwarantowanie praw pracowniczych i wsparcie przekwalifikowania osób, których miejsca pracy są zagrożone przez zmiany technologiczne.
- e) **Projektowanie cyfrowych przemian w duchu technorealizmu** – uznanie, że rozwój technologii nie jest odpowiedzią na wszystkie problemy. Jakkolwiek ma on potencjał do realnej poprawy jakości życia, jednak wiąże się on też z zagrożeniami, na które państwo musi reagować i im zapobiegać.
- f) Przyjęcie założenia, że wprowadzanie nowych rozwiązań cyfrowych **nigdy nie może odbywać się kosztem bezpieczeństwa** – rozumianego zarówno w odniesieniu do obszaru cyberbezpieczeństwa, jak i praw podstawowych obywateli, ich dobrostanu psychicznego i spójności społecznej .
- 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 relacje 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.

Na potrzeby usystematyzowania kierunków interwencji określone zostały 4 obszary horyzontalne, które ze względu na rangę i znaczenie, istotnie wpływają na efektywność działań w innych obszarach i stanowią punkt wyjścia dla transformacji cyfrowej wielu dziedzin życia społeczno-gospodarczego. Są to: komunikacja elektroniczna, kompetencje przyszłości, cyberbezpieczeństwo oraz koordynacja transformacji cyfrowej.



Obszary horyzontalne



Tu tworzymy przyszłość

Obszary horyzontalne

1.1 Komunikacja elektroniczna

Diagnoza – jak jest?

W Polsce wciąż ok. 24% gospodarstw domowych ma dostęp do sieci o przepustowości poniżej 100 Mb/s, której nie można zwiększyć do przepustowości gigabitowej. Natomiast usługi w technologii 5G dostępne są tylko na 54% obszaru kraju i objętych jest nimi 82% gospodarstw domowych. Jednocześnie, wraz z postępującym rozwojem jakości usług łączności elektronicznej i ich dostępności, coraz większym wyzwaniem staje się pobudzenie popytu na korzystanie z internetu – na koniec 2023 roku zaledwie 65,5% gospodarstw domowych abonowało usługę stacjonarnego dostępu do internetu.

Zapewnienie powszechnego dostępu do bardzo szybkiego internetu wszystkim obywatelom jest jednym z determinantów rewolucji cyfrowej.

Umożliwia budowę kapitału cyfrowego społeczeństwa, upowszechnienie kwalifikacji cyfrowych, wspieranie kompetencji cyfrowych wśród dzieci i młodzieży w procesie edukacji, czy też upowszechnienie cyfrowych usług publicznych. Proces ten nie może odbyć się bez zapewnienia bezpiecznej, wydajnej i zrównoważonej infrastruktury cyfrowej. Na tej płaszczyźnie coraz większym wyzwaniem staje się sukcesywna eliminacja tzw. białych plam NGA (ang. Next-generation access) ze względu na konieczność dotarcia z inwestycjami do najtrudniejszych – z punktu widzenia dostępności i ukształtowania terenu oraz gęstości zaludnienia – punktów adresowych, które generują konieczność znacznych nakładów finansowych. Ze względu na potencjalnie niską opłacalność dla przedsiębiorców telekomunikacyjnych inwestycje w tych obszarach muszą być finansowane przede wszystkim ze środków pochodzących ze źródeł publicznych.

Za uzupełnienie infrastruktury naziemnej służyć mogą technologie satelitarne, użyteczne szczególnie na obszarach o niskim zaludnieniu.

Należy mieć również na uwadze widoczny trend w zakresie konwergencji sieci naziemnych z nienaziemnymi, w szczególności satelitarnymi. Zakłada się, że sieci komórkowe kolejnej

generacji (6G) będą zintegrowane z sieciami satelitarnymi. Obecnie coraz częściej dochodzi do współpracy operatorów komórkowych z operatorami satelitarnymi odnośnie testowania możliwości odbioru sygnałów satelitarnych poprzez urządzenia mobilne. Po 2030 r. można spodziewać się w pełni zintegrowanych usług w urządzeniach końcowych. Oznacza to, że użytkownicy będą mieli możliwość dostępu do usług telekomunikacyjnych niezależnie od miejsca przebywania. Konwergencja sieci umożliwi również dalszy rozwój usług typu IoT oraz usług autonomicznych, w szczególności związanych z transportem.

Łączność satelitarną należy też uznać za zasób podwójnego zastosowania (cywilny i wojskowy), który w przypadku potencjalnego zagrożenia umożliwia reakcję na trudne do przewidzenia sytuacje oraz dostarczenie informacji na czas. Dlatego też, w perspektywie długofalowej, należy rozważyć budowanie i rozwijanie krajowych zdolności w obszarze łączności satelitarnej. Da to dalsze możliwości rozwoju bezpiecznej łączności państwowej, na potrzeby cywilne i militarne.



Cel 1: Wszyscy użytkownicy na terenie kraju mają dostęp do ultraszybkich usług telekomunikacyjnych – mobilnych i stacjonarnych.

Co umożliwi realizację celu:

- a) Kontynuacja wsparcia finansowego dla przedsiębiorców telekomunikacyjnych dla rozwoju infrastruktury, szczególnie na obszarach tzw. białych plam – terenach problematycznych z punktu widzenia dostępności, ukształtowania terenu i gęstości zaludnienia;
- b) Wykorzystanie alternatywnych technologii do zapewnienia łączności w najtrudniejszych inwestycyjnie obszarach, gdzie nie ma możliwości uzyskania przepustowości gigabitowych za pomocą technologii przewodowych;
- c) Likwidowanie barier prawnych i systemowych dla rozwoju sieci telekomunikacyjnych poprzez nowelizację tzw. Megaustawy¹⁷, która obejmować będzie zidentyfikowane zarówno przez resort cyfryzacji, jak i zgłaszane przez branżę telekomunikacyjną bariery inwestycyjne. Ponadto, wdrożenie do polskiego porządku prawnego postanowień rozporządzenia unijnego Gigabit Infrastructure Act (GIA)¹⁸ w celu wsparcia rozwoju publicznych sieci telekomunikacyjnych przewidującego uruchomienie m. in. otwartego pojedynczego punktu informacyjnego („jedno okienko”), w którym każdy operator ma prawo składać, również w formie elektronicznej, wnioski o udzielenie wszelkich niezbędnych zezwoleń inwestycyjnych lub o odnowienie zezwoleń lub udzielenie prawa drogi oraz uzyskuje informacje o statusie swojego wniosku;
- d) Zapewnienie jednostkom samorządu terytorialnego wsparcia merytorycznego w prowadzeniu procesów inwestycyjnych w obszarze telekomunikacji i wyznaczenie koordynatorów szerokopasmowych we wszystkich gminach i powiatach do 2026 r.;
- e) Kontynuowanie projektów edukacyjno-informacyjnych dotyczących roli infrastruktury telekomunikacyjnej (stacjonarnej i mobilnej – w tym 5G i 6G) dla rozwoju społeczno-gospodarczego kraju oraz przeciwdziałanie dezinformacji w zakresie sieci mobilnych;
- f) Utrzymanie i rozwój portalu internet.gov.pl (SIDUSIS) dostarczającego każdemu w łatwej i dostępnej formie informacji o dostępności usług dostępu do internetu w danym punkcie adresowym;
- g) Utrzymanie i rozwój portalu SI2PEM w celu zapewnienia dostępności wiedzy o poziomach PEM (poła elektromagnetycznego) oraz popularyzacji tej wiedzy w

¹⁷ Ustawa z dnia 7 maja 2010 r. o wspieraniu rozwoju usług i sieci telekomunikacyjnych (Dz. U. z 2024 r. poz. 604, z późn. zm.)

¹⁸ <https://eur-lex.europa.eu/legal-content/PL/TXT/?uri=CELEX:32024R1309>

celu rozwoju sieci ruchomej oraz niwelowania obaw o wpływ infrastruktury sieci ruchomej na zdrowie i środowisko;

- h) Wspieranie rozwoju samorządowych i prywatnych sieci 5G – prowadzenie działań o charakterze informacyjnym, w tym przygotowywanie publikacji, broszur, raportów, a także organizacja szkoleń dotyczących wdrażania technologii 5G oraz promowanie innowacji – startupów i firm pracujących nad rozwiązaniami wdrażającymi 5G;
- i) Zagwarantowanie odpowiedniej jakości sieci telekomunikacyjnych – wdrożenie narzędzi systemowych i technicznych w celu pomiaru parametrów usług telekomunikacyjnych, a także wdrożenie skutecznych mechanizmów interwencyjnych w celu poprawy jakości usług telekomunikacyjnych.



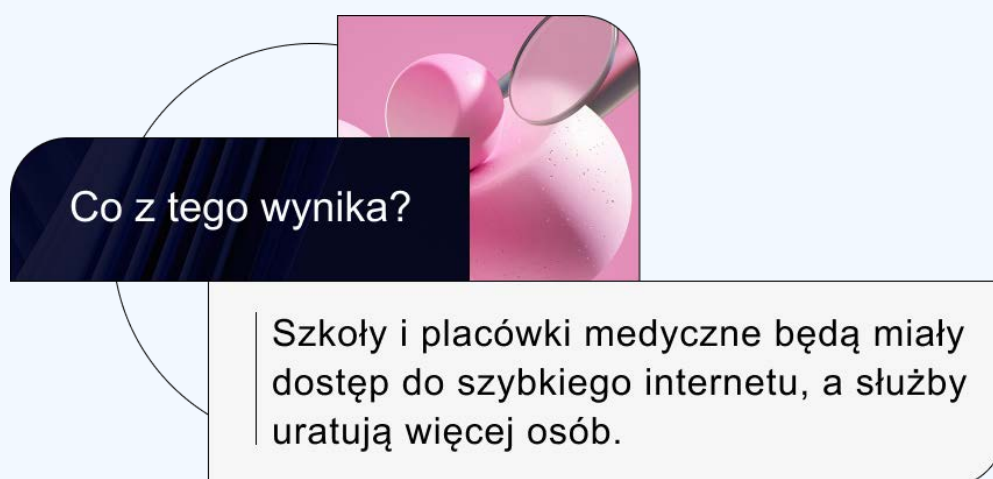
Co z tego wynika?

Gdziekolwiek mieszkaś,
będziesz mieć dostęp do
szybkiego i taniego internetu
i sieci komórkowej.

Cel 2: Bezpieczna łączność elektroniczna jest bezpłatna dla szczególnych grup użytkowników końcowych

Co umożliwi realizację celu:

- a) Zmodernizowanie Ogólnopolskiej Sieci Edukacyjnej (OSE) – zapewnienie szkołom dostępu do sieci umożliwiającej obsługę ruchu o przepustowościach gigabitowych, również w salach lekcyjnych. Włączenie do programu OSE przedszkoli, ośrodków doskonalenia nauczycieli, poradni psychologiczno-pedagogicznych, młodzieżowych ośrodków wychowawczych, młodzieżowych ośrodków socjoterapii, specjalnych ośrodków szkolno-wychowawczych, specjalnych ośrodków wychowawczych dla dzieci i młodzieży oraz ośrodków rewalidacyjno-wychowawczych.
- b) Budowa Ogólnopolskiej Sieci Medycznej – sieć zbudowana analogicznie do OSE, ale łącząca co najmniej szpitale oraz ważniejsze placówki ochrony zdrowia.
- c) Wdrożenie bezpłatnej dla użytkowników końcowych usługi Advance Mobile Location (AML) umożliwiającej precyzyjne lokalizowanie osób dzwoniących na numery alarmowe w oparciu o dane pochodzące z telekomunikacyjnego urządzenia końcowego w sieci ruchomej i przekazywane do regionalnych centrów powiadamiania ratunkowego z wykorzystaniem publicznej sieci ruchomej.



Cel 3: Usługi telekomunikacyjne są powszechnie wykorzystywane wśród społeczeństwa, administracji i biznesu

Co umożliwi realizację celu:

- a) Wprowadzenie programu tzw. bonów łączności – zestawu zachęt ekonomicznych dla użytkowników końcowych do korzystania z usług.
- b) Wsparcie finansowe i organizacyjne podmiotów zaangażowanych w wdrażania sieci ruchomych nowej generacji dzięki utworzeniu Funduszu Zastosowań Sieci Mobilnych (5G i 6G), w ramach którego możliwa będzie współpraca instytucji publicznych z instytutami badawczymi, uczelniami i przemysłem w celu rozwoju zastosowań dla sieci mobilnych wraz zapewnieniem odpowiednich środków na ten cel.



Cel 4: Cele transformacji cyfrowej państwa są wspierane przez suwerenny, bezpieczny system łączności satelitarnej

Co umożliwi realizację celu:

- a) Opracowanie, budowa i wyniesienie satelity telekomunikacyjnego na orbitę geostacjonarną oraz konstelacji satelitów komunikacyjnych łączności szerokopasmowej o wysokiej przepustowości na niskiej orbicie okołoziemskiej. Zdolności satelitarne powinny być w pełni programowalne, wyposażone w możliwości sterowania transmisją radiową w zakresie przepustowości i pokrycia oraz posiadać łączność laserową między sobą na różnych orbitach;
- b) Opracowanie i budowa demonstratora technologii dla systemu GOVSATCOM w zakresie świadczenia usług łączności satelitarnej dla administracji publicznej, służb odpowiedzialnych za zarządzanie kryzysowe i bezpieczeństwo;
- c) Nowe inwestycje i innowacje dla rozwoju i rozbudowy krajowego potencjału w zakresie szybkiej telekomunikacji, opartej na satelitach i naziemnej infrastrukturze dla świadczenia przez operatorów efektywnych kosztowo, wysokiej jakości telekomunikacyjnych usług szerokopasmowych;
- d) Opracowanie i budowa demonstratora technologii (docelowo konstelacji satelitarnej na niskiej orbicie okołoziemskiej z możliwością komunikacji z satelitą na orbicie geostacjonarnej) w zakresie wykorzystania innowacyjnych możliwości technologicznych dla bezpiecznej transmisji i przechowywania danych w przestrzeni kosmicznej.



1.2 Kompetencje przyszłości

Diagnoza – jak jest?

Szeroko pojęte kompetencje przyszłości mają fundamentalne znaczenie dla rozwoju sfery cyfrowej w państwie. Obywatele muszą nie tylko umieć korzystać z technologii cyfrowych, ale także robić to w zdrowy sposób, znać zasady higieny cyfrowej czy umieć rozpoznać dezinformację. Same zaś kompetencje cyfrowe są kluczowe dla efektywności, innowacyjności i konkurencyjności polskiej gospodarki. Według danych Eurostatu¹⁹, w 2023 r. tylko 44% polskich obywateli posiadało co najmniej podstawowe (średnia UE - 56%), a 20% – ponadpodstawowe umiejętności cyfrowe (średnia UE - 27%).

Deficyt kompetencji cyfrowych jest przede wszystkim widoczny wśród osób starszych (w wieku 65-74 lata), gdzie 87% nie posiadało nawet podstawowych umiejętności cyfrowych (średnia UE - 72%) i w grupie wiekowej 55–64 lat, w której takie osoby stanowiły 76% (średnia UE - 56%), podobnie jak wśród rolników i osób z niepełnosprawnościami - 77%. Odnotowano także spore dysproporcje wśród osób zamieszkujących miasta i wieś: odsetek mieszkańców terenów wiejskich z co najmniej podstawowymi kompetencjami cyfrowymi wyniósł 33% (średnia UE - 47%), o 22 punkty procentowe mniej niż w przypadku osób zamieszkujących miasta. Kompetencje cyfrowe powinny umożliwić obywatelom zrozumienie i odnalezienie się w środowisku wykorzystującym technologie w niemal każdym aspekcie życia. Osoby o niskich umiejętnościach cyfrowych znacznie bardziej narażone są na dezinformację i nieumiejętne weryfikowanie informacji otrzymanych drogą cyfrową.

W 2023 r. udział specjalistów ICT w ogólnej liczbie pracujących w Polsce wyniósł 4,3% (średnia UE - 4,8%)²⁰. Wobec przewidywanego wzrostu popytu na tę kategorię pracowników oraz planowanego dla UE w ramach Cyfrowej Dekady na 2030 r. odsetka 10%, należy uznać, że stan ten jest niesatysfakcjonujący.

Kobiety w Polsce, podobnie jak w UE, stanowiły 19% w grupie specjalistów ICT²¹. Ten brak równowagi działa na niekorzyść samych kobiet, jak też sektora ICT i gospodarki. Jak wynika z danych, polski system edukacji nie gwarantuje uzyskania przez absolwentów szkół średnich podstawowego poziomu kompetencji cyfrowych - w 2023 r. co najmniej podstawowe umiejętności cyfrowe posiadało tylko 58% osób w wieku 16-19 lat (średnia

19 Eurostat:

https://ec.europa.eu/eurostat/databrowser/view/isoc_sk_dskl_i21/default/table?lang=en&category=isoc.isoc_sk.isoc_sku

20 Eurostat:

https://ec.europa.eu/eurostat/databrowser/view/isoc_sks_itspt/default/table?lang=en&category=isoc.isoc_sk.isoc_sks.isoc_skslf

21 Eurostat:

https://ec.europa.eu/eurostat/databrowser/view/isoc_sks_itsps/default/table?lang=en&category=isoc.isoc_sk.isoc_sks.isoc_skslf

unijna 66%)²². Kształcenie na poziomie wyższym nie zapewnia stosownego do potrzeb dopływu specjalistów ICT - w 2022 r. tylko 4,3% wszystkich absolwentów (średnia UE - 4,5%) kończyło naukę w dziedzinie ICT²³. Udział kobiet wśród absolwentów ICT wyniósł 22% (średnia UE – 21%)²⁴. W kontekście wsparcia innowacji cyfrowych przez absolwentów szkół wyższych należy również wziąć pod uwagę kształcenie w obszarach STEM, technologii przełomowych i na kierunkach wspierających ich rozwój.

Brakuje systemowego rozwiązania dotyczącego podnoszenia kompetencji cyfrowych pracowników administracji publicznej, dzięki któremu podniósłby się poziom świadczenia usług e-administracji i poziom satysfakcji obywateli.



22 Eurostat:

https://ec.europa.eu/eurostat/databrowser/view/isoc_sk_dskl_i21__custom_12512302/default/table?lang=en&page=time:2023

https://ec.europa.eu/eurostat/databrowser/view/educ_uoe_grad02__custom_12849024/default/table?lang=en

23 Eurostat:

https://ec.europa.eu/eurostat/databrowser/view/educ_uoe_grad03__custom_12512661/default/table?lang=en

24 Eurostat:

https://ec.europa.eu/eurostat/databrowser/view/educ_uoe_grad03__custom_12512714/default/table?lang=en

Cel 1: Co najmniej 85% polskiego społeczeństwa posiada przynajmniej podstawowe umiejętności cyfrowe, a 50% umiejętności ponadpodstawowe

Co umożliwi realizację celu:

- a) Zapewnienie osobom dorosłym, zgodnie z ich potrzebami, możliwości rozwoju umiejętności cyfrowych w tworzonych w zainteresowanych gminach Klubach Rozwoju Cyfrowego (KRC). Każdy dorosły będzie mógł skorzystać z zajęć organizowanych w KRC oraz z porad edukatorów zatrudnionych w klubach;
- b) Inicjowanie działań wspierających osoby z niepełnosprawnościami, obejmujących: wsparcie finansowe w zakupie sprzętu niezbędnego do nabycia kompetencji cyfrowych; organizowanie szkoleń dedykowanych dla osób z niepełnosprawnościami; wsparcie organizacji non-profit w realizacji działań na rzecz podnoszenia kompetencji cyfrowych wśród osób z różnymi niepełnosprawnościami i szczególnymi potrzebami;
- c) Motywowanie społeczeństwa do poszerzania kompetencji cyfrowych poprzez wskazywanie korzyści i możliwości, jakie daje ich posiadanie. Odpowiednie kampanie będą prowadzone zarówno na poziomie ogólnopolskim, jak i lokalnym;
- d) Zapewnienie dostępu do szkoleń, także zakończonych ewaluacją zdobytych kompetencji np. w modelu mikropoświadczeń oraz materiałów edukacyjnych na portalu www.kompetencjegyfrowe.gov.pl, na którym zmapowane zostaną miejsca w sieci, wydarzenia oraz materiały do rozwijania kompetencji cyfrowych;
- e) Budowanie świadomości w zakresie bezpiecznego poruszania się w świecie cyfrowym. Będzie się ono opierać na profilaktyce cyberprzemocy i uzależnień, szerzeniu świadomości zagrożeń i umiejętności reagowania na nie, promowaniu świadomego korzystania z technologii cyfrowych (w tym AI), akcentowaniu konieczności krytycznego myślenia i stosowania zasad higieny cyfrowej, rozwiązywaniu kwestii etycznych pojawiających się wraz z rozwojem AI oraz wyposażaniu społeczeństwa w kompetencje odpowiednie do bezpiecznego i satysfakcjonującego funkcjonowania w świecie cyfrowym;
- f) Systemowe przeciwdziałanie dezinformacji połączone ze zwiększaniem świadomości obywateli o działaniu mechanizmów dezinformacji, rozwijanie kompetencji krytycznego myślenia umiejętności weryfikacji informacji i korzystania z mediów na wszystkich poziomach kształcenia;
- g) Współpraca, mobilizowanie i aktywizowanie podmiotów tworzących ekosystem rozwoju kompetencji cyfrowych w Polsce tj. organizacji non-profit, przedsiębiorstw, placówek edukacyjnych, kulturalnych, partnerów społecznych, administracji publicznej itp.
- h) Zapewnienie uczniom takiego rozwoju kompetencji cyfrowych, aby każdy uczeń posiadał przynajmniej podstawowe, a najlepiej ponadpodstawowe umiejętności

cyfrowe, zgodnie z Polityką Cyfrowej Transformacji Edukacji. System edukacji cyfrowej ma być wspierany dzięki odpowiednio przygotowanej kadrze pedagogicznej i w warunkach aktualnie najlepszych rozwiązań technologii cyfrowych.

Co z tego wynika?

Twoja gmina będzie mogła utworzyć Klub Rozwoju Cyfrowego, a Twoi bliscy czy znajomi będą mogli w nim lepiej poznać cyfrowy świat.



Cel 2: Liczba specjalistek i specjalistów w sektorze ICT odpowiada zapotrzebowaniu polskiej gospodarki

Co umożliwi realizację celu:

- a) wspieranie uczniów, w szczególności dziewcząt, w rozwoju zainteresowań informatyką, inicjowanie programów wspierających rozwój kompetencji w nowych obszarach technologii przełomowych, m.in. AI i technologii kwantowych oraz rozszerzenie Programu Rozwoju Talentów Informatycznych na szkoły podstawowe i uzupełnienie go o komponent technologii przełomowych. Dodatkowym elementem będą działania promocyjne skierowane do rodziców, uczniów i nauczycieli;
- b) Niwelowanie barier ograniczających obecność kobiet w ICT, promowanie kierunków kształcenia i zawodów ICT, a także zwalczanie stereotypów hamujących dopływ kobiet do zawodów cyfrowych;
- c) Prowadzenie kampanii informacyjnych przedstawiających możliwe ścieżki kariery w obszarze ICT;
- d) Stworzenie mechanizmu nowoczesnych szkoleń i szybkich ścieżek umożliwiających chętnym przebranżowienie do zawodu specjalisty ICT;
- e) Inicjowanie projektów wspierających rozwój zaawansowanych kompetencji w zakresie nowych technologii cyfrowych dla pracowników, w szczególności sektora MŚP, przemysłu i usług;
- f) Zwiększenie liczby absolwentów kierunków STEM ze szczególnym uwzględnieniem kierunków koniecznych dla rozwoju technologii przełomowych oraz liczby przeprowadzonych doktoratów w środowisku akademickim w specjalizacjach STEM;
- g) Zwiększenie liczby interdyscyplinarnych specjalistów oraz ekspertów w dziedzinach AI/STEM/ICT, łączących te obszary z innymi kierunkami niezbędnymi dla rozwoju technologii przełomowych;
- h) Monitorowanie udziału kobiet w ICT, a także zmian świadomości i postaw związanych z wizerunkiem przedmiotów ścisłych, zawodów ICT i rolami płciowymi oraz rolą kobiet w ICT.

Cel 3: Na wszystkich poziomach kształcenia dostępna jest efektywna i wysokiej jakości edukacja cyfrowa, uwzględniająca potrzeby osób z grup szczególnie wrażliwych

Co umożliwi realizację celu:

- a) Podniesienie jakości kształtowania kompetencji cyfrowych młodego pokolenia zarówno przez rozwój dydaktyki cyfrowej, dostosowanie podstawy programowej do postępu technologicznego oraz metodycznego, jak i przygotowanie nauczycieli do realizacji zajęć zgodnie z obowiązującą podstawą programową oraz metodyką wykorzystywania nowych technologii w nauczaniu;
- b) Podniesienie kwalifikacji cyfrowych oraz kompetencji w zakresie sztucznej inteligencji (AI) wśród wszystkich nauczycieli, wykładowców, pracowników akademickich i naukowych;
- c) Zamawianie studiów (także podyplomowych i dokształcających) w zakresie nauczania informatyki, kompetencji cyfrowych nauczycieli oraz wykorzystania nowoczesnych metod nauczania z zastosowaniem technologii cyfrowych;
- d) Wykorzystanie technologii cyfrowych w szkołach do podnoszenia jakości kształcenia, zerwania z podającą formą przekazywania wiedzy, do wspomagania pracy zespołowej, realizacji zespołowych projektów, grywalizacji oraz zapewnienia kontaktu z najnowocześniejszymi technologiami cyfrowymi jak np. AI, roboty, mikrokontrolery, drukarki 3D, VR/AR (wirtualnej/rozszerzonej rzeczywistości) itp.;
- e) Wprowadzenie do podstawy programowej kształtowania umiejętności bezpiecznego korzystania z e-usług publicznych i prywatnych (z obszaru zdrowia, nauki, administracji, komunikacji, finansów, zasobów kultury itp.) oraz tematów związanych ze sztuczną inteligencją – tłumaczenie jej funkcjonowania, programowanie, sposoby bezpiecznego, etycznego i odpowiedzialnego korzystania z tej technologii;
- f) Wprowadzenie tematów związanych z dezinformacją, myśleniem krytycznym, umiejętności korzystania z mediów i weryfikacji informacji do programów nauczania w szkołach oraz w programach kształcenia i doszkalania kadry dydaktycznej;
- g) Wprowadzenie do podstawy programowej na wszystkich poziomach kształcenia zagadnień związanych z dostępnością cyfrową.



Co z tego wynika?


Polska szkoła przygotuje uczniów do samodzielnego i bezpiecznego korzystania z technologii cyfrowych oraz będzie wspierała wykrywanie i rozwój talentów informatycznych.



Cel 4: Pracownicy administracji publicznej posiadają kompetencje cyfrowe niezbędne do świadczenia e-usług publicznych o najwyższym poziomie dojrzałości oraz efektywnego działania administracji.

Co umożliwi realizację celu:

- a) Zapewnienie dostępu do wysokiej jakości szkoleń, warsztatów praktycznych oraz pakietów kursów e-learningowych, zakończonych ewaluacją zdobytych kompetencji np. w modelu mikroświadczeń, m.in. w obszarach świadczenia cyfrowych usług publicznych, identyfikacji elektronicznej, zarządzania cyfryzacją, cyfryzacji procesów, cyberbezpieczeństwa, sztucznej inteligencji, systemów chmurowych, zarządzania i analizy danych oraz otwierania danych, inteligentnych miast i wsi (smart city i smart village), open-source (otwarte oprogramowanie) w administracji, zarządzania dostępnością cyfrową i jej wdrażaniem itp.;
- b) wprowadzenie systemowego wsparcia dla pracowników administracji chcących się przekwalifikować do zawodu specjalisty ICT;
- c) wprowadzenie w administracji publicznej prymatu kształcenia własnych kadr w obszarach zdiagnozowanych potrzeb ICT (np. cyberbezpieczeństwo, sztuczna inteligencja).



Co z tego wynika?

Dzięki zwiększeniu własnych kompetencji, urzędnicy skuteczniej pomogą rozwiązać Twoją sprawę.

Cel 5: Wiedza, umiejętności i świadomość polskiego społeczeństwa odpowiadają wyzwaniom i trendom towarzyszącym transformacji cyfrowej i zrównoważonemu rozwojowi.

Co umożliwi realizację celu:

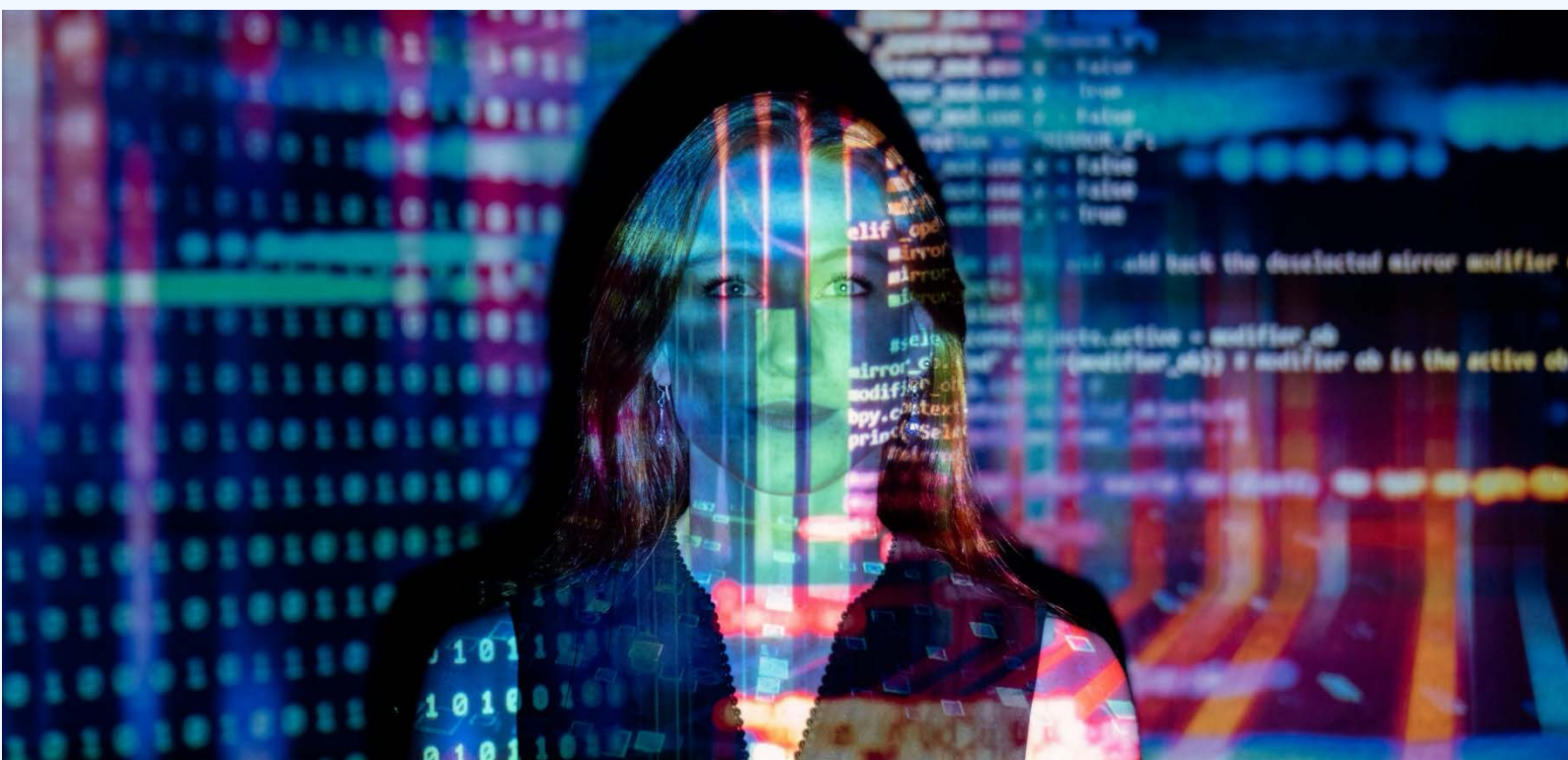
- a) Uwzględnianie w programach kształcenia kwestii wpływu korzystania z usług ICT na środowisko oraz edukowanie na temat tego, jak korzystać z technologii w sposób bardziej zrównoważony. Prowadzenie kampanii społeczno-edukacyjnych podnoszących świadomość w ww. obszarach;
- b) Zwiększanie poziomu edukacji społeczeństwa z zakresu technologii przełomowych, poprzez organizację szkoleń, warsztatów i edukację pozaformalną;
- c) Stworzenie planu komunikacji społecznej w mediach publicznych (w ramach misji publicznej) w celu rozwoju świadomości i wiedzy obywateli na temat zagadnień cyfrowych.



Cel 6: Polskie przedsiębiorstwa posiadają kompetencje cyfrowe kluczowe do efektywnego prowadzenia biznesu, utrzymania pozycji konkurencyjnej na rynku i strategicznego rozwoju firmy przy wykorzystaniu rozwiązań cyfrowych

Co umożliwi realizację celu:

- a) Wzmacnianie świadomości właścicieli przedsiębiorstw i ich pracowników o korzyściach z wdrożeń technologii o różnym poziomie i zastosowaniu, zależnych od potrzeb firmy, poprzez sprofilowane doradztwo eksperckie, dostęp do materiałów informacyjnych i edukacyjnych z zakresu transformacji cyfrowej i pakiet „Cyfrowego Startu dla Biznesu”;
- b) Budowanie zaufania do technologii cyfrowych poprzez wzmacnianie wiedzy o bilansie kosztów, korzyści i ryzyk z wdrożenia rozwiązań cyfrowych, cyberbezpieczeństwie oraz umiejętności krytycznej oceny jakości i wiarygodności źródeł informacji i identyfikacji dezinformacji;
- c) Niwelowanie obaw związanych z przestojami procesów w firmie i ryzykiem nietrafionych inwestycji w rozwiązania cyfrowe poprzez systemowe wsparcie obejmujące rzetelną diagnostykę, ocenę spodziewanych efektów i dobór najlepszych narzędzi do rozwoju cyfrowego firmy.



1.3 Cyberbezpieczeństwo

Diagnoza – jak jest?

Rosnący poziom zagrożeń w cyberprzestrzeni, nowe rodzaje zagrożeń i wzrost aktywności grup cyberprzestępczych, hakywistycznych i powiązanych z innymi państwami mają wpływ na codzienne funkcjonowanie obywateli, przedsiębiorstw i instytucji publicznych. Polska należy do krajów najczęściej atakowanych w cyberprzestrzeni, rokrocznie rośnie liczba cyberincydentów. Jest to związane m.in. rozprzestrzenianiem technologii (np. AI) umożliwiających dokonywanie cyberataków oraz coraz większe ucyfrowienie naszego codziennego życia oraz digitalizacja gospodarki i państw. Polska i inne państwa Zachodu są także celem działań hybrydowych Rosji, Białorusi i innych państw, których duża część ma miejsce w cyberprzestrzeni. W wymiarze wojskowym cyberprzestrzeń stała się domeną operacyjną na równi z lądem, morzem, powietrzem i kosmosem. Cyberbezpieczeństwo naszego kraju ma też fundamentalne znaczenie z uwagi na centralną rolę na wschodniej flance NATO.

Wojna Rosji z Ukrainą, w której Polska stanowi hub logistyczny wsparcia dla broniącej się Ukrainy, wiązała się z licznymi cyberatakami m.in. infrastrukturę transportową, co jest ważną lekcją w kontekście mobilności wojskowej i zdolności do kolektywnej obrony. Nie pozostajemy bierni wobec zagrożeń, ale aktywnie im przeciwdziałamy. Obejmuje to nie tylko zmiany systemowe, które wprowadzamy poprzez nowe akty prawne, ale także rozwijamy zdolności instytucji odpowiedzialnych za cyberbezpieczeństwo na poziomie krajowym, wyposażamy je w odpowiednie narzędzia techniczne, jak również dbamy o odpowiedni zasób specjalistów ds. cyberbezpieczeństwa (świadczenie teleinformatyczne w ramach Funduszu Cyberbezpieczeństwa) oraz powszechne szkolenia z higieny cyfrowej na wszelkich szczeblach.

Polska będzie nieustannie podejmować działania mające na celu systemowe zwiększanie poziomu cyberbezpieczeństwa krajowego i międzynarodowego, zwiększanie poziomu ochrony informacji, a także ograniczanie ryzyk związanych z cyberprzestrzenią.

Będziemy więc kompleksowo rozwijać krajowy system cyberbezpieczeństwa – poprzez zmiany legislacyjne, podnoszenie odporności i zdolności podmiotów tego systemu oraz wprowadzanie nowych mechanizmów koordynacji działań. Fundamentalną kwestią jest potrzeba powołania centralnej instytucji odpowiedzialnej za cyberbezpieczeństwo na poziomie krajowym. Kluczowe będą także upowszechnianie rozwiązań technicznych podnoszących cyberbezpieczeństwo, rozwój krajowego potencjału technologicznego i przemysłowego w obszarze cyberbezpieczeństwa oraz zwiększanie kompetencji

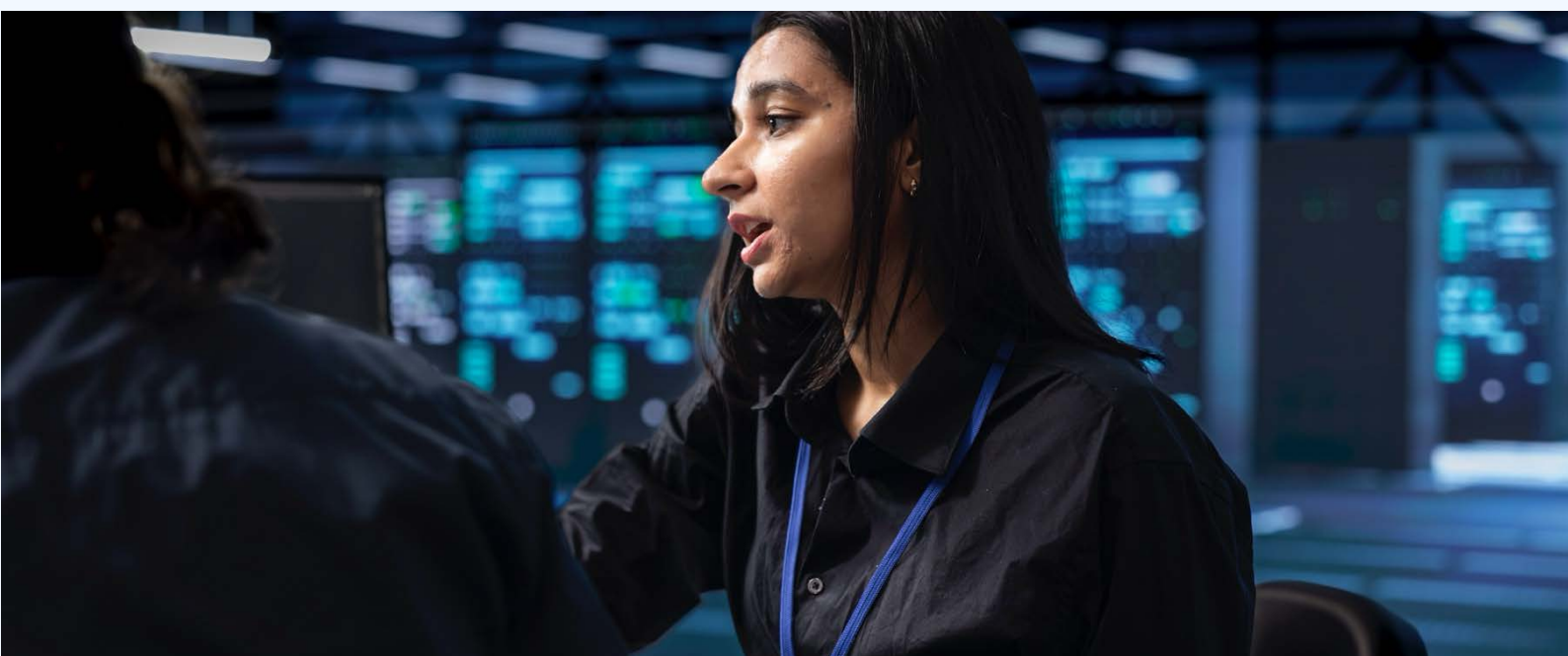
specjalistów oraz społeczeństwa jako całości. Działania na rzecz zwiększania poziomu cyberbezpieczeństwa muszą być podejmowane w ścisłej współpracy z odpowiednimi resortami i instytucjami państwa. Podobnie jest w przypadku zwalczania cyberprzestępczości, bez którego cyfryzacja się nie powiedzie. Za bardzo istotne należy uznać także działania mające na celu zapewnienie synergii między wojskowym a cywilnym wymiarem cyberbezpieczeństwa, a także między cyberbezpieczeństwem a zarządzaniem kryzysowym.



Cel 1: Funkcjonujący krajowy system cyberbezpieczeństwa jest dojrzały i efektywny.

Co umożliwi realizację celu:

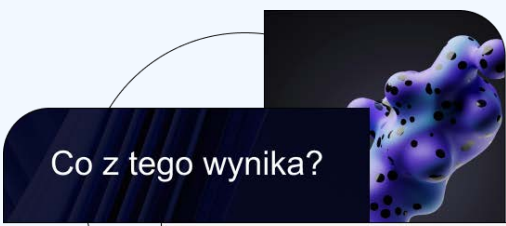
- a) Powołanie centralnej instytucji odpowiedzialnej za cyberbezpieczeństwo na poziomie krajowym i koordynującej działania innych podmiotów zapewniających cyberbezpieczeństwo na poziomie krajowym, dysponującej odpowiednią pozycją ustrojową, kompetencjami, zasobami osobowymi, budżetem i infrastrukturą;
- b) Wzmacnianie roli Pełnomocnika Rządu do Spraw Cyberbezpieczeństwa oraz Połączonego Centrum Operacyjnego Cyberbezpieczeństwa. Pozwoli to zwiększyć efektywność systemu i zapewni sprawniejsze reagowanie na zagrożenia w cyberprzestrzeni;
- c) Rozwijanie Systemu S46 jako podstawy wymiany informacji między podmiotami kluczowymi, ważnymi oraz instytucjami państwowymi;
- d) Wzmacnianie potencjału instytucji odpowiedzialnych za zapewnianie cyberbezpieczeństwa na poziomie krajowym, ze szczególnym uwzględnieniem zespołów reagowania na incydenty bezpieczeństwa komputerowego (CSIRT) poziomu krajowego;
- e) Tworzenie CSIRT-ów sektorowych i współpraca z sektorowymi centrami wymiany i analizy informacji;
- f) Udzielanie podmiotom krajowego systemu cyberbezpieczeństwa wsparcia w modernizacji i rozbudowie infrastruktury cyberbezpieczeństwa w sieciach IT, w tym jednostkom samorządu terytorialnego w budowie samorządowych struktur odpowiedzialnych za cyberbezpieczeństwo.



Cel 2: Systemy informacyjne w sferze publicznej (w tym militarnej) oraz prywatnej posiadają wysoki poziom odporności.

Co umożliwi realizację celu:

- a) Wprowadzenie mechanizmu uwzględniania w zamówieniach publicznych wymogów związanych z cyberbezpieczeństwem w odniesieniu do produktów ICT i usług ICT oraz specyfikacji tych wymogów;
- b) Wprowadzenie mechanizmu umożliwiającego wyłączenie pilnych zakupów związanych z cyberbezpieczeństwem spod wymogów prawa zamówień publicznych, co pozwoli uniknąć długotrwałych postępowań przetargowych negatywnie oddziałujących na cyberbezpieczeństwa państwa;
- c) Wprowadzenie skoordynowanych rozwiązań dotyczących zarządzania podatnościami, w tym ich identyfikowania, katalogowania i ujawniania;
- d) Rozwijanie krajowych rozwiązań i standardów kryptograficznych (w tym w zakresie kryptografii postkwantowej), a także inicjowanie programów i projektów badawczo-rozwojowych i innowacyjnych w tym zakresie, aby Polska dokonała bezpiecznej migracji do kryptografii postkwantowej oraz mogła wykorzystać technologie kwantowe na rzecz bezpieczeństwa państwa;
- e) Uruchomienie chmury do przetwarzania informacji niejawnych (chmury niejawnej);
- f) Rozwijanie zdolności w zakresie rozpoznawania zagrożeń w cyberprzestrzeni (ang. Cyber Threat Intelligence) oraz analityki i przewidywania rozwoju sytuacji w cyberprzestrzeni (ang. Cyber Foresight), tak by móc odpowiadać na aktualne wyzwania. Działania te będą mogły być wykorzystane na potrzeby zarządzania ryzykiem i wprowadzania mechanizmów korygujących cele operacyjne.



Co z tego wynika?

Opracujemy plan migracji do kryptografii postkwantowej, co zabezpieczy komunikację obywateli z instytucjami i firmami np. bankami), gdy nastanie „Dzień Q” – technologie kwantowe uzyskają dojrzałość pozwalającą na łamanie dotychczasowych metod szyfrowania.

Cel 3: Krajowa baza technologiczno-przemysłowa w obszarze cyberbezpieczeństwa posiada rozwinięty potencjał i cechuje się wysokim stopniem suwerenności technologicznej.

Co umożliwi realizację celu:

- a) Zwiększenie bezpieczeństwa łańcuchów dostaw w wymiarze krajowym i międzynarodowym (zarówno w wymiarze sprzętowym jak i oprogramowania), kierując się interesami bezpieczeństwa narodowego oraz polskiej gospodarki;
- b) Wykluczenie produktów ICT, rodzajów usług ICT lub konkretnych procesów ICT pochodzących od dostawców wysokiego ryzyka (wykorzystując mechanizm prawny z ustawy KSC);
- c) Rozwijanie krajowego systemu certyfikacji cyberbezpieczeństwa, zapewniającego procedury niezbędne do prawidłowości procesów certyfikacyjnych;
- d) Realizacja programów i projektów badawczo-rozwojowych i innowacyjnych w dziedzinie cyberbezpieczeństwa, które pozwolą na budowę krajowych kompetencji technologicznych i przemysłowych oraz zwiększenie suwerenności technologicznej Polski;
- e) Realizacja inicjatyw wykorzystujących technologie przełomowe (w tym sztuczną inteligencję) na potrzeby cyberbezpieczeństwa;
- f) Realizacja programów i projektów badawczo-rozwojowych oraz innowacyjnych w dziedzinie cyberbezpieczeństwa, które pozwolą na zabezpieczenie modeli i systemów AI wdrażanych w Polsce.



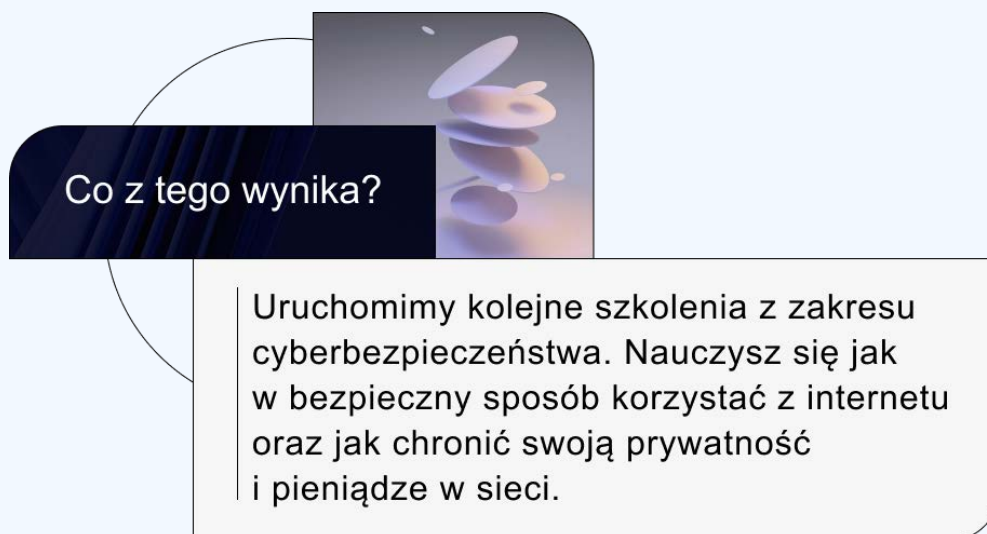
Co z tego wynika?

Umożliwimy wykluczanie dostawców wysokiego ryzyka w przypadku zidentyfikowania zagrożeń dla bezpieczeństwa państwa. Tym samym zapewnimy obywatelom dostęp do bezpiecznych i pewnych produktów, usług i procesów ICT.

Cel 4: Kadry podmiotów krajowego systemu cyberbezpieczeństwa oraz społeczeństwo posiadają świadomość cyberzagrożeń oraz wiedzę i kompetencje w zakresie cyberbezpieczeństwa.

Co umożliwi realizację celu:

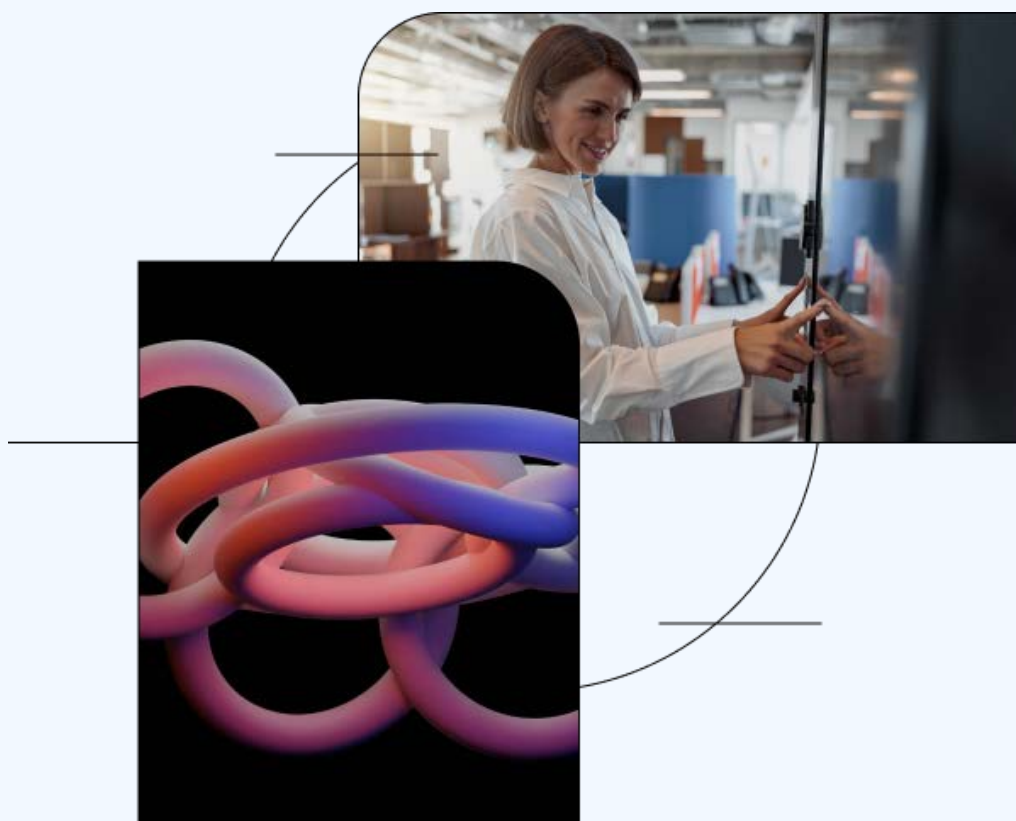
- a) Zwiększanie świadomości i wiedzy społeczeństwa z zakresu cyberbezpieczeństwa poprzez realizację działań w zakresie kształcenia i szkolenia w dziedzinie cyberbezpieczeństwa, podnoszenia umiejętności i świadomości, włączając w to dobre praktyki oraz higienę cyfrową;
- b) Wzmacnianie kompetencji kadr podmiotów krajowego systemu cyberbezpieczeństwa;
- c) Zapewnienie funkcjonowania Funduszu Cyberbezpieczeństwa i świadczeń teleinformatycznych.



Cel 5: Polska posiada silną pozycję międzynarodową w obszarze cyberbezpieczeństwa.

Co umożliwi realizację celu:

- a) Aktywna współpraca międzynarodowa na poziomie strategiczno-politycznym np. udział w pracach (również w wymiarze legislacyjnym) nad podnoszeniem poziomu cyberbezpieczeństwa w wymiarze międzynarodowym, pełnienie przez Polskę kluczowych ról w organizacjach międzynarodowych czy udział w inwestycjach międzynarodowych zwiększających cyberodporność;
- b) Aktywna współpraca międzynarodowa na poziomie operacyjnym oraz technicznym np. wielostronna wymiana informacji i doświadczeń oraz aktywny udział w ćwiczeniach;
- c) Koordynowanie przez Pełnomocnika Rządu do Spraw Cyberbezpieczeństwa działań na arenie międzynarodowej w zakresie współpracy cywilno-wojskowej w obszarze cyberbezpieczeństwa.



1.4 Koordynacja cyfrowej transformacji kraju

Diagnoza – jak jest?

Horyzontalny charakter procesów cyfryzacji sprawia, że nieodzowna jest efektywna międzyresortowa i ponadsektorowa współpraca oraz systematyzacja wiedzy na temat podejmowanych działań w różnych obszarach działalności państwa. Choć dotychczasowe inicjatywy w tym zakresie przyniosły pewną poprawę, to efektywne zarządzanie cyfryzacją wymaga większej koordynacji. Wciąż brakuje kompleksowej, spójnej i uporządkowanej informacji na temat stanu informatyzacji podmiotów publicznych i ich efektów. Ma to kluczowe znaczenie, ponieważ monitorowanie i kontrolowanie wdrażania projektów e-administracji w całym kraju poprawia skuteczność prowadzenia projektów, natomiast koordynacja wydatków na ICT pozwala na optymalizację kosztów i strategiczną priorytetyzację inwestycji w oparciu o potrzeby kraju. Pozwala jednocześnie na zwiększenie transparentności i odpowiedzialności w zakresie wydatków publicznych, a pośrednio przekłada się także na zwiększenie konkurencyjności kraju na arenie międzynarodowej.

Dla sprawnej koordynacji cyfrowej transformacji Polski istotny jest nie tylko wymiar wewnętrzny.

Konieczna jest także poprawa koordynacji w obszarze dyplomacji cyfrowej – nowego obszaru polityki zagranicznej państwa, związanego z szybkim rozwojem technologii cyfrowych i ich upowszechnieniem się w stosunkach międzynarodowych. Obszar ten obejmuje m.in. międzynarodowe zarządzanie sztuczną inteligencją i innymi technologiami cyfrowymi, przyciąganie inwestycji zagranicznych czy relacje państw z globalnymi korporacjami technologicznymi. W Polsce dyplomacja cyfrowa jest słabo rozwinięta – brakuje odpowiednich podstaw koncepcyjnych, koordynacji organizacyjnej czy spójnej krajowej strategii w tym obszarze. Skuteczna dyplomacja cyfrowa wymaga wspólnego działania resortów spraw zagranicznych, rozwoju i cyfryzacji.

Uznajemy, że jednym z filarów cyfrowej transformacji jest Architektura Informacyjna Państwa (AIP), metoda zarządzania informatyzacją państwa, oparta na modelach architektonicznych i obejmująca zasady podstawowe (pryncypia), standardy, wytyczne i rekomendacje architektoniczne, w tym dotyczące interoperacyjności, dostępności, zorientowania na użytkownika, reużywalności danych, komponentów technicznych, dokumentacji, doświadczeń. Kluczowe są zmiany w prawodawstwie, które mogą pomóc skutecznie wdrażać AIP, a także propagowanie jej znaczenia i celów oraz korzyści z jej stosowania, ponieważ deficyt wiedzy o AIP negatywnie wpływa na transformację cyfrową państwa.

Cel 1: Wymiana informacji na temat stanu cyfryzacji jednostek administracji publicznej oraz realizowanych przez nie przedsięwzięć informatycznych jest sprawna i efektywna

Co umożliwi realizację celu:

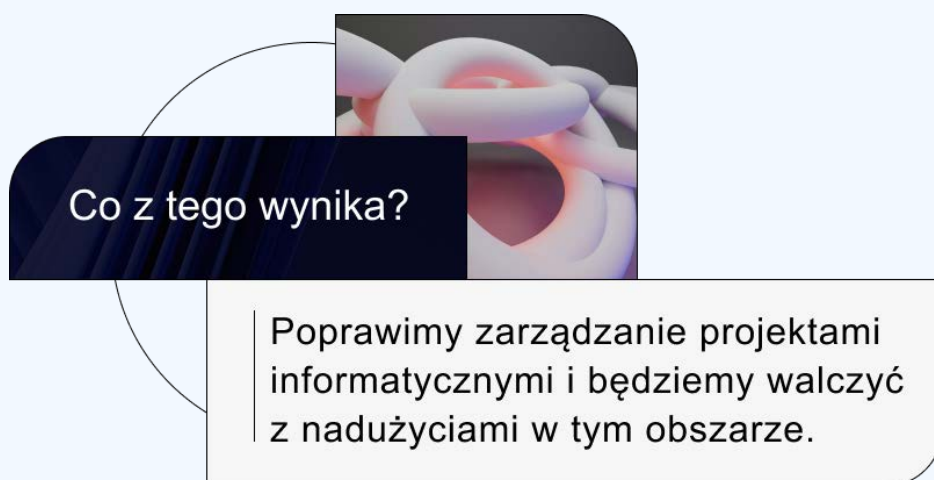
- a) działalność Komitetu do spraw Cyfryzacji, mającego szersze kompetencje niż dotychczas funkcjonujący Komitet Rady Ministrów ds. Cyfryzacji. KdsC ma zapewniać koordynację działań państwa związanych z informatyzacją oraz wsparcie cyfrowego rozwoju państwa. Jego zadania będą obejmowały rozpatrywanie projektów dokumentów rządowych związanych z informatyzacją, monitorowanie, opiniowanie i publikowanie informacji o przedsięwzięciach informatycznych o publicznym zastosowaniu, monitorowanie realizacji strategii i innych dokumentów o charakterze strategicznym związanych z informatyzacją;
- b) Działalność pełnomocników ds. informatyzacji, powoływanych w szczególności w ministerstwach oraz w Kancelarii Prezesa Rady Ministrów. Do ich podstawowych zadań będzie należało koordynowanie realizacji i wdrażania strategii w zakresie spraw należących do właściwości działu administracji rządowej, kierowanego przez właściwego ministra.



Cel 2: Projekty informatyczne są realizowane i zarządzane w sposób skoordynowany, przejrzysty i efektywny

Co umożliwi realizację celu:

- a) Wdrożenie wspólnej metodyki zarządzania przedsięwzięciami informatycznymi realizowanymi we wszystkich jednostkach administracji publicznej pozwalającej na efektywne monitorowanie ich postępów oraz efektów;
- b) Utworzenie i działalność repozytorium standardów prowadzenia przedsięwzięć, dokumentów funkcjonalnych i pozafunkcjonalnych;
- c) Pełne raportowanie dotyczące podmiotów i osób prowadzących przedsięwzięcia informatyczne dla państwa, które umożliwi zwiększenie przejrzystości i optymalizacji wydatkowania środków;
- d) Przeprowadzenie kompleksowej diagnozy efektywności udzielania i realizowania zamówień publicznych (perspektywa zamawiającego i wykonawcy) dotyczących przedsięwzięć informatycznych. Sprawdzi ona możliwość wprowadzenia szczególnych zasad dla tych przedsięwzięć w ramach prawa zamówień publicznych, poprzez bardziej elastyczne rozwiązania prawne uwzględniające konieczność modyfikacji i zmian technologicznych.



Cel 3: Architektura Informacyjna Państwa stanowi powszechną i ugruntowaną metodę strategicznego zarządzania informatyzacją państwa.

Co umożliwi realizację celu:

- a) Implementacja pryncypiów oraz opracowanie i implementacja standardów, wytycznych i rekomendacji architektonicznych w administracji publicznej, a także zobowiązanie podmiotów publicznych wdrażających e-usługi publiczne do ich stosowania;
- b) Wdrożenie przyjętej metody opisu AIP, w tym słownika pojęć, doprecyzowanie zakresu, dla którego metoda będzie stosowana oraz przygotowanie wizji AIP odwzorowującej pożądaną stan cyfryzacji kraju w zakresie realizacji e-usług publicznych. Celem wizji AIP jest zaprezentowanie uniwersalnego podejścia do planowania i efektywnego świadczenia e-usług publicznych z dużym naciskiem na niezbędną w tym zakresie interoperacyjność systemów teleinformatycznych;
- c) Aktualizacja metodyki modelowania oraz wzorcowych modeli AIP (metamodeli) w warstwach legislacyjnej, organizacyjnej, semantycznej i technicznej, umożliwiająca spójne i zintegrowane podejście do tworzenia i modyfikowania procesów oraz systemów teleinformatycznych realizujących cele strategii;
- d) Utrzymywanie w aktualności i rozbudowywanie repozytorium AIP, czyli systemu teleinformatycznego, w którym gromadzone są w szczególności modele architektoniczne oraz pryncypia, standardy, wytyczne i rekomendacje architektoniczne;
- e) Poszerzenie dostępu do informacji zgromadzonych w repozytorium AIP w zakresie dozwolonym ochroną danych (informacje udostępniane kontekstowo w odniesieniu do potrzeb poszczególnych interesariuszy) oraz kooperacja i wymiana bieżących informacji istotnych dla rozwoju i utrzymania AIP, w tym dotyczących identyfikowania reużywalnych komponentów z każdej warstw AIP;
- f) Analizowanie różnic pomiędzy stanem obecnym cyfryzacji kraju a docelową wizją określoną w AIP w celu definiowania przedsięwzięć informatycznych, których realizacja zwiększy efektywność transformację cyfrową kraju;
- g) Wdrożenie mechanizmów nadzoru i monitoringu wdrażania AIP, w tym:
 - powołanie we wszystkich resortach Głównych Architektów Korporacyjnych (których rolę będą mogli pełnić pełnomocnicy ds. informatyzacji) wspierających upowszechnianie, wdrażanie i rozwój AIP oraz biorących udział w pracach zespołu zadaniowego przy Komitecie do spraw Cyfryzacji wspierającego realizację zadań Komitetu w tym zakresie,
 - uzależnienie realizacji i finansowania przedsięwzięć informatycznych o publicznym zastosowaniu od pozytywnej oceny Komitetu do spraw Cyfryzacji

m.in. w szczególności w zakresie zgodności z pryncypiami, standardami, wytycznymi i rekomendacjami architektonicznymi Architektury Informacyjnej Państwa,

- objęcie obowiązkiem inwentaryzacji wszystkich systemów teleinformatycznych i rejestrów publicznych administracji publicznej, w tym systemów dziedzinowych np. księgowych, kadrowych, przy wykorzystaniu systemów inwentaryzacji systemów teleinformatycznych (SIST, SIST JST),
- weryfikowanie w ramach prac Komitetu do spraw Cyfryzacji zgodności projektów aktów prawnych z pryncypiami, standardami, wytycznymi i rekomendacjami architektonicznymi Architektury Informacyjnej Państwa.



Co z tego wynika?

W cyfryzacji administracji będzie przyświecała nam jedna, spójna wizja.



Cel 4: Dyplomacja cyfrowa jest skuteczna i efektywnie koordynowana.

Co umożliwi realizację celu:

- a) Opracowanie wspólnego dla administracji publicznej dokumentu strategicznego wyznającego cele i kierunki działania w obszarze dyplomacji cyfrowej. Selekcja priorytetowych organizacji międzynarodowych oraz państw i opracowanie „geograficznych” polityk cyfrowych zarysowujących plany działania w Ameryce Płn., Afryce i Azji;
- b) Rozwinięcie w urzędzie obsługującym ministra właściwego ds. informatyzacji kompetencji w zakresie pozyskiwania inwestycji zagranicznych w nowoczesne technologie w Polsce i promowania polskich technologii cyfrowych na świecie oraz przeznaczenie odpowiednich zasobów na ten cel. Pozwoli to m.in. na rozwijanie zdolności w zakresie zapewnienia suwerenności technologicznej w kooperacji z partnerami międzynarodowymi;
- c) Stworzenie w polskich placówkach dyplomatycznych i urzędach konsularnych w głównych ośrodkach cyfrowych na świecie attachatów cyfrowych, ewentualnie attachatów cyfrowo-technologiczno-naukowych, uwzględniających wspólny dla kilku resortów zakres właściwości;
- d) Regularne tworzenie, we współpracy z odpowiednimi resortami i instytucjami nadzorowanymi przeznaczonych dla polskich placówek dyplomatycznych materiałów z zakresu cyfrowych technologii i cyfrowej gospodarki. Mają one służyć podwyższaniu kompetencji personelu dyplomatycznego, promowaniu polskich rozwiązań technologicznych, wspierać współpracę międzynarodową z polskimi instytucjami i biznesem oraz ułatwiać pozyskiwanie inwestycji zagranicznych;
- e) Zapewnienie, by technologie cyfrowe w percepcji i działaniach placówek dyplomatycznych stanowiły odrębny zakres aktywności, niebędący podkategorią współpracy naukowej lub gospodarczej, przy jednoczesnej ścisłej korelacji z tymi obszarami współpracy.



Co z tego wynika?

Damy polskiej dyplomacji narzędzia i kompetencje do skutecznego przyciągania cyfrowych inwestycji i promowania polskich innowacji.



Państwo



Ministerstwo
Cyfryzacji

Tu tworzymy przyszłość

Państwo

2.1 E-usługi publiczne

Diagnoza – jak jest?

Kluczowym elementem rozwoju e-administracji są elektroniczne usługi publiczne (e-usługi publiczne), czyli usługi służące realizacji zadań publicznych za pomocą środków komunikacji elektronicznej. System e-usług publicznych w Polsce w ostatnich latach przeszedł zauważalną drogę rozwoju. Serwisy rządowe udostępniają obywatelom ponad 1700 e-usług na minimum 3 poziomie dojrzałości. Dotychczasowe działania koncentrowały się przede wszystkim na udostępnianiu jak największej ilości e-usług publicznych dla obywateli, przedsiębiorców i administracji publicznej mających przynieść wartość dodaną dla użytkownika. Obecne działania skupiają się na kreowaniu i udostępnianiu nowoczesnych e-usług na wyższym poziomie dojrzałości, opartych o istniejące mechanizmy i bazujących na systemach teleinformatycznych, rejestrach publicznych oraz platformach e-administracji.

Dzięki wzrastającej interoperacyjności podmiotom publicznym łatwiej jest uzyskiwać dostęp do danych gromadzonych od lat przez inne podmioty publiczne. Z tego względu uprawnienia i obowiązki wynikające z przepisów prawa mogą być obsługiwane bez konieczności tworzenia nowych elektronicznych usług publicznych na linii podmiot publiczny – usługobiorca. Jest to możliwe, ponieważ informacje niezbędne do ich realizacji znajdują się już w publicznych systemach teleinformatycznych i rejestrach publicznych.

Domyślnie stosowanym podejściem powinien być brak angażowania w realizację zadania publicznego podmiotu (w tym obywatela czy przedsiębiorcy), na którym ciąży obowiązek lub któremu przysługuje uprawnienie wynikające z przepisów prawa.

Skutkuje to oszczędnością czasu i większym poziomem satysfakcji wśród obywateli oraz przedsiębiorców. Oczywiście od takiego podejścia mogą istnieć uzasadnione wyjątki.

Aby elektroniczna realizacja usług publicznych nie sprawiała trudności użytkownikom, e-usługi publiczne powinny być zorientowane na użytkownika, czyli proste i zrozumiałe dla każdego obywatela, przedsiębiorcy i urzędnika. Prowadzenie spraw utrudnia również żargon

urzędniczy i techniczna terminologia, dlatego konieczne jest również powszechne stosowanie prostego i inkluzywnego języka.

Pomimo udostępnienia już wielu e-usług publicznych, wciąż istnieją bariery, które utrudniają ich dostępność, szersze rozpowszechnienie i efektywne wykorzystanie. Wśród nich można wymienić, m.in.:

- brak jednego punktu dostępu do e-usług publicznych dla obywatela, przedsiębiorców i administracji zapewniającego jednolity interfejs i sposób uwierzytelnienia użytkownika oraz zapewniającego funkcjonalności podpisu cyfrowego i pieczęci elektronicznej;
- wdrożenie różnorodnych narzędzi (platform) realizacji e-usług publicznych, które nie są zbudowane w oparciu o jednolite standardy umożliwiające uwzględnienie specyficznych potrzeb użytkowników e-usług, m.in.
 - a. narzędzi projektowania formularzy elektronicznych,
 - b. narzędzi pozwalających na przekształcenie zdefiniowanych i ustandaryzowanych procesów biznesowych będących podstawą realizacji e-usługi na aplikację wspomagającą jej realizację,
 - c. mechanizmów przesyłania dokumentów elektronicznych, oraz które nie wykorzystują rozwiązań horyzontalnych wspierających realizację e-usług publicznych, m.in. katalogów administracji publicznej, platform udostępniania rejestrów referencyjnych, systemów realizacji e-płatności lub repozytorium spraw;
- brak wspólnych dla administracji publicznej katalogów wspierających interoperacyjność organizacyjną, semantyczną i techniczną administracji publicznej (katalogów administracji publicznej), w tym katalogów procesów, spraw, e-usług publicznych, wzorów dokumentów, rejestrów, pełnomocnictw i upoważnień;
- ograniczony katalog e-usług publicznych umożliwiających załatwianie spraw w pełni on-line;
- niezintegrowane rejestry publiczne oraz systemy teleinformatyczne administracji publicznej, brak katalogu metadanych rejestrów publicznych oraz katalogu API (interfejsów programistycznych aplikacji) publicznych systemów teleinformatycznych, a także brak platform udostępniania publicznych rejestrów referencyjnych poprzez API zapewniających ich interoperacyjność, co wymusza m.in. wielokrotne wprowadzanie przez użytkownika danych będących w zasobach administracji publicznej;
- niewystarczający poziom otwartości danych oraz stosowania otwartych formatów wymiany danych, a także wykorzystania platform ich udostępniania w celu wsparcia realizacji e-usług publicznych;

- brak mechanizmów zarządzania i monitorowania realizacji e-usług publicznych w celu opracowywania kierunków zwiększania ich efektywności;
- brak e-usług publicznych akceptujących transgraniczne metody uwierzytelnienia;
- niewykorzystany potencjał nowych technologii w procesach tworzenia e-usług publicznych, w tym chmury obliczeniowej;
- wykluczenie cyfrowe części społeczeństwa utrudniające elektroniczną komunikację z administracją publiczną, np. poprzez nierówny dostęp do internetu, niedostosowanie e-usług do osób ze szczególnymi potrzebami czy osób starszych, niedostateczne umiejętności cyfrowe.



Cel 1: E-usługi publiczne są dostępne w jednym miejscu i uwzględniają potrzeby wszystkich użytkowników

Co umożliwi realizację celu:

- a) Wdrożenie jednego punktu dostępu do e-usług publicznych dla obywateli, przedsiębiorców i administracji. Zapewniać on będzie jednolity interfejs uspojnający dostępne kanały komunikacji realizacji e-usług;
- b) Prowadzenie badań potrzeb obywateli, przedsiębiorców lub administracji publicznej w zakresie nowych i modyfikacji istniejących e-usług publicznych. Pozwoli to na wskazywanie głównych kierunków tworzenia, rozwijania i optymalizowania rozwiązań cyfrowych wspierających realizację e-usług;
- c) Dostosowanie wymaganych i kluczowych e-usług publicznych do wymogów krajowego i europejskiego portfela tożsamości cyfrowej, będącej certyfikowanym, uznawanym środkiem identyfikacji elektronicznej na wysokim poziomie bezpieczeństwa;
- d) Wsparcie użytkownika e-usług publicznych i identyfikacja zgłaszanych przez niego potrzeb przy wykorzystaniu chatbota, wytrenowanego na danych pochodzących z obszarów administracji publicznej;
- e) Organizacja systemowego wsparcia podmiotów świadczących e-usługi publiczne w uspojnieniu działań w zakresie zapewnienia jednolitego dostępu do e-usług oraz środków identyfikacji elektronicznej.



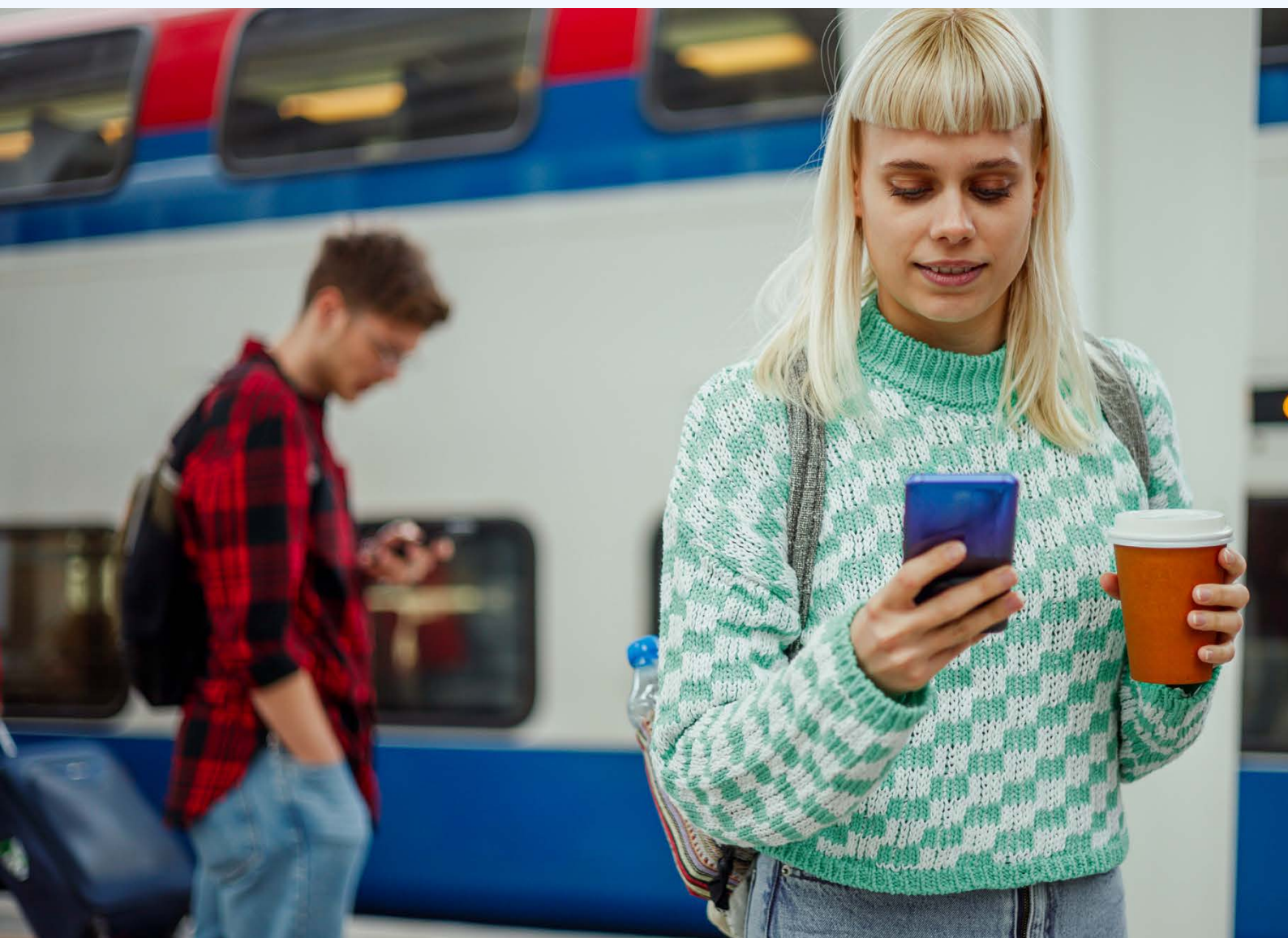
Cel 2: Wdrożone jednolite narzędzia służące realizacji e-usług publicznych ułatwiają interakcję podmiotów świadczących e-usługi z ich użytkownikami

Co umożliwi realizację celu:

- a) Budowa, udostępnienie i rozwój platform realizacji e-usług publicznych świadczonych na poziomie krajowym, w tym obszarowym, regionalnym i lokalnym, zapewniających standaryzację realizacji e-usług, ich bezpieczeństwo oraz wysoki poziom dojrzałości, w tym Systemu mObywatel;
- b) Zwiększenie zakresu e-usług publicznych świadczonych przy wykorzystaniu jednolitych platform realizacji e-usług;
- c) Wyposażenie platform w narzędzia pozwalające na automatyczne przekształcenie zdefiniowanych i ustandaryzowanych procesów biznesowych, będących podstawą realizacji e-usługi publicznej, na rozwiązania wspomagające jej realizację;
- d) Wyposażenie podmiotów świadczących e-usługi publiczne w generator formularzy - intuicyjne narzędzie do wsparcia samodzielnego wdrażania e-usług publicznych w jednym wspólnym standardzie, dzięki czemu będą one użyteczniejsze i bardziej przyjazne dla użytkownika;
- e) Wdrożenie funkcjonalności wspierających użytkownika w szybkim załatwieniu spraw online bez nadmiernego angażowania użytkownika;
- f) Wdrożenie mechanizmów bezpiecznego przesyłania dokumentów elektronicznych, w tym przy wykorzystaniu systemu e-Doręczeń;
- g) Wdrożenie funkcjonalności automatycznej obsługi spraw załatwianych w ramach realizacji e-usług publicznych, w tym w systemach elektronicznego zarządzania dokumentacją;
- h) Rozbudowę obecnego portfela wzorów dokumentów, umożliwiającego obywatelom posługiwanie się elektronicznymi wersjami dokumentów o charakterze krajowym, regionalnym, lokalnym i zawodowym;
- i) Zapewnienie dla platform e-usług publicznych odpowiedniej infrastruktury, która pozwoli zagwarantować wysoką jakość e-usług i wydajność systemów wspomagających ich realizację.

Co z tego wynika?

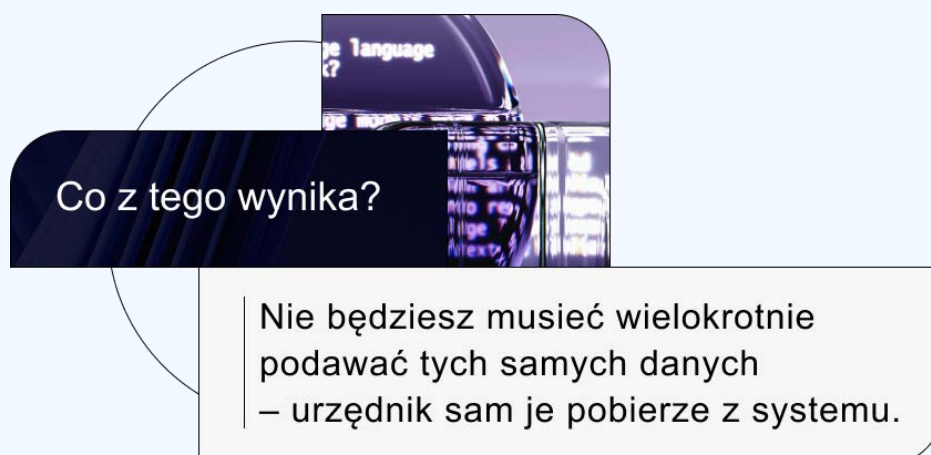
E-usługę zrealizujesz szybko i bezpiecznie – pobierzesz dokument z portfela wzorów dokumentów, bezpiecznie prześlesz dane dzięki systemowi e-Doręczenia, a Twoja sprawa zostanie możliwie automatycznie obsłużona przez urząd.



Cel 3: Rozwiązania horyzontalne zapewniają optymalizację świadczonych e-usług publicznych

Co umożliwi realizację celu:

- a) Wdrożenie rozwiązań horyzontalnych wspierających realizację e-usług publicznych, zapewniających w praktyce bezpieczeństwo oraz wysoki poziom dojrzałości świadczonych e-usług oraz zwiększoną interoperacyjność publicznych systemów teleinformatycznych i rejestrów publicznych wspomagających ich realizację, w tym:
- referencyjnych rejestrów publicznych Katalogów Administracji Publicznej, tj. Katalogu Procesów Administracyjnych, Katalogu Spraw, Katalogu Usług Publicznych, Katalogu Wzorów Dokumentów, oraz Katalogu Rejestrów Publicznych i Katalogu Podmiotów Publicznych, uspojnających i zwiększających efektywność działań podejmowanych przez administrację publiczną, w tym wobec obywateli i przedsiębiorców w ramach świadczenia lub realizacji e-usług publicznych;
 - krajowej platformy udostępniania danych, katalogu metadanych rejestrów publicznych i API publicznych systemów teleinformatycznych usprawniających wykorzystanie udostępnionych danych, w szczególności danych referencyjnych;
 - systemu obsługi e-płatności wspierającego realizację e-usług publicznych poprzez funkcjonalności obsługi rozrachunków i rozliczeń z obywatelem lub przedsiębiorcą, ze szczególnym uwzględnieniem administracji w ramach samorządów;
 - repozytorium spraw gromadzących informacje o załatwianych przez obywatela i przedsiębiorcę sprawach urzędowych, w tym o statusie tych spraw.



2.2 Cyfryzacja procesów administracyjnych i postępowań sądowych

Diagnoza – jak jest?

Cyfryzacja działania podmiotów publicznych jest procesem ciągłym i ewoluującym. Zależy od wielu czynników, takich jak możliwości technologiczne, potrzeby społeczeństwa, kompetencje cyfrowe obywateli i pracowników instytucji, uwarunkowania prawne. Dlatego też konieczne jest stałe monitorowanie poziomu cyfryzacji instytucji publicznych, analizowanie zjawisk warunkujących ten poziom i odpowiednie reagowanie na bariery we wdrażaniu rozwiązań cyfrowych.

Obecnie w sektorze publicznym funkcjonuje wiele systemów i miejsc, w których są gromadzone dane i załatwiane sprawy obywateli.

Warto wspomnieć o całkowitej cyfryzacji procesu wnioskowania o dokumenty paszportowe, stworzeniu systemu rejestrów państwowych, czy rozwoju systemów klasy EZD (elektronicznego zarządzania dokumentacją) wykorzystywanych w organach administracji publicznej jako narzędzia elektronicznego obiegu dokumentacji.

Niemniej ich potencjał nadal nie jest w pełni wykorzystany. Cyfrowa administracja w Polsce rozwijała się do tej pory w sposób niewystarczająco skoordynowany. Poszczególne podmioty samodzielnie tworzyły różne systemy teleinformatyczne, np. w celu zapewnienia e-usług publicznych, elektronicznego obiegu dokumentów, czy realizacji specyficznych dla danego podmiotu spraw. Taki stan rzeczy spowodował, że wydawano środki na budowę tych systemów i infrastrukturę, mimo dostępności np. platformy ePUAP. Efektem takiego stanu rzeczy jest to, że obywatel lub przedsiębiorca chcąc załatwić sprawę w sposób elektroniczny, musi używać kilku systemów teleinformatycznych niezależnie, a nawet posługiwać się dokumentami w postaci papierowej. Co więcej, obywatele i przedsiębiorcy często nie wiedzą, w którym miejscu, za pośrednictwem którego systemu e-usług publicznych mają załatwić swoją sprawę.

Dodatkowo, pomimo iż wskutek dotychczasowej cyfryzacji instytucji publicznych powstało wiele dużych, skomplikowanych systemów i rejestrów, to nadal występują obszary niezainformatyzowane, gdzie wymagana jest budowa i dostarczenie rozwiązań teleinformatycznych z poziomu centralnego.

Aż 63 proc. instytucji publicznych²⁵ wciąż funkcjonuje w oparciu o papierowy obieg dokumentów, a w obszarze cyfrowej transformacji instytucji publicznych widać wiele wyzwań.

Część z nich ma charakter systemowy, co uniemożliwia stawienie im czoła na poziomie poszczególnych instytucji. Tak jest m.in. w przypadku niedostatecznej integracji między publicznymi systemami teleinformatycznymi, braku zunifikowanych, ustandaryzowanych narzędzi elektronicznych dla realizacji zadań publicznych czy faktu, że część rejestrów publicznych wciąż jest prowadzona w postaci papierowej. Brak też standaryzacji wykorzystywanego przez administrację publiczną stosu technologicznego oraz komponentów architektury zorientowanej na usługi. Zarazem dostępność dostosowanej do potrzeb administracji, skalowalnej infrastruktury jest niska. Zróżnicowany poziom kompetencji urzędników oraz różnice w potencjalne finansowym instytucji publicznych przekładają się na nierównomierny poziom ich cyfryzacji. Tymczasem, wobec nieustającego postępu w sektorze informatycznym, konieczne jest ciągłe dostosowywanie publicznych systemów teleinformatycznych do nowoczesnych rozwiązań.

Działania te obniżą koszty realizacji procesów i ich obsługi w instytucjach publicznych np. poprzez wprowadzenie centralnych zamówień na usługi w zakresie chmury publicznej, dzięki którym jednostki korzystające z nich będą mogły nabywać usługi chmurowe w krótkim czasie przy znacznie mniejszym zaangażowaniu swoich urzędników.



²⁵ Informacja na podstawie badań własnych NASK: „Systemy klasy EZD w administracji publicznej - badanie samorządów”, marzec 2022; „Badanie potrzeb jednostek administracji rządowej w zakresie wdrożeń EZD”, październik 2023;

Cel 1: Procesy back-office w administracji publicznej są prowadzone cyfrowo

Co umożliwi realizację celu:

- a) Wdrożenie ujednoliconego sposobu opisu i ustandaryzowanych procesów oraz procedur dotyczących funkcjonowania administracyjnego zaplecza jednostek administracji publicznej, które wspomagają realizację głównych zadań dotyczących załatwiania spraw po stronie obywatela, przedsiębiorcy i administracji;
- b) Automatyzacja i optymalizacja wykonywania procesów administracyjnych, z wykorzystaniem referencyjnych procesów z Katalogu Procesów Administracyjnych, danych pozyskiwanych przez API publicznych systemów teleinformatycznych oraz rozwiązań sztucznej inteligencji - przy zachowaniu nadzoru i możliwości interwencji przez człowieka;
- c) Wprowadzenie obowiązku wdrożenia elektronicznego zarządzania dokumentacją przez podmioty publiczne przy użyciu systemów teleinformatycznych klasy EZD. Konieczna będzie też standaryzacja wymagań dla systemów klasy EZD oraz zapewnienie podmiotom publicznym wsparcia we wdrażaniu i utrzymaniu systemów;
- d) Nowelizacja przepisów kancelaryjno-archiwalnych oraz monitorowanie poziomu wykorzystania systemów klasy EZD w podmiotach realizujących zadania publiczne pod kątem redukcji spraw dokumentowanych papierowo;
- e) Rozwój i upowszechnianie bezpłatnej aplikacji EZD RP oraz udostępnienie usług chmurowej EZD RP na rzecz administracji państwowej, rządowej i samorządowej. Zapewnienie podmiotom publicznym wsparcia we wdrażaniu i utrzymaniu EZD RP oraz wsparcie procesu migracji do EZD RP;
- f) Ustawowe umocowanie systemu EZD RP oraz powołanie Operatora EZD odpowiedzialnego za rozwój systemu EZD RP, bezpłatne wsparcie wdrożeniowe i utrzymaniowe EZD RP świadczone na rzecz podmiotów realizujących zadania publiczne.
- g) Przyjęcie „Polityki wdrażania EZD w RP”, wyznaczającej planowany zakres działań w obszarze cyfryzacji back-office administracji publicznej do 2030 r.



Co z tego wynika?

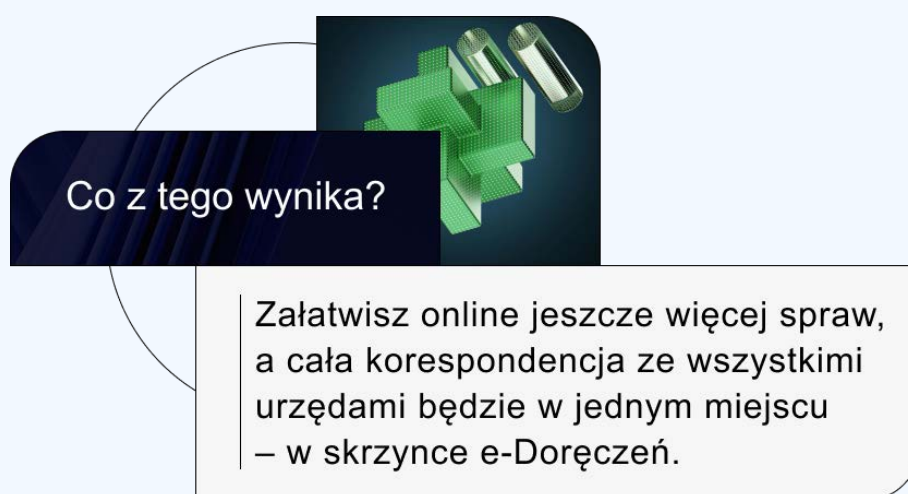
Komunikacja wewnątrz urzędów i pomiędzy nimi będzie uproszczona i bardziej efektywna, a praca urzędników łatwiejsza i szybsza.



Cel 2: Otoczenie prawne sprzyja informatyzacji podmiotów publicznych

Co umożliwi realizację celu:

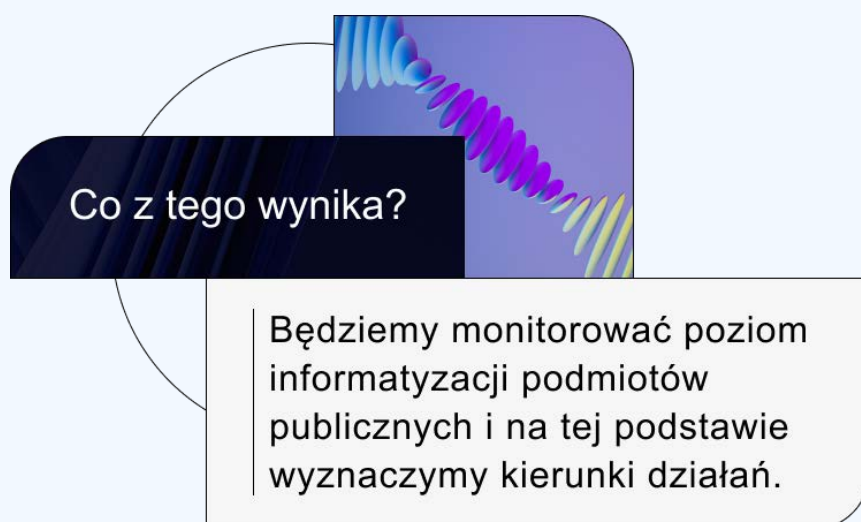
- a) Dostosowanie przepisów prawa do realizacji spraw urzędowych za pomocą środków komunikacji elektronicznej, w tym wprowadzenie domyślności cyfrowej w KPA (kodeksie postępowania administracyjnego), uproszczenie procedur administracyjnych oraz wprowadzanie elektronicznych wersji dokumentów. Ułatwi to znacznie użytkownikom komunikację z organami administracji publicznej i innymi podmiotami zewnętrznymi;
- b) Pełne wdrożenie i upowszechnienie elektronicznych doręczeń (e-Doręczeń) zarówno w relacjach z podmiotami publicznymi, jak i między podmiotami niepublicznymi;
- c) Wprowadzenie obowiązku integracji e-usług z e-Doręczeniami, co zapewni obywatelom jedno miejsce, w którym będą mieli zgromadzoną całą korespondencję z urzędami, bez względu na to, z którego serwisu udostępniającego e-usługi korzystali.



Cel 3: Monitorowanie informatyzacji podmiotów publicznych pozwala efektywniej kierować procesem wdrażania zmian w tym zakresie

Co umożliwi realizację celu:

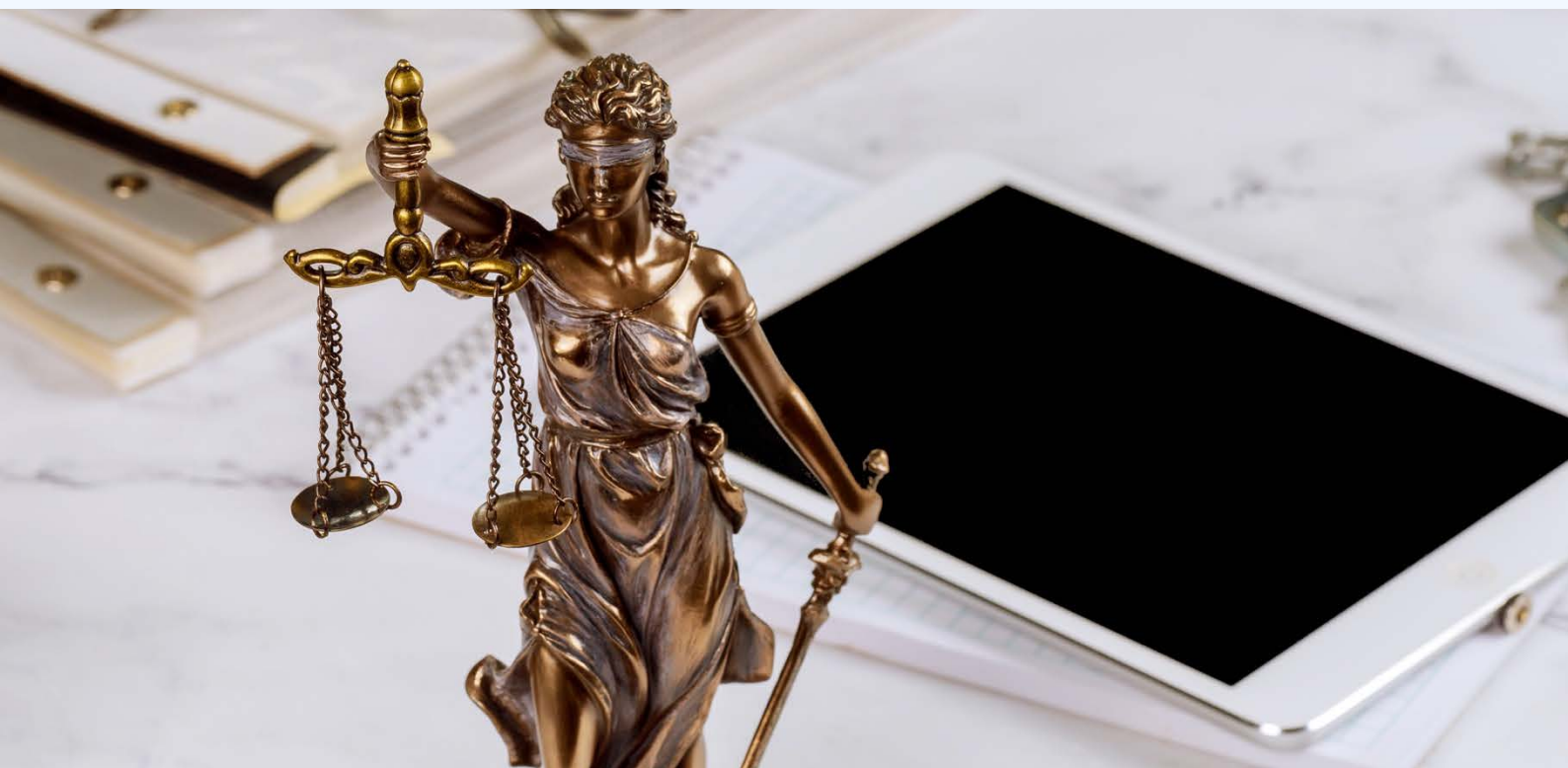
- a) Monitorowanie wdrażania w budowanych lub rozwijanych systemach teleinformatycznych, w tym wspierających realizację e-usług publicznych, rozwiązań horyzontalnych, w tym środków identyfikacji elektronicznej, platform udostępniania danych, systemów realizacji e-płatności i repozytorium spraw;
- b) Monitorowanie postępów i efektów realizowanych przedsięwzięć informatycznych o publicznym zastosowaniu w ramach prac Komitetu do spraw Cyfryzacji;
- c) Formułowanie wniosków z przeprowadzonego monitoringu działań podejmowanych w ramach informatyzacji podmiotów publicznych i weryfikacja przyjętych kierunków działań na tej podstawie.



Cel 4: Funkcjonowanie wymiaru sprawiedliwości usprawnione jest dzięki wykorzystaniu e-usług i nowoczesnych technologii

Co umożliwi realizację celu:

- a) Udostępnienie zaawansowanych e-usług z zakresu wymiaru sprawiedliwości wspieranych nowoczesnymi technologiami, pozwalających na elektroniczny dostęp do informacji i elektroniczne załatwienie spraw obywateli i przedsiębiorców ze zwiększeniem poziomu transparentności postępowania;
- b) Optymalizacja ekonomiki procesowej przy uwzględnieniu stosowania elektronicznych dokumentów, elektronicznych czynności procesowych czy przeprowadzania posiedzeń i rozpraw w formie wideokonferencji;
- c) Podniesienie komfortu i jakości pracy pracowników wymiaru sprawiedliwości poprzez automatyzację;
- d) Uzyskanie wysokiego poziomu interoperacyjności systemów wymiaru sprawiedliwości z systemami krajowym i międzynarodowymi z ich otoczenia pozwalający na wzmocnienie cyfrowej współpracy sądowej oraz dostępu do danych;
- e) Stworzenie narzędzia AI do tworzenia przejrzystego prawa.



2.3 Systemy i rejestry

Diagnoza – jak jest?

Systemy i rejestry wykorzystywane przez administrację publiczną nie są w pełni interoperacyjne. Znaczna część danych jest bez potrzeby gromadzona wielokrotnie, co sprawia, że podmioty publiczne napotykają wiele barier, które utrudniają optymalne rozwiązania dla realizacji zadań publicznych. Liczne niezgodności danych w różnych rejestrach powodują trudności w zidentyfikowaniu zasobów, które są już dostępne w systemach administracji i podmioty publiczne mogłyby z nich korzystać. Instytucje publiczne mają wciąż niewystarczającą wiedzę o dostępnych danych i rozwiązaniach gotowych do ponownego wykorzystania oraz możliwości ich wykorzystania na etapie wdrażania nowych lub rozwijanych istniejących rozwiązań IT dla administracji. Powoduje to niewystarczająco sprawną współpracę instytucji publicznych. W efekcie podmioty publiczne angażują pracowników do czasochłonnego poszukiwania i weryfikacji danych w wielu źródłach, bez gwarancji jakości tych danych.

Dane do rejestrów publicznych są w dużej mierze dostarczane i aktualizowane wskutek obowiązków, jakimi objęte są podmioty publiczne. Biorąc pod uwagę liczbę systemów i rejestrów, w których podmioty muszą uzupełniać dane oraz brak komunikacji i wymiany danych między systemami i rejestrami w zakresie tych samych danych, a także rozwiązań automatyzujących te procesy, utrzymanie wysokiej jakości danych jest obciążone ryzykiem.

Widoczny jest także niedostatek danych i narzędzi do analizy zachowań użytkowników systemów i rejestrów wykorzystywanych przez administrację publiczną, a także samych produktów wytwarzanych na rzecz administracji publicznej. Jest to istotne, aby zidentyfikować potrzeby użytkowników i newralgiczne punkty w dostarczanych rozwiązaniach

Podmioty publiczne są zobowiązane do udostępniania danych z rejestrów publicznych innym podmiotom na warunkach, w sposób, w zakresie i terminie określonym w przepisach, na których podstawie jest prowadzony rejestr. Istotnym wyzwaniem pozostaje brak standardów określających, jak powinny przebiegać procedury uzyskiwania dostępu do rejestrów publicznych. Brak jest powszechnie obowiązującego i jawnego standardu API dla systemów teleinformatycznych służących do realizacji zadań publicznych, który ułatwiłby i przyspieszał integrację rozwiązań cyfrowych, przyczyniając się do zwiększenia interoperacyjności, w tym dostępności i jakości zasobów informacyjnych państwa.

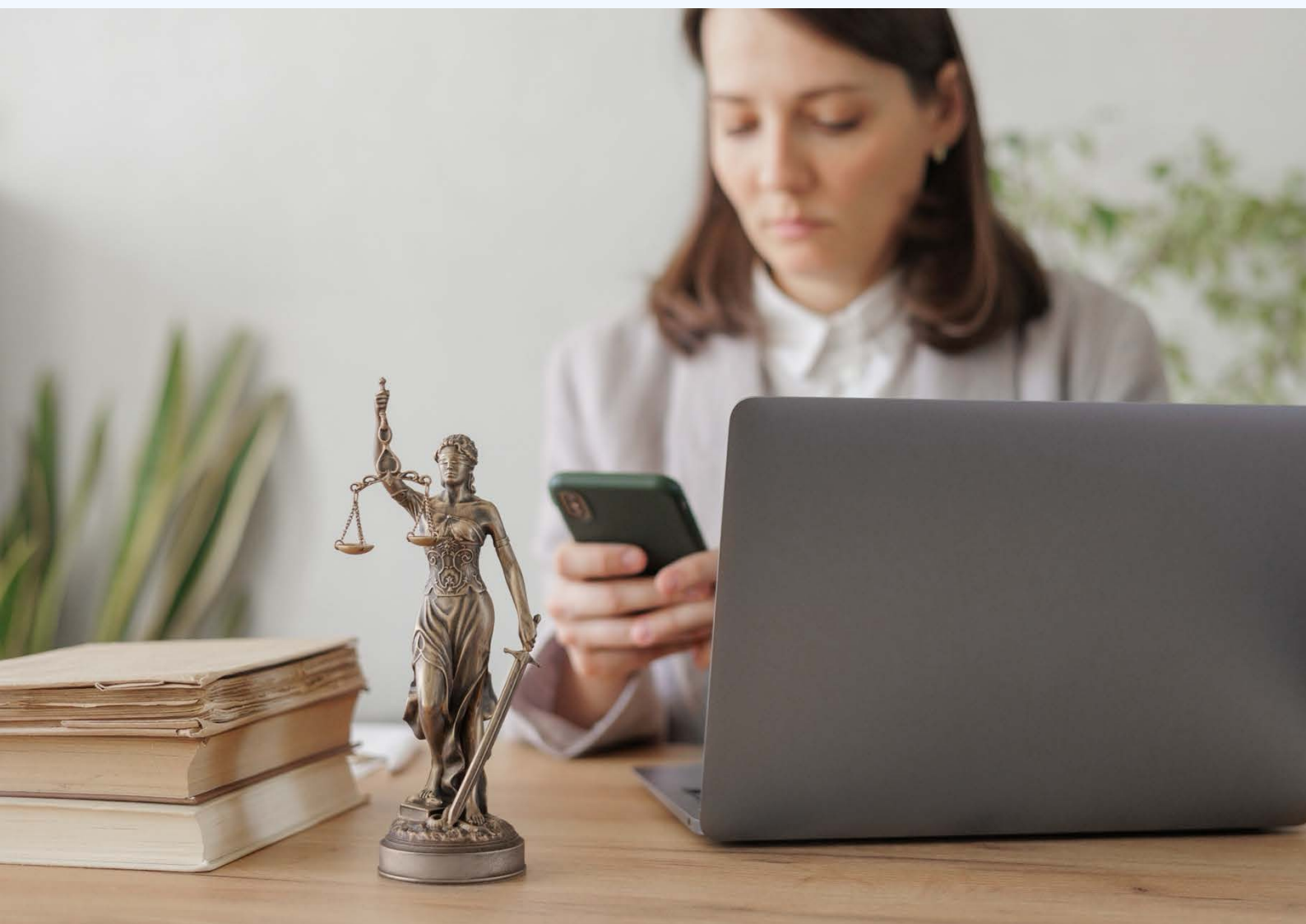
Cel 1: Publiczne systemy teleinformatyczne i rejestry publiczne są interoperacyjne

Co umożliwi realizację celu:

- a) Upowszechnienie i wdrożenie pryncypiów architektonicznych oraz standardów, wytycznych i rekomendacji architektonicznych, w tym dotyczących interoperacyjności systemów teleinformatycznych i rejestrów publicznych oraz reużywalności danych i komponentów technicznych, jako podstawowych zasad tworzenia i rozwoju systemów informacyjnych państwa;
- b) Opracowanie i przyjęcie nowego rozporządzenia Rady Ministrów w sprawie Krajowych Ram Interoperacyjności, minimalnych wymagań dla rejestrów publicznych, minimalnych wymagań dla systemów teleinformatycznych używanych do realizacji zadań publicznych i wymiany danych z podmiotami publicznymi, zapewniającego możliwie jak najszerszy i najwygodniejszy dostęp do zasobów informacyjnych państwa przez interfejsy programistyczne aplikacji, w trybie do odczytu maszynowego. Budowane powinny być rozwiązania unikające nadmiernego angażowania ich użytkowników, spełniające wymagania interoperacyjności organizacyjnej, semantycznej i technologicznej;
- c) Zapewnianie zgodności publicznych systemów teleinformatycznych i rejestrów publicznych z Krajowymi Ramami Interoperacyjności oraz minimalnymi wymaganiami dla systemów teleinformatycznych i rejestrów publicznych, a także dokonywanie cyklicznie przeglądu standardów oraz specyfikacji, w celu ich oceny pod kątem zdolności do zapewniania interoperacyjności;
- d) Uzależnienie realizacji i finansowania przedsięwzięć informatycznych o publicznym zastosowaniu od pozytywnej oceny Komitetu do spraw Cyfryzacji, m.in. w zakresie zgodności ze strategią informatyzacji i strategią cyberbezpieczeństwa, przepisami dotyczącymi interoperacyjności europejskiej oraz krajowej, a także minimalnymi wymaganiami dla publicznych systemów teleinformatycznych, rejestrów publicznych i wymiany danych z podmiotami publicznymi;
- e) Weryfikowanie w ramach prac Komitetu do spraw Cyfryzacji zgodności projektów aktów prawnych ze strategią informatyzacji i strategią cyberbezpieczeństwa, zgodności z przepisami dotyczącymi interoperacyjności europejskiej oraz krajowej, a także zgodności z minimalnymi wymaganiami dla publicznych systemów teleinformatycznych, rejestrów publicznych i wymiany danych z podmiotami publicznymi;
- f) Przeprowadzanie ocen interoperacyjności krajowej i oceny interoperacyjności transgranicznej, obejmujących analizę wpływu zmian wprowadzanych w publicznych systemach teleinformatycznych i rejestrach publicznych na krajowe i europejskie podmioty publiczne;
- g) Zapewnienie unikalnych identyfikatorów dla zasobów informacyjnych państwa w ramach warstw interoperacyjności (dotyczących m.in. aktów prawa powszechnego, dokumentów strategicznych, rejestrów publicznych, publicznych systemów teleinformatycznych), w celu zapewnienia jednoznacznego przywoływania takich

zasobów w dokumentacji i jednoznacznej identyfikacji powiązań między takimi zasobami (w tym na potrzeby wyników ocen interoperacyjności krajowej i transgranicznej);

- h) Zwiększanie interoperacyjności transgranicznej zgodnie z zasadami Europejskich Ram Interoperacyjności:
- digital-by-default (tj. domyślne dostarczanie usług i danych za pośrednictwem kanałów cyfrowych),
 - cross-border-by-default (tj. dostępne dla wszystkich obywateli UE),
 - open-by-default (tj. umożliwiające ponowne wykorzystanie, uczestnictwo/dostęp i przejrzystość).



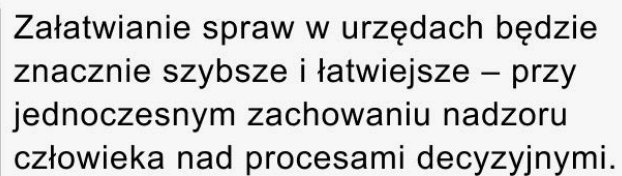
Cel 2: Udostępnianie wysokiej jakości danych z rejestrów publicznych i publicznych systemów teleinformatycznych odbywa się w sposób bezpieczny i zautomatyzowany

Co umożliwi realizację celu:

- a) Umocowanie w przepisach koncepcji referencyjnych rejestrów publicznych, czyli rejestrów publicznych formalnie wskazanych jako zaufane wzorce odniesienia dla innych rejestrów publicznych i systemów teleinformatycznych w określonym zakresie danych;
- b) Przygotowanie, udostępnienie i aktualizacja referencyjnych rejestrów publicznych „Katalogów Administracji Publicznej”, tj. Katalogu Procesów Administracyjnych, Katalog Spraw, Katalog Usług Publicznych, Katalog Wzorów Dokumentów (uwzględniając funkcjonujące Centralne Repozytorium Wzorów Dokumentów Elektronicznych) oraz Katalog Rejestrów Publicznych (uwzględniając przygotowane repozytorium interoperacyjności);
- c) Umocowanie prawne katalogów administracji publicznej w celu automatycznego zasilania i wymiany danych oraz zmniejszenia obciążeń administracyjnych obywateli, przedsiębiorców i administracji publicznej związanych z dostarczaniem i aktualizowaniem tych danych, w tym Katalogu Podmiotów Publicznych (KPP) w zakresie obligatoryjnej integracji KPP z systemami administracji publicznej, które wymagają danych dotyczących podmiotów publicznych i niepublicznych, którym powierzono lub zlecono realizację zadań publicznych;
- d) Pełne zobligowanie prawne do prowadzenia rejestrów publicznych jedynie przy pomocy systemów teleinformatycznych oraz stosowania jednolitych mechanizmów ułatwiających walidację i monitorowanie jakości gromadzonych w nich danych;
- e) Nałożenie wymogu udostępniania danych z publicznych systemów teleinformatycznych i rejestrów publicznych przez API;
- f) Udostępnianie publicznie katalogu API publicznych systemów teleinformatycznych, a także informacji o strukturze i znaczeniu danych przechowywanych we wszystkich rejestrach publicznych; poszerzone o informacje o słownikach, schematach klasyfikacyjnych, taksonomiach oraz listach kodowych w rejestrach publicznych;
- g) Stworzenie krajowej platformy udostępniania danych, jako rozwiązania organizacyjno-technicznego, zapewniającego ustandaryzowane mechanizmy dostępu do danych przetwarzanych w rejestrach publicznych.



Co z tego wynika?



Załatwianie spraw w urzędach będzie znacznie szybsze i łatwiejsze – przy jednoczesnym zachowaniu nadzoru człowieka nad procesami decyzyjnymi.



2.4 Cyfrowa tożsamość

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.

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 usług zaufania kwalifikowane podpisy elektroniczne.

Powyższe modele obarczone są jednak ograniczeniami, które wpływają negatywnie na powszechność zastosowania środków identyfikacji elektronicznej, podpisów elektronicznych i szerzej e-usług publicznych.

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.

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 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.

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 umożliwiłoby proste składanie wielu podpisów z poziomu e-usługi publicznej.

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.

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.

Polska posiada dwa notyfikowane środki identyfikacji elektronicznej: profil zaufany i profil osobisty, jednak ich praktyczne użycie w usługach online innych państw członkowskich jest nieznaczące.

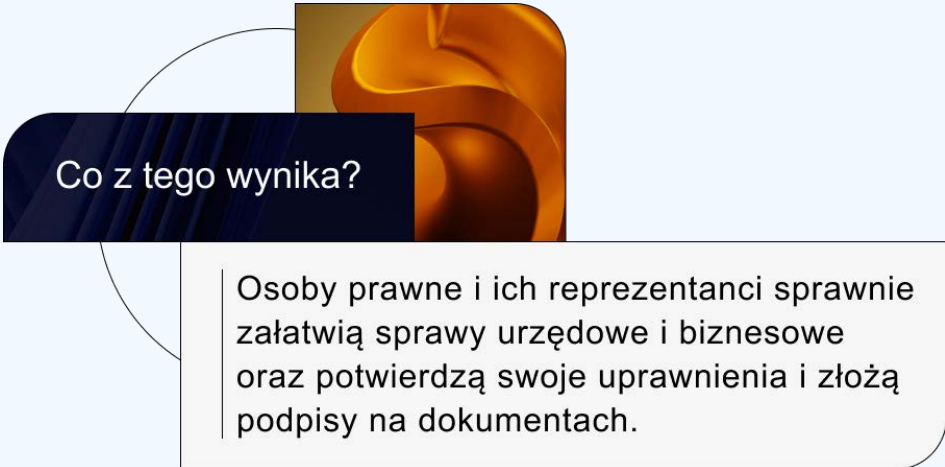
Jednak warto zauważyć, że do zdecydowanej większości krajowych usług online wymagany jest numer PESEL, co powoduje, że w praktyce akceptowalność notyfikowanych środków z innych państw członkowskich również jest na bardzo niskim poziomie. Komisja Europejska, dostrzegając te systemowe praktyczne problemy 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 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. 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.

W celu promowania i przyspieszania rozwoju systemów identyfikacji elektronicznej, a także jednoczesnego dbania o bezpieczeństwo ich licznych użytkowników, konieczne jest ciągle 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, cyberatakami i innym niebezpiecznym sytuacjom w internecie.

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 osoby prawnej oraz środka identyfikacji elektronicznej dla osoby fizycznej reprezentującej osobę prawną;
- b) Skuteczne umocowanie prawne środka identyfikacji elektronicznej dla osoby prawnej oraz środka identyfikacji elektronicznej dla osoby fizycznej reprezentującej 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;
- 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;
- 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");
- e) Udostępnienie europejskiego portfela tożsamości cyfrowej do użytku osób prawnych.



Co z tego wynika?

Osoby prawne i ich reprezentanci sprawnie załatwią sprawy urzędowe i biznesowe oraz potwierdzą swoje uprawnienia i złożą podpisy na dokumentach.

Cel 2: Podpisy elektroniczne są dostępne i powszechnie używane, a ich weryfikacja jest 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;
- 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.



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;
- b) Dodanie do węzła krajowego środka identyfikacji o wysokim poziomie bezpieczeństwa, jakim będzie europejski portfel tożsamości cyfrowej;
- c) Dodanie do węzła krajowego historii użycia środków identyfikacji elektronicznej;
- d) Dodanie weryfikacji, czy urządzenie, z którego następuje logowanie do systemów teleinformatycznych przyłączonych do węzła krajowego, jest na liście urządzeń zaufanych użytkownika;
- e) Realizacja działań edukacyjnych, które wspomogą użytkowników w bezpiecznym korzystaniu ze środków identyfikacji elektronicznej.



Co z tego wynika?

Skorzystasz z bezpiecznych środków identyfikacji elektronicznej – zabezpieczymy je przed kradzieżą tożsamości, naruszeniem danych osobowych, cyberatakami i innymi niebezpiecznymi sytuacjami w internecie, a także umożliwimy sprawdzenie historii ich użycia.

Cel 4: Obywatele i przedsiębiorcy swobodnie i bezpiecznie korzystają z transgranicznych komercyjnych i publicznych usług

Co umożliwi realizację celu:

- a) Utworzenie obowiązkowego rejestru podmiotów, które będą chciały świadczyć swoje usługi w oparciu o europejski portfel tożsamości cyfrowej;
- 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;
- c) Udostępnienie nieodpłatnych kwalifikowanych podpisów elektronicznych w europejskim portfelu tożsamości cyfrowej dla osób fizycznych, przynajmniej do użytku nieprofesjonalnego;
- 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;
- 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).



Co z tego wynika?

Będziesz bezpiecznie i wygodnie potwierdzać swoje dane oraz swobodnie korzystać z wielu usług w krajach Unii Europejskiej.

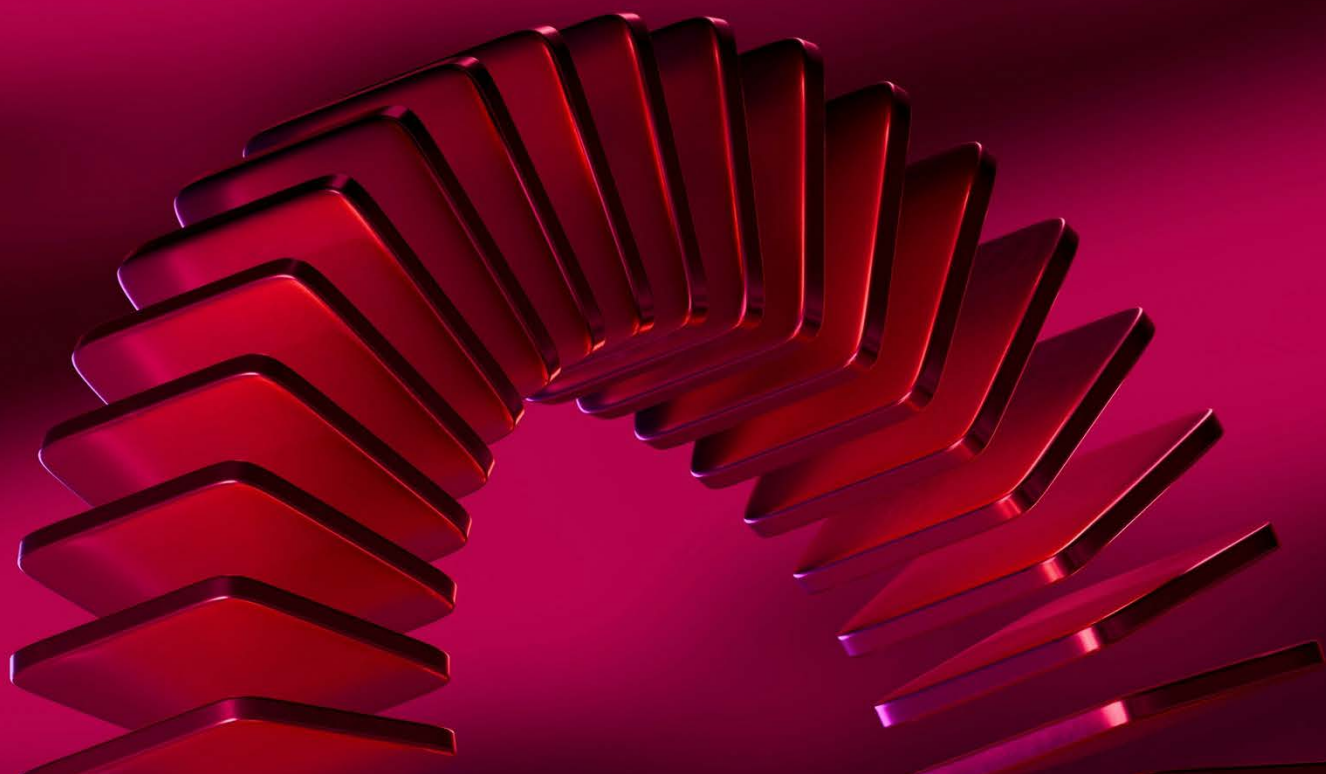
2.5 Chmura obliczeniowa

Diagnoza – jak jest?

Koszt realizacji procesów i ich obsługi w instytucjach publicznych jest wysoki, a wdrażanie nowych e-usług publicznych i systemów teleinformatycznych zbyt powolne. W konsekwencji, rozwój e-usług o wyższym poziomie dojrzałości i złożoności jest hamowany. Jednocześnie konieczne jest zwrócenie uwagi na ryzyko przerwania ciągłości działania e-usług publicznych i systemów teleinformatycznych oraz utraty danych kluczowych systemów administracji publicznej.

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 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.



Cel 1: Rządowa infrastruktura chmurowa i usługi oparte na danych są rozwinięte

Co umożliwi realizację celu:

- a) Wytworzenie w ramach Rządowej Chmury Obliczeniowej i Chmury Samorządowej innowacyjnych usług chmurowych dedykowanych administracji publicznej. Będą to usługi dostarczane w modelach infrastruktura jako usługa (IaaS), platforma jako usługa (PaaS) czy oprogramowanie jako usługa (SaaS), w zależności od charakterystyki wspierające działanie systemów informatycznych, możliwe do wykorzystania jako bloki budowlane do tworzenia nowoczesnych systemów informatycznych, wspomagających projektowanie i wdrażanie oprogramowania w oparciu o usługi chmury obliczeniowej lub niezależnie do realizacji usług publicznych i procesów obsługiwanych w jednostkach;
- b) Zapewnienie, że wdrażane usługi będą spełniać najwyższe standardy bezpieczeństwa, będą zgodne z polskimi i unijnymi regulacjami prawnymi i będą bazować na najlepszych standardach światowych zgodnie z pryncypiami Architektury Informacyjnej Państwa;
- c) Zwiększenie dostępności skalowalnych usług infrastrukturalnych dostarczanych w modelu chmury obliczeniowej, dostosowanych do zmieniających się potrzeb administracji;
- d) Uproszczenie stosu technologicznego, komponentów architektury zorientowanych na usługi oraz udostępnienie standardów architektonicznych i predefiniowanych modułów oprogramowania, pozwalające na uproszczenie i przyspieszenie procesu wdrożenia nowych e-usług publicznych i systemów IT;
- e) Stworzenie ambasad danych – zlokalizowanych poza granicami kraju jednostek umożliwiających składowanie kluczowych danych i informacji z rejestrów i systemów państwowych oraz zapewnienie ciągłości działania tych rejestrów i systemów w przypadku wystąpienia sytuacji kryzysowych na terytorium RP.



Co z tego wynika?

Zabezpieczymy działanie kluczowych systemów i rejestrów przed zakłóceniami, a dane w nich gromadzone przed utratą.

Cel 2: Infrastruktura przetwarzania danych jest nowoczesna i rozbudowana

Co umożliwi realizację celu:

- a) Budowa i rozwój Krajowego Centrum Przetwarzania Danych, obejmującego budowę trzech nowoczesnych, skalowalnych i wysoce wydajnych centrów przetwarzania, które zapewnią ciągłość działania systemów i bezpieczeństwo zasobów administracji publicznej. Połączone światłowodami centra będą wykorzystywały zieloną energię;
- b) Zapewnienie ciągłości świadczenia e-usług publicznych i funkcjonowania systemów teleinformatycznych poprzez zabezpieczenie danych systemów administracji publicznej przetwarzające dane o charakterze referencyjnym, przed utratą, określenie gwarantowanego czasu odtworzenia danych w przypadku poważnej awarii oraz udostępnienie ustandaryzowanych usług wspomagających plany zachowania ciągłości działania, tworzenia archiwów i kopii bezpieczeństwa, w tym do długotrwałego składowania danych, odtworzenia danych oraz wspierających przywrócenie działania standardowych komponentów systemów teleinformatycznych;
- c) Rozbudowa państwowej infrastruktury na rzecz świadczenia e-usług publicznych umożliwiającej efektywne przetwarzanie danych, w tym optymalizację sieci ośrodków obliczeniowych zabezpieczających ciągłość świadczenia e-usług oraz przepływu danych na potrzeby systemów teleinformatycznych wspierających ich realizację, m.in. dla sektora ochrony zdrowia, finansów, sądów.



Cel 3: Podmioty publiczne mają zapewnione wsparcie w nabywaniu, wdrażaniu i wykorzystywaniu systemów i rozwiązań informatycznych w oparciu o usługi chmurowe

Co umożliwi realizację celu:

- a) Prowadzenie regularnych badań popytu na usługi rządowej i publicznej chmury obliczeniowej w administracji publicznej;
- b) Koordynacja i realizacja przez wyznaczony podmiot centralnych zamówień na usługi w zakresie chmury publicznej w przypadku usług najczęściej wykorzystywanych przez administrację publiczną, w tym zawieranie umów ramowych poszerzających katalog usług chmurowych dostępnych dla administracji publicznej po przeprowadzaniu uproszczonych postępowań wykonawczych;
- c) Wspieranie bezpiecznego pozyskiwania usług chmurowych w ramach postępowań zakupowych dzięki systemowi Zapewniania Usług Chmurowych (ZUCH). System zapewni obsługę pełnego procesu zakupowego PZP poprzez integrację z e-Zamówieniami i implementację obsługi postępowań wykonawczych oraz podpisywanie umów i porozumień bezpośrednio w systemie ZUCH;
- d) Wspieranie konkurencyjności w pozyskiwaniu i wyszukiwaniu usług chmurowych przez bezpośrednią integrację systemu ZUCH z portalami zarządzania usługami chmurowymi dla chmur publicznych i prywatnych wspierających procesy porównywania, powoływania, raportowania i rozliczania usług, co pozwoli na zapewnienie niezależności od konkretnych dostawców usług;
- e) Udostępnienie w systemie ZUCH funkcjonalności Biznesowej Platformy Zarządzania Usługami Chmurowymi od wielu dostawców usług chmurowych do prostego zarządzania usługami od różnych dostawców usług chmurowych;
- f) Udostępnienie w systemie ZUCH, dla nowotworzonych innowacyjnych usług chmurowych na rządowej chmurze obliczeniowej, funkcjonalności do konfiguracji, zarządzania i rozliczania wykorzystania tych usług chmurowych;
- g) Utworzenie Akademii Chmury, gdzie jednostki administracji będą mogły pozyskać wiedzę o bezpiecznych rozwiązaniach i dobrych praktykach w tworzeniu i utrzymaniu rozwiązań na infrastrukturze chmury obliczeniowej.



Co z tego wynika?

Wszystkie usługi chmurowe dla administracji publicznej będą zamawiane centralnie, co zwiększy bezpieczeństwo i przejrzystość tego procesu, a także zmniejszy koszty dla administracji.



2.6 Otwarte dane i wymiana danych

Diagnoza – jak jest?

Dane mają wysokie znaczenie w gospodarce i społeczeństwie. Generowane przez komputery, smartfony i urządzenia codziennego użytku opatrzone licznymi czujnikami napędzają rozwój gospodarczy, konkurencyjność, innowacyjność i postęp społeczny. Według Komisji Europejskiej bezpośrednia wartość ekonomiczna informacji sektora publicznego została obliczona w ocenie skutków na 52 mld EUR w 2018 r., a szacuje się, że do 2030 r. wzrośnie do 149 mld EUR²⁶. Wnioski z systemu monitorowania Programu otwierania danych na lata 2021-2027²⁷, wskazują m.in. na konieczność zwiększenia ilości danych w portalu dane.gov.pl oraz obiektów w kronika.gov.pl, dbanie o jakość danych oraz zwiększenie zakresu danych, podjęcie cyklicznego i długotrwałego działania na rzecz podniesienia poziomu wiedzy i umiejętności kadry administracyjnej w zakresie otwierania danych i zarządzania nimi, wdrożenie działań z zakresu promowania polityki otwartego dostępu do danych oraz działań informujących o możliwości udostępniania danych w portalu dane.gov.pl i płynących z tego korzyściach.

Ponadto, mając na względzie dynamiczny rozwój sztucznej inteligencji, która bazuje na dobrych jakościowo danych, niezbędne są działania ulepszające jakość zasobów publikowanych w portalu dane.gov.pl również na potrzeby uczenia maszynowego.

Ewaluacja ustawy o otwartych danych i ponownym wykorzystywaniu informacji sektora publicznego²⁸ wskazała obszary wymagające podjęcia zintensyfikowanych działań pozalegisłacyjnych. Należą do nich: potrzeba wzmocnienia sieci pełnomocników do spraw otwartości danych, dalszy rozwój portalu dane.gov.pl, podjęcia działań informacyjnych, edukacyjnych oraz promocyjnych nakierowanych na poszerzenie wiedzy na temat procesu otwierania i ponownego wykorzystywania danych publicznych.

Na poziomie UE, Komisja Europejska podejmuje działania w celu zwiększania wymiany i dzielenia się danymi pomiędzy różnymi aktorami, tj. konsumentami, przedsiębiorstwami i podmiotami sektora publicznego. Następnym przyjmowania unijnych aktów prawnych jest konieczność zapewniania przez Polskę, jako państwo członkowskie, odpowiedniego stosowania lub wdrażania przyjmowanych przez UE instrumentów prawnych dot. danych.

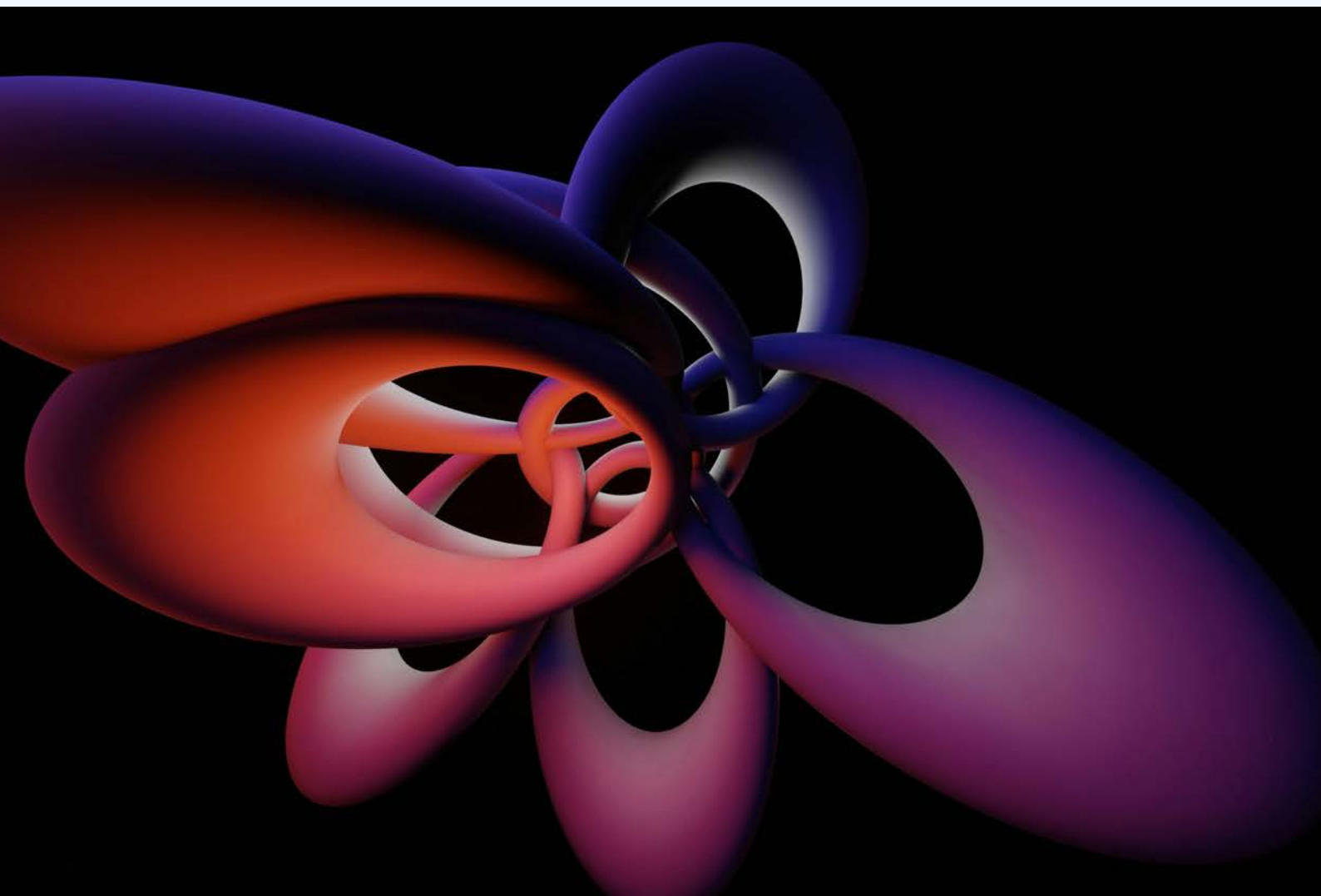
²⁶ Open data maturity report 2023, <https://data.europa.eu/en/publications/open-data-maturity/2023>, za <https://digital-strategy.ec.europa.eu/en/library/impact-assessment-review-directive-200398ec-reuse-public-sector-information>.

²⁷ Uchwała nr 28 Rady Ministrów z dnia 18 lutego 2021 r. w sprawie Programu otwierania danych na lata 2021-2027 (M.P. poz. 290).

²⁸ Ustawa z dnia 11 sierpnia 2021 r. o otwartych danych i ponownym wykorzystywaniu informacji sektora publicznego (Dz. U. z 2023 r., poz. 1524).

Stały monitoring przepisów krajowych i unijnych jest kluczowy dla dostosowania się do zmieniających się potrzeb użytkowników danych.

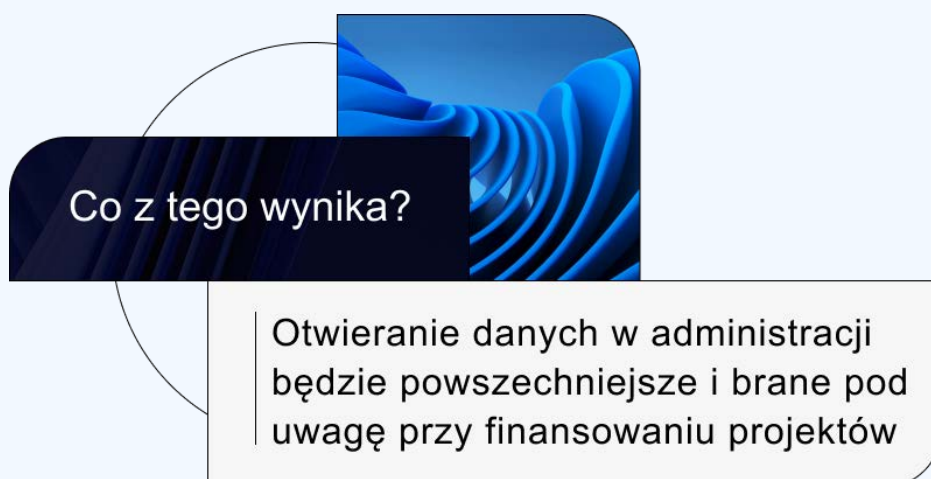
Identyfikujemy potrzebę stymulowania powstającego w Polsce rynku danych, który podlegać ma nowoprzyjętym europejskim ramom regulacyjnym (dotyczy to w szczególności sektora pośredników danych i organizacji altruizmu danych). Podejmowane przez nas działania będą miały na celu wsparcie wymiany danych pomiędzy uczestnikami niewykształconego jeszcze w pełni rynku, który musi się szybko dostosować do nakładanych na niego regulacji. Ważne jest w szczególności włączenie polskich podmiotów z sektora publicznego oraz spoza niego w powstające jednolite europejskie przestrzenie danych. Równolegle trzeba tworzyć warunki do powstawania, w oparciu o możliwości jakie niosą wdrażane przez nas nowe regulacje unijne, mniejszych odpowiedników europejskich przestrzeni danych, które mogłyby korzystać z potencjału powoływanych sukcesywnie pośredników danych i organizacji altruizmu danych.



Cel 1: Administracja publiczna świadomie działa na rzecz otwartości danych

Co umożliwi realizację celu:

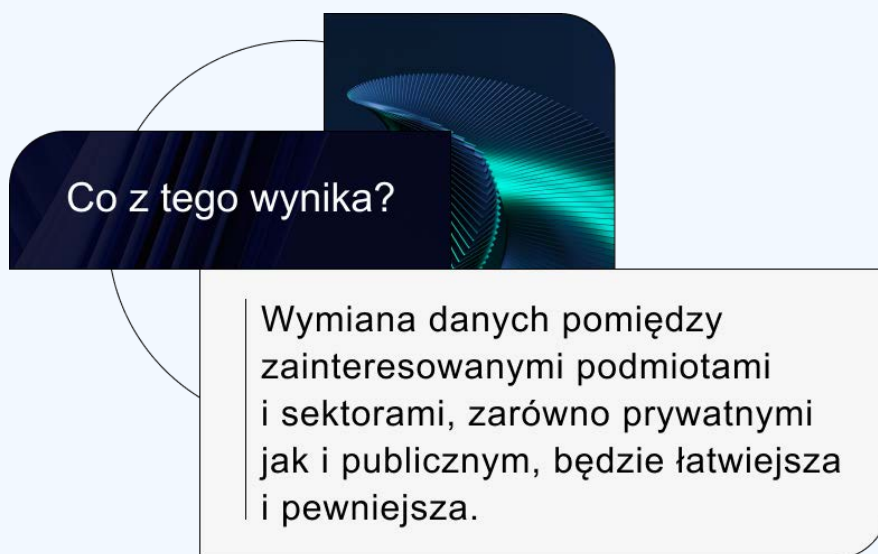
- a) Uzależnienie realizacji i finansowania przedsięwzięć informatycznych od pozytywnej oceny Komitetu do spraw Cyfryzacji m.in. w zakresie zgodności z zasadami tworzenia danych;
- b) Upowszechnianie zasad tworzenia danych w fazie projektowania i otwartości domyślnej w procesach i projektach, w tym informatycznych realizowanych przez administrację publiczną, oraz uwzględnienie w nich udostępniania danych poprzez API;
- c) Poszerzenie sieci pełnomocników ds. otwartości danych na wielu poziomach instytucjonalnych.



Cel 2: Otoczenie prawne w obszarze zarządzania danymi sprzyja rozwojowi ekosystemu wymiany danych

Co umożliwi realizację celu:

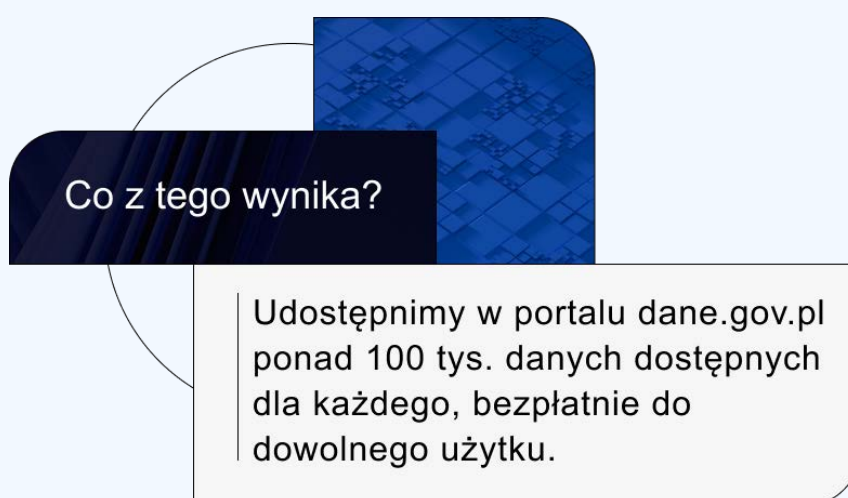
- a) Ustanowienie przyjaznego środowiska legislacyjnego dla dzielenia się danymi z pobudek altruistycznych oraz wymiany danych w relacjach B2B oraz B2G, (w tym przyjęcie przepisów krajowych służących stosowaniu Aktu w sprawie zarządzania danymi i Aktu w sprawie danych);
- b) Uczestnictwo w tworzeniu kolejnych aktów prawnych urzeczywistniających jednolity rynek danych w UE i oraz w rewizji unijnych aktów prawnych zgodnie z potrzebami i kierunkami rozwoju krajowego rynku danych;
- c) Optymalizacja przepisów ustawy o otwartych danych w kierunku ułatwienia i poszerzenia zakresu ponownego wykorzystania danych publicznych.



Cel 3: Dostęp do danych o wysokiej jakości do ponownego wykorzystywania i uczenia maszynowego jest powszechny

Co umożliwi realizację celu:

- a) Badania w zakresie określenia poziomu podaży i popytu w odniesieniu do danych;
- b) Współpraca z posiadaczami danych w zakresie zwiększenia wolumenu danych²⁹, w tym danych połączonych oraz dynamicznych, w portalu dane.gov.pl, w szczególności dostępnych za pośrednictwem API przykładowo w obszarach dotyczących mieszkalnictwa, zanieczyszczenia środowiska, sektora energetycznego;
- c) Rozwój zaufanego portalu dane.gov.pl w ramach modułu komunikacji z użytkownikami, modułu jakości danych i użyteczności portalu oraz modułu statystyk;
- d) Mechanizmy poprawiające jakość danych w portalu dane.gov.pl;
- e) Identyfikacja danych o wysokiej wartości i w partnerstwach publicznych budowanie API, które będą je udostępniać.



²⁹ Dane w kontekście portalu dane.gov.pl rozumiane są jako każda treść lub jej część, niezależnie od sposobu utrwalenia, w szczególności w postaci papierowej, elektronicznej, dźwiękowej, wizualnej lub audiowizualnej, będąca w posiadaniu podmiotu zobowiązanego zgodnie z ustawą o otwartych danych i ponownym wykorzystywaniu informacji sektora publicznego lub będąca w posiadaniu innego podmiotu niż podmiot zobowiązany i przez niego wytworzona. Zbiór danych rozumiany jest jako zestaw, gromadzący dane z konkretnej tematyki.

Cel 4: Dostęp do zasobów z obszaru nauki i kultury za pośrednictwem portalu kronika.gov.pl jest łatwiejszy

Co umożliwi realizację celu:

- a) Badania w zakresie określenia poziomu podaży i popytu w odniesieniu do zasobów z obszaru nauki i kultury;
- b) Współpraca z interesariuszami danych w zakresie zwiększenia wolumenu zasobów w portalu kronika.gov.pl na potrzeby ponownego wykorzystywania i zabezpieczenia w repozytorium zapasowym;
- c) Rozwój zaufanego portalu kronika.gov.pl jako cyfrowej przestrzeni zasobów nauki i kultury polskiej;
- d) Budowanie API pomiędzy portalem kronika.gov.pl a instytucjami publikującymi dane z obszaru nauki i kultury, by ułatwić integrację zasobów publikowanych w „wyspowych” serwisach w ramach huba informacyjnego jakim jest kronika.gov.pl;
- e) Działania informacyjno-promocyjne w zakresie ponownego wykorzystywania danych z obszaru nauki i kultury;
- f) Współpraca ze środowiskiem akademickim w zakresie powiązania prezentowanych obiektów cyfrowych z obszaru kultury z publikowanymi wynikami badań naukowych oraz utworzenia katalogu prac naukowych bazujących na zasobach publikowanych w kronika.gov.pl.



Cel 5: Polski rynek wymiany danych jest dojrzały

Co umożliwi realizację celu:

- a) Rekomendowanie systemowego finansowania projektów wspierających rozwój usług pośrednictwa danych i altruizmu danych w ramach nowej perspektywy finansowej UE;
- b) Stymulowanie wymiany danych z interesariuszami spoza administracji oraz pomiędzy nimi.



Ludzie



Ministerstwo
Cyfryzacji

Tu tworzymy przyszłość

Ludzie

3.1 Bezpieczna przestrzeń cyfrowa

Diagnoza – jak jest?

Wśród głównych czynników mających wpływ na podejście społeczeństwa do e-państwa można wyróżnić: użyteczność narzędzi, aspekty społeczne (zachowania innych), potencjalne ryzyka oraz dostępny już obywatelowi sprzęt i umiejętności. Szczególnie jednak istotnym czynnikiem, wpływającym m.in. na wykorzystanie e-usług publicznych, jest zaufanie.

Z tego względu, państwo ma obowiązek dążenia do budowy bezpieczeństwa szeroko pojętej sfery cyfrowej – dbałości o bezpieczeństwo użytkowników, respektowania zasad demokratycznego państwa prawa i praw obywatelskich, a także ochrony przestrzeni informacyjnej w sieci.

Za kluczową należy uznać ochronę bezpieczeństwa obywateli i ich danych, konkurencji rynkowej czy budowania suwerenności technologicznej. Konieczne jest więc podążanie za regulacjami oraz standardami cyfrowymi chroniącymi prawa obywatelskie, powstającymi w Unii Europejskiej. Szczególnie istotna jest implementacja na gruncie krajowym unijnej deklaracji praw i zasad cyfrowych w cyfrowej dekadzie z 2022 r. Jej celem jest wspieranie transformacji cyfrowej w UE, w tym ukierunkowanie tej transformacji na człowieka, solidarność i włączenie społeczne, swoboda wyboru, czy bezpieczeństwo i ochrona. Przyjęcie założenia, że ochrona obywateli stanowi priorytet, musi przekładać się m.in. na zapewnianie odpowiednich zasobów instytucjonalnych dla wdrażania i stosowania krajowych i unijnych aktów legislacyjnych w tym obszarze.

Prawa obywatelskie o charakterze cyfrowym realizują się zarówno w relacjach jednostki z instytucjami władzy, jak i użytkowników z usługodawcami cyfrowymi. W kontekście tych ostatnich, zagrożeniem są kwestie nieuzasadnionej moderacji treści przez platformy, niejasności w regulaminach i standardach cyfrowych społeczności, tzw. zwodniczych interfejsów, braku transparentności algorytmów i rozliczalności za działania platform. Problemy te wiążą się z modelem biznesowym opartym na walce o zaangażowanie użytkowników, stwarzającym ryzyka dla prywatności i wykorzystania danych osobowych. Brak reakcji na te zjawiska skutkuje długotrwałą i rosnącą społeczną polaryzacją, co podważa zarówno ład demokratyczny, jak i ład informacyjny państwa.

Na prawa podstawowe w sferze cyfrowej należy patrzeć również z perspektywy jej wpływu na pracowników.

Nowe trendy związane z automatyzacją i digitalizacją procesów w firmach dotyczą zarówno pracowników fizycznych, jak i umysłowych. Narzędzia cyfrowe pozwalają na szeroko zakrojoną kontrolę pracowników, co może wiązać się z naruszaniem ich prywatności i dobrostanu. Wzrost popularności pracy zdalnej umożliwił elastyczną organizację czasu i przyniósł korzyści wielu pracownikom i pracodawcom. Równocześnie jednak generuje ryzyko związane z oczekiwaniem ciągłej dostępności od pracownika oraz utrudnia rozgraniczanie życia zawodowego i osobistego. Obserwujemy także dalszy intensywny rozwój niekonwencjonalnych modeli biznesowych, na czele których znalazła się gospodarka współdzielenia. Z jednej strony otworzyła ona przed konsumentami, przedsiębiorcami i pracownikami nowe możliwości, z drugiej jednak doprowadziła do destabilizacji warunków pracy i pozbawienia osób pracujących za pośrednictwem aplikacji ich podstawowych praw. Tym samym, przerzucenie odpowiedzialności i kosztów działalności na pracowników platform - których liczba w UE ma sięgnąć 43 mln³⁰ - prowadzi do wzrostu niepewności zatrudnienia i upowszechniania się zjawiska prekariatu.

Wreszcie, zapewnienie kompleksowego bezpieczeństwa sfery cyfrowej wymaga skutecznej walki z dezinformacją. Jest ona rozumiana jako nieprawdziwe lub wprowadzające w błąd (zmanipulowane) informacje, tworzone, przedstawiane i rozpowszechniane w celu uzyskania korzyści gospodarczych lub wprowadzenia w błąd opinii publicznej, które mogą wyrządzić szkodę publiczną. Należy rozróżnić dwa rodzaje dezinformacji – pochodzenia zewnętrznego oraz wewnętrznego (stosowaną przez konkretne podmioty/środowiska wobec obywateli tego samego państwa). Dezinformacja jako działanie zorganizowane ma charakter strategiczny i długoterminowy.

Dezinformacja wewnętrzna prowadzona jest w celu budowania kapitału społecznego, politycznego lub finansowego. Z kolei podmioty zewnętrzne stosują ją, m.in. by destabilizować sytuację społeczno-polityczną w kraju i stymulować polaryzację społeczną. Najaktywniejszym adwersarzem państwa polskiego są państwa prowadzące przeciwko Polsce wojnę informacyjną, w tym Rosja i Białoruś. Prowadzone przez nie działania obejmują kompleksowe działania dezinformacyjne, zaawansowane operacje wpływu czy działania wywiadowcze i dywersyjne, a także ataki fizyczne. Propagowane przez antagonistycznie nastawione państwa przekazy dezinformacyjne służą z jednej strony realizacji celów wewnętrznych (w tym zwiększaniu poparcia dla liderów), z drugiej – zewnętrznych (takich jak stymulowanie nastrojów antynatowskich, antyunijnych, antyamerykańskich i antyukraińskich).

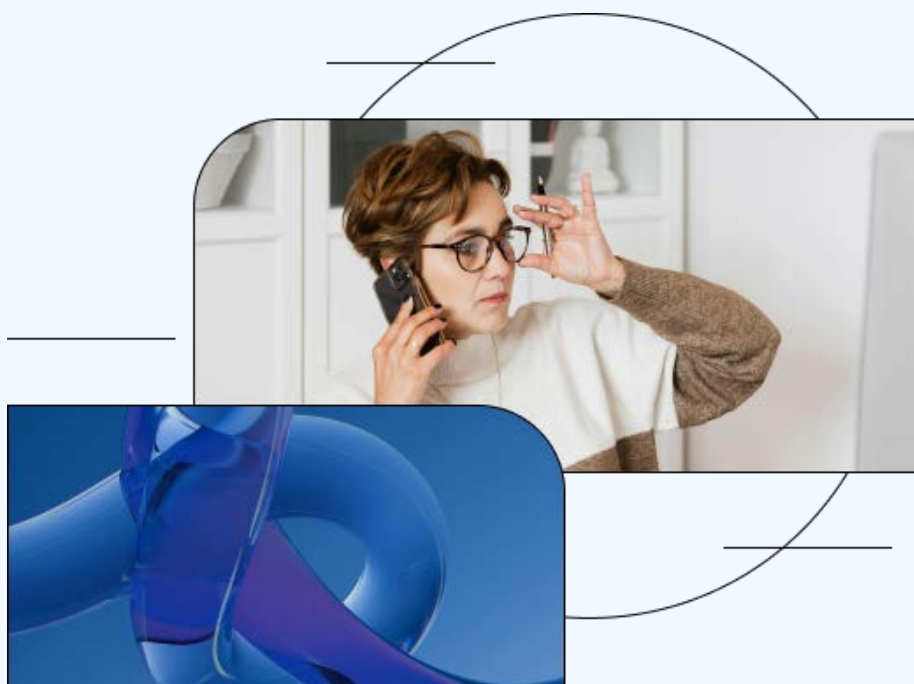
W Polsce zadania związane z przeciwdziałaniem dezinformacji prowadzone są przez szereg instytucji, w tym NASK-PIB, Ministerstwo Spraw Zagranicznych, Krajową Radę Radiofonii i Telewizji (edukacja medialna), Rządowe Centrum Bezpieczeństwa (analiza zagrożeń, w tym związanych z dezinformacją), odpowiednie służby (w tym SKW – Służba Kontrwywiadu Wojskowego i ABW – Agencja Bezpieczeństwa Wewnętrznego) oraz komisję ds. badania wpływów rosyjskich i białoruskich. Zgodnie z unijnym aktem o usługach cyfrowych w działania – jako koordynator ds. usług cyfrowych – włączy się też Prezes Urzędu

³⁰ <https://www.consilium.europa.eu/pl/policies/platform-work-eu/>

Komunikacji Elektronicznej. Wielość instytucji działających w obszarze dezinformacji przekłada się na jedno z głównych wyzwań w tym obszarze – brak odpowiedniej koordynacji i komunikacji, a także niespójność w metodach działania.

Wśród innych wyzwań wskazać należy:

- Rozwój nowych technologii (w tym AI) umożliwiających szybsze i skuteczniejsze tworzenie treści dezinformacyjnych;
- Nieefektywną współpracę z platformami społecznościowymi w procesie identyfikacji oraz zdejmowania treści dezinformacyjnych jak i kont je rozpowszechniających (w tym botów);
- Konieczność pogłębienia działań zmierzających do analizowania kampanii dezinformacyjnych w sposób kompleksowy;
- Niską świadomość społeczną oraz potrzebę rozwoju kompetencji w zakresie edukacji medialnej, myślenia krytycznego oraz bezpieczeństwa informacyjnego;
- Rozproszenie i niewystarczające finansowanie organizacji pozarządowych zajmujących się przeciwdziałaniem dezinformacji;
- Brak ustalonych na poziomie centralnym oraz samorządowym strategii reagowania na dezinformację lub komunikacji kryzysowej.



Cel 1: Otoczenie instytucjonalne i regulacyjne w sferze cyfrowej wspiera ochronę praw podstawowych

Co umożliwi realizację celu:

- a) Wspieranie silnego otoczenia instytucjonalnego wokół regulacji mających za zadanie zapewnić poszanowanie uznanych wartości i praw jednostek w sieci poprzez wyposażenie podmiotów odpowiedzialnych za egzekwowanie ich przepisów w środki techniczne, osobowe i finansowe;
- b) Promowanie tego, by projektowanie, opracowywanie, wdrażanie i wykorzystywanie rozwiązań technologicznych odbywało się z poszanowaniem praw podstawowych poprzez stosowanie zasady „etyki już na etapie projektowania” („ethics by design”)
- c) Przeprowadzanie oceny wpływu na prawa podstawowe obywateli (FRIA) w przypadku wykorzystywania systemów automatycznego podejmowania decyzji oraz systemów AI w administracji państwowej
- d) Stworzenie formularza do oceny wymiaru etycznej SI stosowanej przez państwo;
- e) Wypracowanie krajowych rozwiązań w zakresie domniemania istnienia stosunku pracy w obszarze gospodarki współdzielenia oraz niezwłoczne wdrożenie do polskiego prawa dyrektywy o pracownikach platformowych;
- f) Bieżące badanie wpływu technologii cyfrowych, zwłaszcza AI, na rynek pracy;
- g) Zapewnianie skutecznego przestrzegania reguł prawa pracy i aktualności polityk publicznych w odniesieniu do dynamicznie zmieniającego się pod wpływem digitalizacji i wywołanej nią trendów rynku pracy. Mowa tutaj o ochronie pracowników przed ryzykiem bycia ciągle dostępnym (przyjęcie prawa do odłączenia się), nieprzejrzystym „scoringiem” i zbudowanymi na uprzedzeniach ocenami pracowników (wdrożenie regulacji związanych z wykorzystywaniem SI w obszarze pracy) i cyfrową inwigilacją (egzekwowanie przepisów dot. prywatności);
- h) Aktywność na forum krajowym i unijnym na rzecz wdrażania rozwiązań, w szczególności legislacyjnych, dla ochrony prawa do prywatności, ochrony danych osobowych i prawa do odłączenia się.

Cel 2: Publiczna przestrzeń cyfrowa jest przyjazna użytkownikom i budzi zaufanie obywateli

Co umożliwi realizację celu:

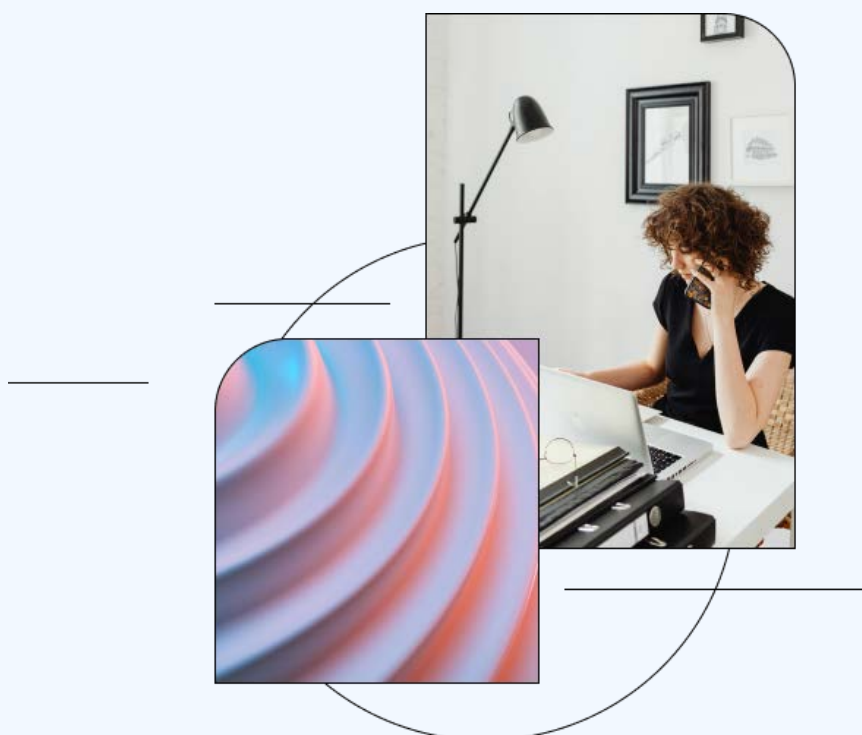
- a) Praktyczna realizacja założeń Europejskiej deklaracji praw i zasad cyfrowych w cyfrowej dekadzie we wszelkich interakcjach państwa z obywatelami w sferze cyfrowej;
- b) Budowa zaufania do e-państwa poprzez większe włączenie obywateli w proces tworzenia cyfrowego prawa (w tym z wykorzystaniem narzędzi cyfrowych) i cyfrowych usług publicznych, a także zlikwidowanie luki w cyfryzacji dokumentów istotnych dla opinii publicznej (publikowanie w sposób dostępny cyfrowo, w formacie umożliwiającym odczyt maszynowy takich dokumentów jak np. oświadczenia majątkowe parlamentarzystów) i dążenie do większej przejrzystości procesu przetwarzania spraw i danych obywatela;
- c) Zaprojektowanie rozwiązań mających umożliwić obywatelom dostęp do informacji o tym, jaki organ i w jakiej sprawie miał dostęp do ich danych – wykorzystywanie mechanizmów „privacy by design” (prywatności w fazie projektowania) i „security by design” (bezpieczeństwo w fazie projektowania) z uwzględnieniem reguł RODO, wprowadzenia zasady automatycznego wykrywania operacji na danych umożliwiającej obywatelom kontrolę ich danych i zgłaszanie naruszeń oraz wykorzystywania analizy historii zapytań o dane w celu wychwytywania zagrożeń.



Cel 3: Działania jednostek przeciwdziałających dezinformacji są skoordynowane

Co umożliwi realizację celu:

- a) Ustalenie organu odpowiedzialnego za nadzorowanie i integrowanie działań różnych podmiotów zajmujących się przeciwdziałaniem dezinformacji;
- b) Zapewnienie klarownej struktury komunikacyjnej i przepływu informacji między wszystkimi zaangażowanymi jednostkami poprzez regularne spotkania i platformy wymiany danych;
- c) Opracowanie jednolitych lub zbliżonych procedur i standardów operacyjnych stosowanych przez wszystkie jednostki zajmujące się przeciwdziałaniem dezinformacji;
- d) Zapewnienie zaawansowanych narzędzi technologicznych oraz szkoleń dla pracowników jednostek.



Cel 4: Poziom świadomości społecznej na temat dezinformacji jest stale pogłębiany

Co umożliwi realizację celu:

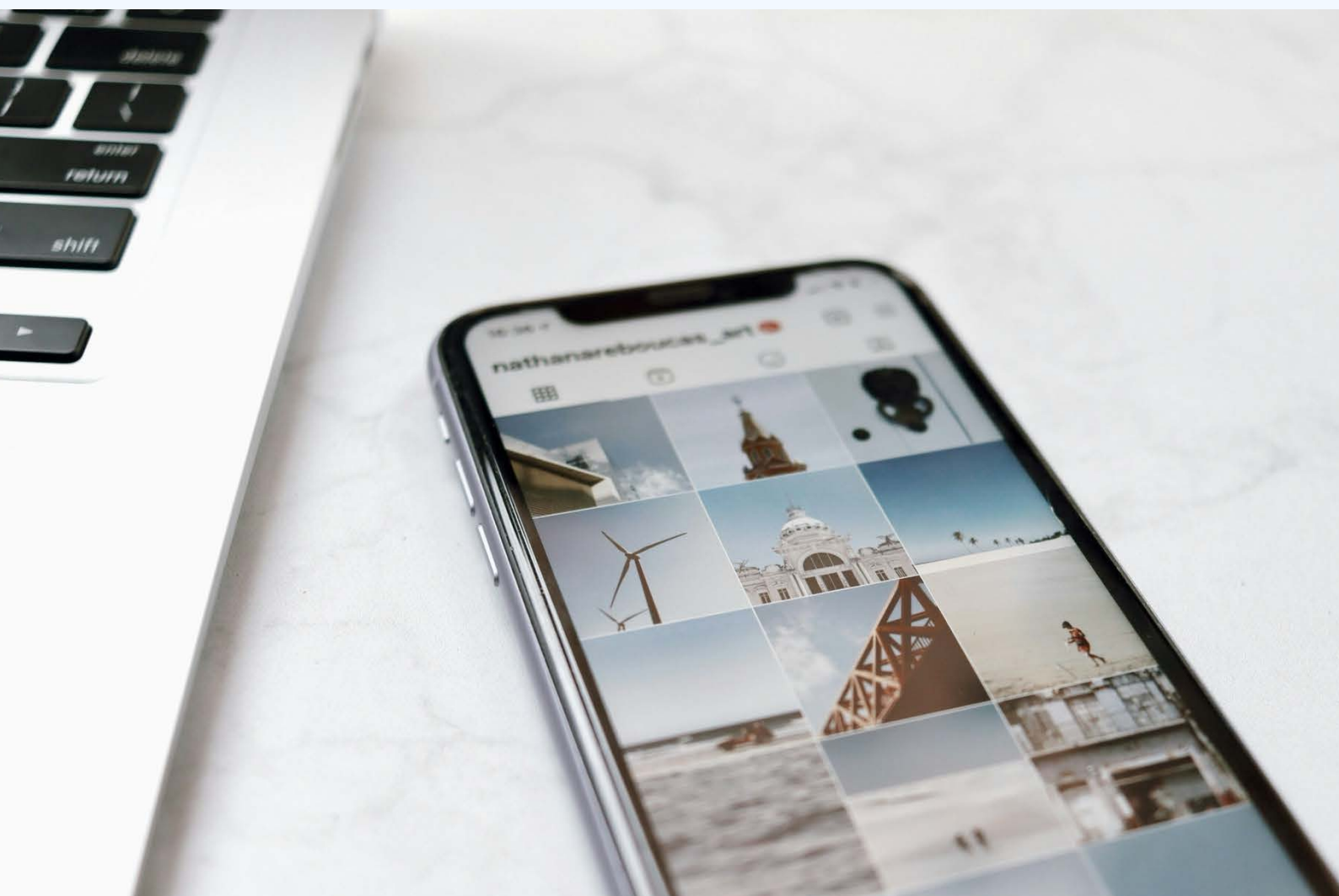
- a) Realizacja kampanii informacyjnych i społecznych na temat dezinformacji i odpowiedzialnego korzystania z mediów;
- b) Prowadzenie działań edukacyjnych do wybranych grup społecznych;
- c) Prowadzenie dedykowanych kampanii informacyjnych w związku z kluczowymi wydarzeniami, jak np. w okresie wyborczym;
- d) Stworzenie interaktywnych platform e-learningowych i multimedialnych materiałów dydaktycznych;
- e) Organizowanie dyskusji, debat i warsztatów na temat etycznych aspektów działalności medialnej, takich jak prywatność, ochrona danych, prawa autorskie i odpowiedzialność za publikowane treści.



Cel 5: Platformy społecznościowe sprawnie usuwają treści szkodliwe

Co umożliwi realizację celu:

- a) Stały monitoring treści znajdujących się na platformach społecznościowych;
- b) Ustanowienie odpowiednich ścieżek wymiany informacji dla zaufanych podmiotów sygnalizujących (zgodnie z Aktem o Usługach Cyfrowych);
- c) Ustanowienie jasnych i transparentnych kryteriów prowadzących do uzyskania statusu zaufanego podmiotu sygnalizującego. Zaufane podmioty sygnalizujące powinny posiadać szczególną wiedzę fachową i kompetencje w zakresie wykrywania, identyfikowania i zgłaszania nielegalnych treści oraz są niezależne od platform internetowych;
- d) Wdrożenie efektywnych mechanizmów penalizujących platformy mediów społecznościowych oraz usługodawców IT za brak działań ukierunkowanych na zwalczanie dezinformacji;
- e) Utworzenie ram współpracy z sektorem prywatnym, szczególnie z platformami mediów społecznościowych.



3.2 Cyfrowe zdrowie

Diagnoza – jak jest?

Kompleksowa diagnoza sytuacji relacji między sferą technologii a zdrowiem wymaga dostrzeżenia dwóch, często sprzecznych wymiarów tej relacji. Pierwszym z wymiarów jest

negatywny wpływ niektórych aspektów wykorzystania technologii cyfrowych na kondycję psychiczną obywateli.

Wiąże się on m.in. z uzależniającym mechanizmem działania platform społecznościowych i szkodliwym – sensacyjnym, rysującym nierealne standardy urody czy gloryfikującym przemoc – charakterem niektórych pojawiających się tam treści. Szczególnie wyraźnie rysującym się problemem, również wobec niedostatecznej skuteczności mechanizmów weryfikacji wieku, jest powszechny dostęp dzieci do treści szkodliwych, godzących w ich rozwój i propagujących niewłaściwe wzorce. Istotnym problemem jest też wykorzystywanie małoletnich w sieci. Państwo jest zobowiązane do tego, by na te wyzwania reagować – również w ramach współpracy międzynarodowej, której charakter wyzwań niejednokrotnie wymaga.

Drugi aspekt relacji między technologiami a zdrowiem ma bardziej pozytywny wydźwięk i wiąże się z

ogromnymi możliwościami, jakie cyfryzacja tej sfery daje w odniesieniu do zwiększania skuteczności leczenia i profilaktyki.

Diagnoza sytuacji wokół cyfryzacji sektora zdrowia w Polsce wskazuje na zaawansowaną, ale wciąż rozwijającą się infrastrukturę e-zdrowia. Wg unijnego raportu o stanie cyfrowego zdrowia ostatniej dekady, Polska zajmuje, odpowiednio, 6. oraz 5. miejsce pod względem dostępu do Elektronicznej Dokumentacji Medycznej (EDM) oraz dostępu do technologii wśród 27 krajów UE31, zajmując miejsce poniżej średniej dla UE jedynie w zakresie kategorii dostępnych dla pacjenta danych.

Kluczowymi elementami polskiego cyfrowego zdrowia jest Platforma e-Zdrowie (P1) oraz różnorodne rejestry, systemy dziedziczne i platformy regionalne. Platforma P1 stanowi centralny punkt cyfrowych usług zdrowotnych, oferując m.in. e-recepty, elektroniczne skierowania, a także dostęp do EDM. Rozwój tej platformy wpłynął na zwiększenie wykorzystania Internetowego Konta Pacjenta (IKP), z którego korzysta obecnie ponad 18 mln Polaków. Wskazać należy też na sukces wdrożenia systemu e-recept, który pozwolił na wystawienie 2 mld e-recept do kwietnia 2024³². Wprowadzone w pierwszej kolejności e-

31 <https://op.europa.eu/en/publication-detail/-/publication/78938111-461e-11ee-92e3-01aa75ed71a1/language-en>

32 <https://pacjent.gov.pl/aktualnosc/48-proc-polakow-uzywa-ikp>

usługi zdrowotne stanowią jednak przede wszystkim cyfrowe odzwierciedlenie tradycyjnych procesów i nie wykorzystują pełni potencjału digitalizacji.

Na poziomie lokalnym, wg badania stopnia informatyzacji Podmiotów Wykonujących Działalność Leczniczą (PWL) prowadzonego przez Centrum e-Zdrowia, na koniec 2023 roku ponad 84% szpitali prowadziło EDM w podstawowym zakresie, 78% wdrożyło indeksowanie EDM w P1, a ponad 1/3 prowadzi wymianę EDM z innymi podmiotami³³. Odsetek ten jest znacznie niższy dla podmiotów niebędących szpitalami.

Warunkiem rozwoju usług cyfrowych w zdrowiu jest zapewnienie bezpieczeństwa danych.

Mimo działań podejmowanych przez Centrum e-Zdrowia oraz Ministerstwo Zdrowia, poziom cyberbezpieczeństwa na poziomie lokalnym nadal nie jest zadowalający. Wg danych ankietowych Centrum e-Zdrowia na kwiecień 2022 roku, 81% podmiotów leczniczych nie ma planu zarządzania podatnościami, w 68% brak odmiejscowionych kopii bezpieczeństwa, a 86% kierowników jednostek nie odbyło szkoleń z zakresu cyberbezpieczeństwa³⁴.

Istotnym problemem dla rozwoju e-zdrowia jest również silosowość danych, która nie pozwala uzyskać pełnego obrazu zdrowia pacjenta, i brak demokratycznych zasad dostępu do danych na cele badawczo-rozwojowe (R&D). Niejasne zasady dostępu do zgromadzonych już danych, w tym wątpliwości dotyczące podstawy prawnej przetwarzania danych o stanie zdrowia w celach R&D – oraz niepewność co do adekwatności zebranych w centralnych rejestrach danych³⁵ wpływają na spowolnienie rozwoju medycyny.

Odsetek podmiotów leczniczych korzystających z nowych technologii, takich jak sztuczna inteligencja, jest rosnący i wynosi obecnie prawie 7% dla szpitali³⁶. Rośnie również zainteresowanie i świadomość korzyści wynikających ze stosowania AI w medycynie.

33 https://cez.gov.pl/sites/default/files/paragraph.attachments.field_attachments/2023-12/vii_edycja_raport_2023.pdf

34 Dane Centrum e-Zdrowia

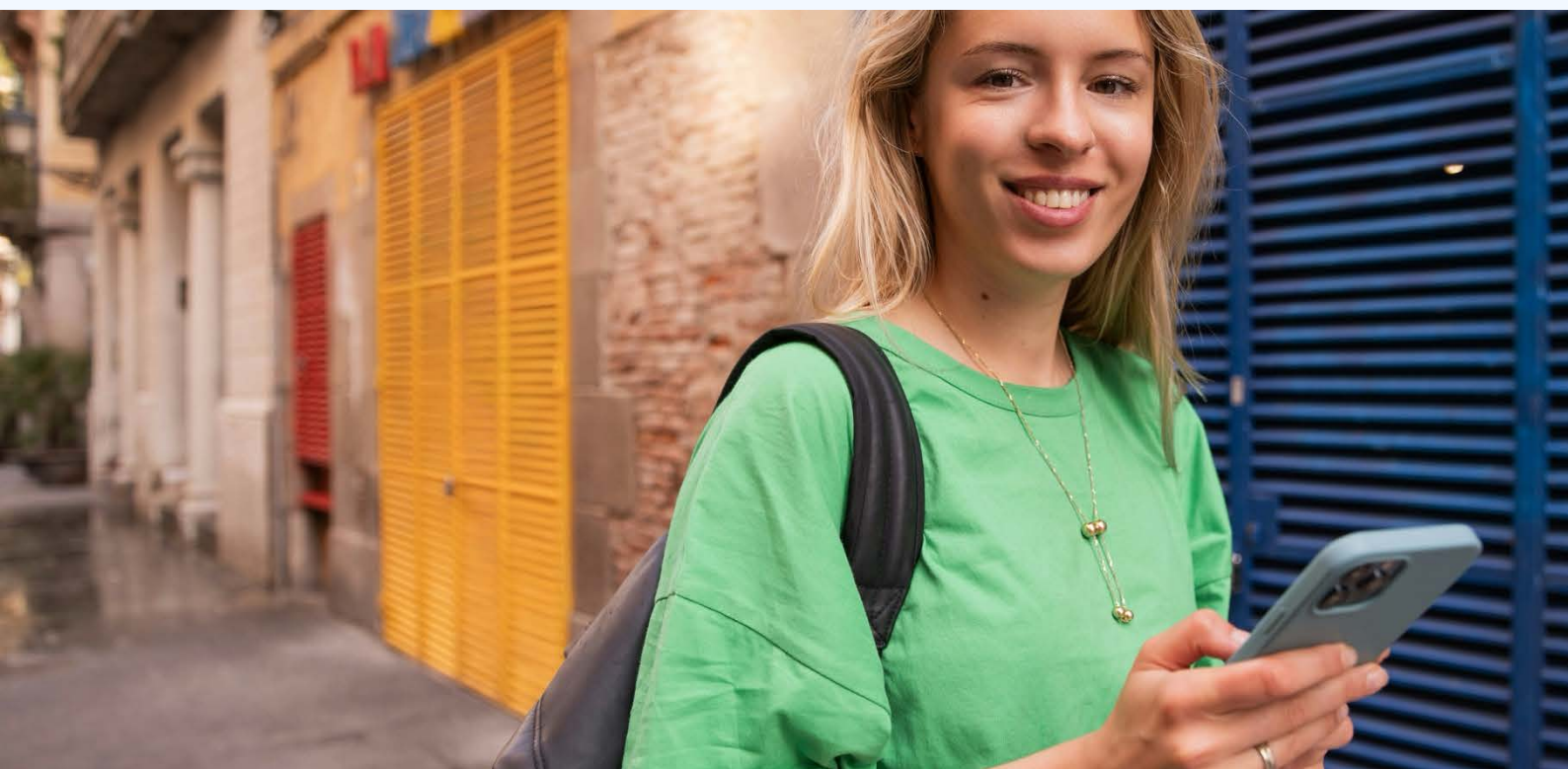
35 <https://www.mdpi.com/1660-4601/19/19/11964>

36 https://cez.gov.pl/sites/default/files/paragraph.attachments.field_attachments/2023-12/vii_edycja_raport_2023.pdf

Cel 1: Państwo działa na rzecz minimalizacji negatywnego wpływu technologii cyfrowych na dobrostan psychiczny

Co umożliwi realizację celu:

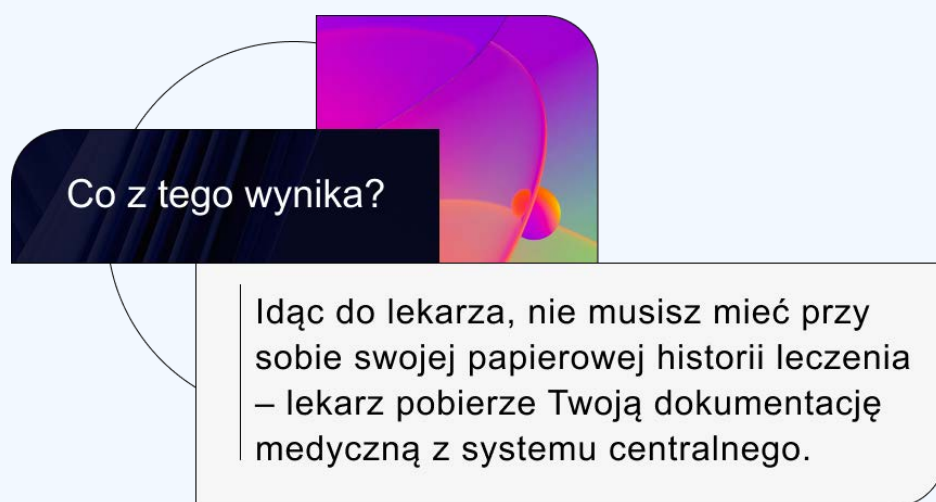
- a) Uruchomienie programu finansowania badań wpływu technologii cyfrowych na zdrowie psychiczne i rozwój psychospołeczny obywateli, w szczególności dzieci i młodzieży.
- b) Realizacja kampanii społecznych i informacyjnych na temat higieny cyfrowej i praw obywateli (w tym zwłaszcza dzieci) w przestrzeni cyfrowej.
- c) Wdrażanie środków zapobiegających wykorzystywaniu seksualnemu małoletnich w internecie;
- d) Wprowadzenie standardów ochrony małoletnich w produktach i usługach cyfrowych. Powinny one:
 - Opierać się o utworzony katalog treści destrukcyjnych;
 - Nakładać na dostawców produktów i usług cyfrowych obowiązek prewencji lub przynajmniej interwencji w przypadku pojawienia się w ich produktach i usługach treści uwzględnionych w katalogu;
 - Zakładać wykorzystanie narzędzi skutecznej weryfikacji wieku użytkownika, przy zachowaniu anonimowości i ochrony jego danych osobowych;
 - Wykluczać rozwiązania prowadzące do utraty kontroli nad czasem ekranowym;
 - Wprowadzać rozwiązania chroniące wizerunek dzieci i młodzieży w internecie.



Cel 2: Elektroniczna Dokumentacja Medyczna jest powszechna, kompletna i prowadzona w sposób umożliwiający wymianę dokumentacji między podmiotami leczniczymi

Co umożliwi realizację celu:

- a) Dalszy rozwój systemów e-usług zdrowotnych w systemie P1;
- b) Wdrożenie systemu zachęt finansowych dla podmiotów, które prowadzą EDM wraz z indeksowaniem w systemie P1 oraz możliwością wymiany dokumentacji z innym podmiotem;
- c) Umożliwienie wzbogacania danych gromadzonych w systemie P1 o dane gromadzone przez urządzenia noszalne i wszczepialne;
- d) Uspójnienie sposobu prowadzenia dokumentacji medycznej szczególnie w zakresach, w których dane nie są zesłownikowane;
- e) Promowanie interoperacyjności pomiędzy systemami informatycznymi w ochronie zdrowia i jakości gromadzonych danych.



Cel 3: Dysponujemy dużymi zasobami wiarygodnych danych o stanie zdrowia, a zasady dostępu do nich dla celów R&D są transparentne, demokratyczne i efektywne

Co umożliwi realizację celu:

- a) Wdrożenie działań operacyjnych w związku z wejściem w życie European Health Data Space (Europejskiej Przestrzeni Danych Medycznych) oraz Data Governance Act (Aktu w sprawie zarządzania danymi);
- b) Promowanie idei dawstwa (altruizmu) danych medycznych wśród pacjentów;
- c) Uregulowanie zasad dostępu do danych jednostkowych i statystycznych na cele R&D, w tym wystandaryzowanie zasad dostępu do danych gromadzonych w rejestrach publicznych oraz dokumentacji medycznej przechowywanej przez PWDL;
- d) Ustalenie standardu anonimizacji i pseudonimizacji danych medycznych.



Co z tego wynika?

Będziesz mieć szerszy dostęp do nowych terapii, wytycznych, rozwiązań cyfrowych, które są dostosowane do diagnozowania i leczenia takich pacjentów jak Ty. Będziesz decydować o tym, co się dzieje z Twoimi danymi medycznymi.

Cel 4: Sztuczna inteligencja oraz inne nowe technologie cyfrowe są wykorzystywane w sposób bezpieczny i skuteczny dla poprawy jakości opieki nad pacjentem.

Co umożliwi realizację celu:

- a) Finansowanie stosowania nowych technologii cyfrowych w zdrowiu, w tym AI i aplikacji zdrowotnych, ze środków publicznych w ramach świadczeń gwarantowanych, poprzez m. in.:
- b) Uwzględnienie tych rozwiązań w opisie standardu istniejących świadczeń gwarantowanych,
- c) Wprowadzenie mechanizmu refundacji dla tych rozwiązań,
- d) Alokowanie niezbędnych środków na pokrycie kosztów finansowania tych rozwiązań,
- e) Wprowadzenie niezbędnych zmian w administracji publicznej, w tym wprowadzenie nowych przepisów, procedur i wzmocnienie kompetencji w zakresie finansowania i monitorowania rozwiązań cyfrowych, m. in. poprzez stworzenie standardu oceny kosztowo-efektywności technologii opartych o AI przez Agencję Oceny Technologii Medycznych i Taryfikacji.
- f) Wprowadzenie nowych e-usług zdrowotnych umożliwiających analizę danych medycznych gromadzonych w rejestrach centralnych w celu profilowania zdrowotnego, analityki predykcyjnej i podejmowania interwencji w oparciu o uzyskane wyniki np. kontakt z pacjentem czy porada edukacyjna, przy uwzględnieniu najwyższych standardów prywatności i umożliwieniu pacjentowi zadecydowania, czy chce być objęty takim programem;
- g) Rozszerzenie modułu e-recept o dwustronną komunikację, umożliwiającą wyświetlanie alertów umożliwiających optymalizację farmakoterapii;
- h) Prowadzenie uczciwej komunikacji i edukacji w zakresie możliwości i ograniczeń związanych ze stosowaniem AI w zdrowiu skierowanej zarówno do pacjentów, jak również do pracowników medycznych;
- i) Dostosowanie wytycznych ministerialnych dla kierunków medycznych do edukacji studentów zakresie nowych technologii cyfrowych, w tym AI;
- j) Ułatwienie dostępu dla pacjenta do informacji dot. organizacji opieki zdrowotnej i wiedzy medycznej przy wykorzystaniu sztucznej inteligencji.



Co z tego wynika?

Otrzymasz leczenie z wykorzystaniem najnowocześniejszej, sprawdzonej technologii. Będziesz otrzymywać informacje o ryzyku zachorowania zanim nastąpi incydent zdrowotny, co umożliwi Ci podjęcie działań profilaktycznych.



Cel 5: W sposób kompleksowy i transparentny monitorujemy jakość interwencji zdrowotnych, w oparciu o dane ze świata rzeczywistego

Co umożliwi realizację celu:

- a) Umożliwienie bieżącego monitorowania ścieżek diagnostyczno-leczniczych pacjentów o określonym profilu, bazującego na realnych danych ze świata rzeczywistego;
- b) Wprowadzenie publicznie dostępnego systemu monitorowania jakości udzielanych świadczeń w PWDL;
- c) Zapewnienie dostępu do danych ze świata rzeczywistego dla celów wdrażania instrumentów dzielenia ryzyka dla technologii lekowych i wybranych technologii nielekowych, opartych o mierzalny efekt zdrowotny dla pacjentów, przy czym dane te w formie statystycznej dostępne byłyby publicznie.



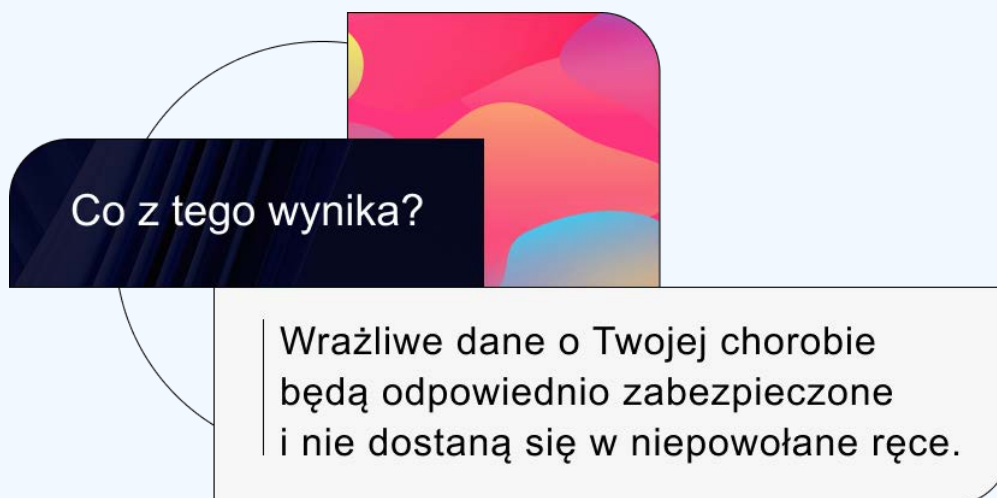
Co z tego wynika?

Otrzymasz świadczenia medyczne o najwyższej jakości, która będzie potwierdzona na podstawie realnych danych.

Cel 6: Poziom cyberbezpieczeństwa w PWDL i centralnych repozytoriach danych jest wysoki.

Co umożliwi realizację celu:

- a) Kontynuowanie programów dofinansowań dla szpitali w celu poprawy infrastruktury IT oraz wzmocnienia cyberbezpieczeństwa, w tym korzystania z usług wyspecjalizowanych podmiotów trzecich;
- b) Przekształcenie Sektorowego Zespołu Cyberbezpieczeństwa w Centrum e-Zdrowia w sektorowy CSIRT oraz wzmocnienie go w zakresie proaktywnego wspierania PWDL w utrzymaniu odpowiedniego poziomu cyberbezpieczeństwa;
- c) Regularne szkolenia dla kadry zarządzającej jednostkami leczniczymi oraz personelu medycznego w zakresie podstawowej wiedzy z cyberbezpieczeństwa;
- d) Zwiększenie budżetu przeznaczanego na cyberbezpieczeństwo systemów centralnych;
- e) Dostosowanie wytycznych ministerialnych dla kierunków medycznych do edukacji studentów w zakresie podstawowych zasad cyberbezpieczeństwa;



3.3 Branże kreatywne

Diagnoza – jak jest?

Przemysły kreatywne są stosunkowo nowym sektorem światowej gospodarki, opierającym się na kreatywnych, innowacyjnych i wynikających z talentu działaniach twórców szeroko pojętej sztuki, mediów i projektowania. Specyfiką sektora jest wysoki poziom wartości dodanej charakteryzujący wytwarzane w nim dobra, który bazuje na zaawansowanej i multidyscyplinarnej wiedzy twórców. Znaczenie gospodarcze sektora rośnie zarówno w odniesieniu do generowanej wartości, jak i rynku. W 2021 r. sektory kultury i kreatywne w Polsce wygenerowały bezpośrednio 31,2 mld złotych wartości dodanej. Uwzględniając wpływ pośredni było to nawet ponad 82 mld PLN (3,58 proc. PKB). Pod względem udziału wartości dodanej tworzonej w tych sektorach w PKB Polska znajduje się poniżej średniej UE, jednak gdy weźmie się pod uwagę również wpływ pośredni Polska zajmuje trzecie miejsce w Europie, ustępując tylko Cyprowi i Szwecji (spośród 15 badanych państw).

Mierzenie wpływu tego sektora na rozwój państwa nie może jednak być mierzone jedynie wskaźnikami gospodarczymi.

Lokuje się on bowiem na przecięciu obszarów gospodarki, kultury, technologii i biznesu – ma duże znaczenie kulturotwórcze i edukacyjne, sprzyjając jednocześnie innowacyjności. Jego rozwój jest zaś relatywnie mało zależny od wykorzystania surowców naturalnych czy infrastruktury przemysłowej. Zmiany społeczne, ważne dla budowania popytu na produkty i usługi, rysują dobre perspektywy dla rozwoju branż kreatywnych. Nie sposób jednak pominąć kilku istotnych zagrożeń. Można wśród nich wymienić m.in. niewystarczające finansowanie, niesprzyjające i skomplikowane regulacje prawne, wzrost konkurencji międzynarodowej czy deficyt wykwalifikowanych pracowników.

Z perspektywy strategii cyfryzacji, spośród różnorodnych przemysłów kreatywnych – na które składają się m.in. przemysły filmowy oraz muzyczny, media i rynek wydawniczy szczególne znaczenie ma sektor gier wideo i powiązanego z nim e-sportu. W Polsce funkcjonuje blisko 500 spółek prowadzących działalność w branży gier wideo, które w 2022 roku osiągnęły przychody rzędu 128 mln EUR³⁷. Polską specjalizacją są gry klasy premium na duże platformy sprzętowe – komputery i konsole. Pod względem liczby zatrudnionych osób w branży (15 tys. osób), Polskę w Europie wyprzedza jedynie Wielka Brytania oraz Francja. Eksportowy charakter sektora (krajowa sprzedaż nie przekracza kilku procent) oznacza konieczność konfrontacji z nasiloną konkurencją, w tym ze strony największych światowych graczy. Tymczasem zarówno polski, jak i światowy gamedev mierzy się z kryzysem, wynikającym m.in. z odwrócenia nieorganicznych trendów wzrostowych z czasów pandemii.

37 https://en.parp.gov.pl/storage/publications/pdf/The_Game_Industry_Poland_2023_12_07.pdf

W kontekście rozwoju branży należy uwzględnić także jej kulturowy i kulturotwórczy aspekt.

Po gry sięgają już nie tylko dzieci, młodzież i ludzie w średnim wieku, lecz także osoby starsze, a w związku ze starzeniem się polskiego społeczeństwa, zjawisko tzw. *silver gamingu* będzie coraz powszechniejsze. Trend ten jest istotny z perspektywy myślenia o dostępności gier dla szerokiego grona odbiorców, w tym osób z niepełnosprawnościami. Uznajemy, że gry powinny być traktowane jako tekst kultury podobnie jak filmy czy literatura, co oznacza m.in. wsparcie dla ich polonizacji i archiwizacji. Konieczne jest jednak nieustanne zwracanie uwagi na kwestie higieny cyfrowej i przeciwdziałania uzależnieniom.

Działania państwa powinny objąć także obszar e-sportu, czyli profesjonalnych rozgrywek w branży gier. Globalny rynek e-sportu w 2023 roku osiągnął wartość 3,8 miliarda USD; przewidywane tempo jego rocznego wzrostu do 2028 r. to 14,8%. Polska zajmuje 20. miejsce na arenie międzynarodowej z sektorem o wartości 596 milionów dolarów³⁸. Krajowi gracze mogą pochwalić się zauważalnymi osiągnięciami, w Polsce odbywa się też jedna z największych światowych imprez branżowych. Rynek e-sportu wciąż się rozwija, co w dużej mierze wiąże się z przenikaniem kultury gamingowej do kultury popularnej. Zwiększająca się obecność gamingu i e-sportu w kulturze popularnej przyciąga więcej widzów, a także sponsorów. Należy więc spodziewać się dalszej popularyzacji tego obszaru, w tym wśród polskich dzieci i młodzieży. Tymczasem jednak środowisko nie jest wolne od (propagowanych na popularnych kanałach) negatywnych wzorców – toksycznych zachowań graczy względem siebie, niekorzystnego wpływu długotrwałej gry na zdrowie fizyczne i psychiczne, dyskryminacji ze względu na płeć etc. Należy więc zaś z jednej strony wspierać rozwój środowiska i polskie sukcesy, z drugiej zwalczać wciąż pojawiające się w tym sektorze negatywne tendencje.



³⁸ <https://markethub.pl/rynek-e-sportu/>

Cel 1: Rozwój branży gamingowej jest szybki

Co umożliwi realizację celu:

- a) Rozwinięcie istniejącego wsparcia dla producentów gier poprzez powiększenie kwot, o które mogą się oni ubiegać, i rozciągnięcie programów wsparcia na kilka lat;
- b) Wsparcie w promocji i marketingu gier na rynkach docelowych, szczególnie tych trudnych ze względu na geograficzną odległość i koszty, jak USA, oraz budowanie pozytywnej atmosfery poprzez wykorzystanie narzędzi z zakresu dyplomacji kulturalnej i ekonomicznej w miejscach istotnych dla branży;
- c) Wsparcie w wykorzystaniu szans jakie niesie rewolucja AI dla rozwoju branży gier;
- d) Utworzenie lub dostosowanie zadań jednej z instytucji rządowych posiadającej kompetencje oraz narzędzia umożliwiające świadczenie realnego i wymiernego wsparcia, w tym mentorskiego, tylko dla branży gier wideo;
- e) Systemowe wsparcie dla programów stażowych i stypendialnych ułatwiających wejście w branżę młodym, zdolnym ludziom oraz ułatwienia podatkowe dla studiów zatrudniających osoby stawiające pierwsze kroki w branży;
- f) Ułatwienia dla studiów zatrudniających wysokiej klasy ekspertów oraz managerów spoza Polski w obszarach, gdzie brak wykwalifikowanych polskich pracowników;
- g) Wsparcie dla procesów lokowania oddziałów zagranicznych firm w Polsce oraz oddziałów polskich firm poza granicami kraju;
- h) Wsparcie, we współpracy z sektorem akademickim, edukacji w zakresie kompetencji niezbędnych w studiach tworzących gry: programowanie gier, projektowanie grafiki, realizacja dźwięku, pisanie scenariuszy, zarządzanie firmą, etc.;
- i) Wsparcie przez instytucje publiczne lokalnych wydarzeń branżowych o zasięgu międzynarodowym;
- j) Walka z toksycznością w środowisku gamedevu, działania na rzecz większej inkluzywności branży (szczególnie w stosunku do kobiet), walka z patologiami środowiska pracy (np. praca w godzinach nadliczbowych, mobbing etc.) i promowanie właściwych relacji między pracownikami i pracodawcami;
- k) Promowanie gier wideo jako dzieła kultury – ze szczególnym uwzględnieniem polskich wersji językowych (zarówno gier polskich producentów, jak i zagranicznych);
- l) Opracowanie mechanizmu archiwizacji polskich gier wideo;
- m) Promowanie implementacji technologii dostępnościowych w grach wideo.

Cel 2: Bariery prawne utrudniające rozwój branży e-sportowej w Polsce są likwidowane, a e-sport popularyzowany

Co umożliwi realizację celu:

- a) Stosowanie prawnych aspektów e-sportu, w skład których wchodzi m.in. prawnoautorski status gier wideo, odzwierciedleń wizerunków i transmisji wydarzeń e-sportowych;
- b) Popularyzacja zawodów e-sportowych poprzez wsparcie w organizacji amatorskich zawodów na poziomie szkolnym;
- c) Promowanie profilaktyki zdrowia fizycznego i psychicznego u graczy, a także pozytywnych i inkluzywnych zachowań społecznych;
- d) Wprowadzenie specjalistycznych programów edukacyjnych w szkołach i na uczelniach wyższych, które będą kształcić przyszłych profesjonalistów w dziedzinie e-sportu, zarówno jako zawodników, jak i menedżerów czy analityków;
- e) Stworzenie przepisów prawnych, które będą regulować kwestie związane z e-sportem, takie jak kontrakty zawodników, prawa do transmisji czy ochrona młodzieży;
- f) Reprezentowanie polskiego e-sportu na międzynarodowych konferencjach i targach branżowych;
- g) Finansowanie i pomoc organizacyjna dla lokalnych klubów e-sportowych, które promują zdrową rywalizację i rozwój talentów.



Cel 3: Branże kreatywne są wspierane w procesie rozwoju

Co umożliwi realizację celu:

- a) Dotacje i granty na rozwój projektów kreatywnych, umożliwiające artystom i firmom rozwijanie nowych projektów i technologii;
- b) Wsparcie rozwoju programów edukacyjnych i szkoleń, które kształcą w zakresie kreatywności, nowych technologii i zarządzania projektami kreatywnymi, a także współpraca z uniwersytetami i szkołami wyższymi w celu rozwijania programów nauczania dostosowanych do potrzeb branż kreatywnych;
- c) Uwzględnienie w stypendiach i programach mentorskich dla młodych talentów w obszarze kultury branż kreatywnych i ich specyfiki;
- d) Tworzenie klastrów i inkubatorów, które zapewniają przestrzeń do pracy, wsparcie techniczne i możliwość współpracy z innymi podmiotami z branży;
- e) Działania ułatwiające twórcom dostęp do nowoczesnych technologii i narzędzi, które wspierają twórczość i innowacje;
- f) Organizowanie kampanii promujących polskie branże kreatywne na arenie międzynarodowej, w tym uczestnictwo w targach i wystawach;
- g) Wzmocnienie przepisów dotyczących ochrony własności intelektualnej, co zapewni twórcom lepszą ochronę ich prac i zachęci do innowacji;
- h) Wspieranie organizacji konferencji, warsztatów i spotkań networkingowych, które umożliwią wymianę doświadczeń i nawiązywanie kontaktów;
- i) Tworzenie partnerstw z sektorem prywatnym w celu realizacji wspólnych projektów i inicjatyw wspierających rozwój branż kreatywnych;
- j) Wprowadzenie programów wsparcia dla startupów, które oferują mentoring, dostęp do finansowania i sieci kontaktów branżowych;
- k) Wspieranie współpracy międzybranżowej i międzysektorowej.



3.4 Cyfrowa akademia

Diagnoza – jak jest?

Rozwój cyfrowego państwa i gospodarki wymaga współpracy z akademią i sektorem naukowym, ale także dostrzeżenia konieczności długofalowego wsparcia dla rozwoju tego obszaru.

Bez oparcia się o silną krajową bazę naukową, polska sfera cyfrowa nie będzie rozwijała się harmonijnie.

Tymczasem polska nauka zmagają się ze strukturalnymi problemami, wynikającymi m.in. z niskiej atrakcyjności kariery, w szczególności wśród początkujących naukowców. Odpływ kadr oraz relatywnie niski odsetek absolwentów STEM stanowią poważne przeszkody dla rozwoju zrównoważonego systemu szkolnictwa wyższego i nauki, a niewielki przepływ doświadczonych naukowców między nauką a przemysłem ogranicza innowacyjność gospodarki. Te strukturalne problemy ulegają wzmocnieniu w przypadku kierunków ICT, które od lat dominują ranking wynagrodzeń w systemie monitorowania Ekonomicznych Losów Absolwentów³⁹. Ze względu na silną presję ze strony przemysłu część studentów nie kończy studiów, koncentrując się na rozwoju kariery zawodowej. Bardzo niewiele osób decyduje się na karierę akademicką, co prowadzi do coraz silniej obserwowanej luki pokoleniowej w wielu ośrodkach akademickich⁴⁰. Na braki specjalistów IT wskazuje także raport Polskiego Instytutu Ekonomicznego przygotowany we współpracy z Software Development Association Poland (SoDA)⁴¹. Z kolei przygotowany przez Uniwersytet Stanforda raport „2024 AI Index Report” sugeruje, że te luki doprowadziły już do spadku liczby kształconych w Polsce specjalistów ICT⁴².

Negatywne trendy w rozwoju talentów IT są poważnym problemem, zwłaszcza za względu na szybki rozwój AI. Coraz większe strategiczne znaczenie tej technologii sprawia, że konieczny jest jej rozwój na poziomie krajowym. Polski system akademicki musi ulec wzmocnieniu w zakresie kształcenia specjalistów AI oraz możliwości horyzontalnego wykorzystania AI w interdyscyplinarnych badaniach naukowych. Należy podkreślić, że ze względu na dwa unikatowe wypracowane przez lata uwarunkowania, polska nauka jest w dobrej pozycji startowej w wyścigu o prymat w nadchodzących zmianach. Po pierwsze, mimo braku wzrostu ilości studentów, mamy bardzo wysoki poziom kształcenia informatycznego, a polskiej szkole algorytmiki i programowania zawdzięczamy istotne sukcesy polskich informatyków w licznych konkursach, zawodach i olimpiadach. Po drugie, Polska jest jednym z liderów informatyzacji szkolnictwa wyższego i nauki w Europie, przede wszystkim dzięki

39 <https://ela.nauka.gov.pl/>

40 <https://www.zycieuczelni.p.lodz.pl/luka-pokoleniowa-problem-dla-uczelni-i-biznesu/>

41 https://pie.net.pl/wp-content/uploads/2022/11/PIE_Raport_Ilu-specjalistow-IT-brakuje-w-Polsce.pdf

42 <https://aiindex.stanford.edu/report/>

sieci Zintegrowanego Systemu Informacji o Szkolnictwie Wyższym i Nauce POL-on, a także budowanych na jej podstawie e-usług publicznych.



Cel 1. Pracownicy akademicki kluczowi dla rozwoju kadr na potrzeby cyfrowego państwa są efektywnie wspierani w pracy naukowej i dydaktycznej.

Co umożliwi realizację celu:

- a) Zadbanie o stabilność i bezpieczeństwo zatrudnienia w uczelni. Stworzenie mechanizmów uznawania znaczenia naukowej mobilności międzysektorowej (w tym wzajemnego uznawania doświadczenia między sektorami) oraz zmiany systemu oceny publikacji na skoncentrowaną na jakości i znaczeniu wyników prowadzonych badań. W technologiach cyfrowych bardzo wielu badaczy często przepływa między nauką a przemysłem, dlatego ważne jest promowanie znaczenia takiego przemysłowego doświadczenia w uczelni, oraz akademickiego w przemyśle. Dzięki tak ułatwionemu przepływowi ludzi zwiększy się i zacieśni współpraca nauki z biznesem;
- b) Zwiększenie wsparcia finansowego dla młodych naukowców w dziedzinie ICT. Uznajemy, że bez zabezpieczenia godnego poziomu życia znacznie trudniej o dobre wyniki naukowe. Planujemy także poszukiwanie innych modeli wsparcia finansowego oraz nagród i premii za badania i publikacje IT, AI i STEM we wszystkich dyscyplinach;
- c) Promocja kariery naukowej w zakresie STEM w obszarze nowych technologii, jako dającej duże możliwości rozwoju – od pracy w jednostkach i centrach badawczych, na uczelniach po zakładanie startupów. Wsparcie współpracy między różnymi typami jednostek badawczych;
- d) Ustrukturyzowanie w zakresie nietradycyjnych ścieżek kariery, w tym stworzenie stanowisk inżynierów badawczych na uczelniach, oraz inne mechanizmy zapewniające lepszą mobilność między sektorem publicznym i prywatnym. Zwiększenie znaczenia doświadczenia zdobytego w przemyśle w karierze akademickiej.

Cel 2: Polska nauka jest wspierana przez zaawansowaną infrastrukturę informatyczną.

Co umożliwi realizację celu:

- a) Inwestycje w moce obliczeniowe na potrzeby prowadzenia badań naukowych, w szczególności potrzebne do wykorzystania AI w interdyscyplinarnych dziedzinach nauki. Zwiększenie mocy obliczeniowych musi następować razem z stworzeniem w ramach HPC (wysokowydajne przetwarzanie, ang. high-performance computing)/plGRID systemów raportowania obciążenia, liczby projektów/grantów oraz wspartych startupów;
- b) Dalszy rozwój systemów POL-on (Zintegrowany System Informacji o Szkolnictwie Wyższym i Nauce), ELA (Ekonomiczne Losy Absolwentów) i OSF (Obsługa Strumieni Finansowania), aby stały się referencyjnymi źródłami danych dla e-usług publicznych pozwalającymi skuteczniej mierzyć i analizować efektywność realizowanych projektów naukowych i komercjalizować wyniki badań;
- c) Rozwój e-usług cyfrowych skierowanych do kandydatów na studia, studentów, doktorantów i absolwentów uczelni takich jak: system wspierający kandydatów na studia w wyborze uczelni i kierunku studiów, eDyplomy, udostępnienie zestawu narzędzi wspierających właściwy wybór kierunków studiów, mLegitymacje;
- d) Stworzenie portalu, który semi-automatycznie, dzięki wsparciu AI, tworzyłby bazę technologii, usług i infrastruktury, oraz gromadził w jednym miejscu potencjał badawczy, komercjalizacyjno-wdrożeniowy, usługowy i aparaturowy wszystkich jednostek naukowych w Polsce. Byłby on dostępny z jednej strony dla instytucji naukowych, z drugiej – dla przedsiębiorców, którym umożliwiłby nawiązywanie współpracy np. w celu realizacji wspólnych projektów w konsorcjach naukowo-przemysłowych.



Cel 3: Polska nauka w dziedzinie ICT jest widoczna na arenie międzynarodowej

Co umożliwi realizację celu:

- a) Promocja oraz umiędzynarodowienie polskiej nauki, m.in. poprzez współpracę z najlepszymi uczelniami w Europie i na świecie oraz propagowanie sukcesów polskich informatyków;
- b) Rozwój dyplomacji naukowej w zakresie podwyższenia poziomu pozyskiwania zagranicznych środków publicznych (w tym europejskich) na badania naukowe.
- c) Dostosowanie i poprawa systemu oceny parametrycznej jednostek naukowo-badawczych tak by bardziej wspierała komercjalizację wyników badań naukowych oraz wypracowanie nowych ścieżek komercjalizacji badań uwzględniających nowoczesne, międzynarodowe modele prowadzenia badań;
- d) Wsparcie udziału polskich instytucji oraz naukowców w międzynarodowych sieciach oraz organizacjach technologicznych, które na celu mają wspieranie rozwoju w sektorze ICT;
- e) Wzmocnienie wiodących uczelni informatycznych i centrów badawczych oraz stworzenie w Polsce instytucji badawczych, które mają szansę zyskać renomę międzynarodową. Uznajemy, że istnienie w kraju instytucji badawczych o renomie międzynarodowej jest jednym z najbardziej skutecznych działań przeciwdziałających drenażowi mózgów. Wykorzystanie Instytutu IDEAS, który poprzez prowadzenie interdyscyplinarnych badań będzie promował też wykorzystania AI w zróżnicowanych dziedzinach.



Biznes i technologie



Ministerstwo
Cyfryzacji

Tu tworzymy przyszłość

Biznes i technologie

4.1 Cyfrowa transformacja przedsiębiorstw

Diagnoza – jak jest?

W 2023 r. ponad trzy czwarte polskich przedsiębiorstw została zakwalifikowana do grupy o bardzo niskiej lub niskiej intensywności cyfrowej, a jedynie 21% przedsiębiorstw charakteryzowało się wysokim lub bardzo wysokim poziomem intensywności cyfrowej. 99,8% ogółu przedsiębiorstw w Polsce tworzy sektor MŚP, który generuje 43,6% PKB (dane za 2020 r.). Małe i średnie przedsiębiorstwa pełnią kluczową rolę w rozwoju polskiej gospodarki, a ich transformacja cyfrowa jest warunkiem utrzymania i poprawy pozycji konkurencyjnej Polski na rynku międzynarodowym.

W 2023 r. odsetek przedsiębiorstw mających szerokopasmowy dostęp do Internetu wyniósł prawie 99%. 36% przedsiębiorstw korzystało z oprogramowania typu ERP (ang. Enterprise Resource Planning), a sprzedaż poprzez sieci komputerowe prowadziło 18%. W 2022 r. prawie 73% przedsiębiorstw wystawiało i wysyłało faktury elektroniczne, w tym nienadające się do automatycznego przetwarzania – 67%, a tych, które mogły być automatycznie przetwarzane – 14,8%⁴³. W 2023 r. ze średniozaawansowanych i zaawansowanych technologii chmurowych korzystało 47% firm, z analityki danych – 19%, a ze sztucznej inteligencji – 4% firm⁴⁴. 32% MŚP nie wykorzystuje żadnych narzędzi cyfrowych (39% wśród mikrofirm), natomiast te, które ich używają, najczęściej wskazują podstawowe narzędzia cyfrowe, jak media społecznościowe i płatności online (38%). Tylko 14% używa chmury, a 13% narzędzi informatycznych do zarządzania procesami.

Poziom cyfryzacji przedsiębiorstw skorelowany jest z ich wielkością: im większe, tym przeciętnie więcej wydatków przeznaczają na prace badawczo-rozwojowe i wdrażanie nowych technologii.

Podobna zależność występuje w przypadku innowacyjności przedsiębiorstw: największy odsetek podmiotów aktywnych innowacyjnie występuje wśród przedsiębiorstw dużych. Częściej wprowadzane są innowacje w procesach biznesowych niż innowacje produktowe.

⁴³ Społeczeństwo informacyjne w Polsce w 2023 r., GUS

⁴⁴ Dane za: Eurostat 2023

Innym aspektem cyfrowej transformacji jest wdrażanie zaawansowanych technologii Przemysłu 4.0. Diagnoza wdrażania Przemysłu 4.0 w Polsce na lata 2022-2024 wskazuje na stopniowe, choć nierównomierne postępy w adaptacji nowoczesnych technologii w różnych sektorach gospodarki, jak również w zależności od wielkości przedsiębiorstwa (najczęściej technologie te wdrażają duże firmy o przychodach przekraczających 500 milionów złotych). Polska jest w początkowej fazie wdrażania Przemysłu 4.0, jednak z dużym potencjałem wzrostu, zwłaszcza wśród dużych przedsiębiorstw. Niemniej niskie tempo adopcji technologii przełomowych i brak długoterminowych planów w zakresie technologii Przemysłu 4.0 stawia polski przemysł w niekorzystnej pozycji w porównaniu z innymi krajami Unii Europejskiej, gdzie inwestycje w cyfryzację są na wyższym poziomie.

Poziom zaawansowania technologicznego polskich firm, w tym zwłaszcza małych i średnich przedsiębiorstw, wymaga podniesienia, aby możliwy był wzrost ich produktywności.

To z kolei jest warunkiem dalszego, dynamicznego rozwoju polskiej gospodarki. Z badań dotyczących produktywności polskich przedsiębiorstw wynika, że istnieje duży potencjał do zwiększenia jej poziomu dzięki zastosowaniu usprawnień w postaci nowoczesnych narzędzi cyfrowych.

W Polsce dominuje produkcja niskoseryjna o dużej różnorodności, dlatego tradycyjne podejście do cyfryzacji, automatyzacji i robotyzacji nie może przynieść oczekiwanych efektów ekonomicznych. Różnego typu zaawansowane urządzenia, maszyny, obrabiarki i roboty wymagają wykwalifikowanej obsługi ludzkiej. Niż demograficzny może jeszcze bardziej pogorszyć obecną sytuację. Koszty przygotowania produkcji oraz pozyskania nowych zleceń stanowią większy udział w ogólnych kosztach produkcji. Ten obszar w ogóle nie jest objęty automatyzacją.

Poza zaprojektowaniem odpowiednich instrumentów wsparcia finansowego dla firm konieczne są również działania związane ze zwiększaniem świadomości firm z korzyści, jakie niesie za sobą zastosowanie nowych technologii, rozwój kompetencji i umiejętności pracowników oraz osób zarządzających przedsiębiorstwami w zakresie stosowania nowoczesnych rozwiązań cyfrowych, a także rozwój systemu otoczenia biznesu sprzyjającego innowacjom.

Do głównych barier w obszarze transformacji cyfrowej należą⁴⁵:

- brak przekonania o korzyściach – typu zysk z inwestycji w cyfryzację;
- niedobór specjalistów na rynku oraz brak kompetencji, w szczególności w zakresie umiejętności tworzenia oprogramowania, złożonej analizy danych i matematycznych, umiejętności zarządzania projektem z wykorzystaniem narzędzi IT czy opracowania strategii cyfrowej i zdolności przywódczych;

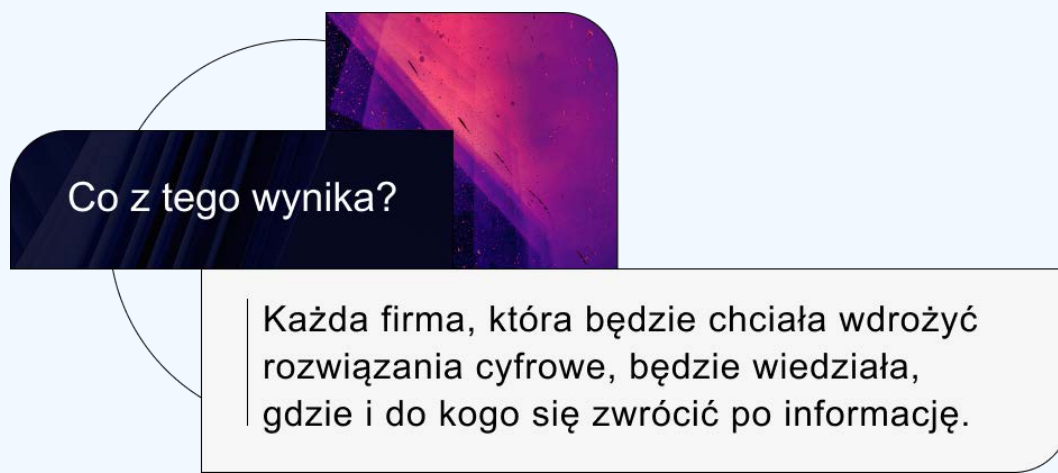
45 eSkills for Jobs Index, Dojrzałość technologiczna polskich firm oraz raport BGK z 2024 r. Cyfryzacja w sektorze MŚP – szanse i ograniczenia

- wysokie koszty wdrożenia narzędzi cyfrowych i brak odpowiednich możliwości finansowania;
- brak czasu na wdrażanie rozwiązań cyfrowych;
- problemy z bezpieczeństwem informatycznym.

Cel 1: Funkcjonuje sprawny system zarządzania działaniami w obszarze wspierania transformacji cyfrowej przedsiębiorstw

Co umożliwi realizację celu:

- a) Powołanie podmiotu koordynującego transformację cyfrową przedsiębiorstw, w tym zwłaszcza sektora MŚP, który definiowałby cele i działania, monitorował postępy, oceniał stopień realizacji zakładanych celów, identyfikował potrzeby technologiczne oraz oczekiwania i możliwości MŚP;
- b) Opracowanie wspólnej i spójnej na poziomie krajowym wizji cyfryzacji przedsiębiorstw, w tym przede wszystkim sektora MŚP, uwzględniającej wpływ dużych przedsiębiorstw na cyfryzację MŚP w ich łańcuchu dostaw, a także określającej strategię i standardy, które będą wspierać integrację MŚP z cyfrowymi rozwiązaniami wdrażanymi przez duże firmy;
- c) Zapewnienie zrozumiałości i dostępności informacyjnej programów wspierających cyfryzację przedsiębiorstw;
- d) Udostępnienie w jednym miejscu kompleksowej informacji o dostępnych programach wsparcia oraz przeznaczonych dla przedsiębiorców materiałach i szkoleniach.



Co z tego wynika?

Każda firma, która będzie chciała wdrożyć rozwiązania cyfrowe, będzie wiedziała, gdzie i do kogo się zwrócić po informację.

Cel 2: Przedsiębiorcy postrzegają transformację cyfrową jako proces ułatwiający działalność firmy i zwiększający jej efektywność

Co umożliwi realizację celu:

- a) Prowadzenie działań edukacyjnych budujących świadomość korzyści płynących z procesu cyfryzacji oraz rozwoju kompetencji cyfrowych pracowników i kadry menedżerskiej;
- b) Ocena istniejących rozwiązań wspierających cyfryzację przedsiębiorstw oraz zaprojektowanie, na podstawie przeprowadzonej diagnozy, i zaimplementowanie nowych instrumentów wspierających transformację cyfrową przedsiębiorstw, które będą dopasowane do potrzeb poszczególnych kategorii przedsiębiorców;
- c) Określenie branż kluczowych, które gwarantują transfer technologii i tworzenie wewnętrznego łańcucha dostaw opartego na rodzimych firmach, w których Polska posiada potencjał do przewagi konkurencyjnej i skierowanie w te obszary celowanych działań. Kluczowe będą te branże, które mają istotny wpływ na polskie PKB, duży udział w eksporcie oraz znaczący potencjał wzrostu produktywności w wyniku transformacji cyfrowej i wdrażania technologii Przemysłu 4.0.;
- d) Wprowadzenie instrumentu „Cyfrowy start dla biznesu”, który wspierałby nowopowstałe firmy w rozwoju cyfrowym. Pakiet ten zawierałby propozycje rozwiązań, cyfryzujących procesy biznesowe już na początku działania firmy i ułatwiających jej prowadzenie – np. oprogramowanie biurowe, księgowo i finansowe, zarządzania relacjami z klientami oraz dokumentami, programy do komunikacji i współpracy, oprogramowanie cyberbezpieczeństwa, ewentualnie systemy planowania zasobów przedsiębiorstwa;
- e) Świadczenie usług dla przedsiębiorców polegających w szczególności na doradztwie, szkoleniach, rozwoju umiejętności, możliwości przetestowania i eksperymentowania rozwiązań w ramach pilotaży oraz wsparcia w znalezieniu źródeł finansowania transformacji cyfrowej (na przykładzie sieci EDIH – European Digital Innovation Hubs, czyli europejskich centrów innowacji cyfrowych).



Co z tego wynika?

Ułatwimy przedsiębiorstwom zrozumienie korzyści z cyfryzacji i poprowadzimy je za rękę przez transformację cyfrową, proponując najlepsze dla firmy narzędzia.



Cel 3: Cyfrowe usługi publiczne dla przedsiębiorców są proaktywne i dojrzałe, a interoperacyjność systemów umożliwia zredukowanie obciążeń administracyjnych

Co umożliwi realizację celu:

- a) Rozwijanie usług publicznych do coraz wyższego stopnia dojrzałości, opartych o potrzeby użytkowników, które proponują użytkownikom wykonanie czynności lub akceptację działań wykonanych przez system;
- b) Pełna cyfryzacja relacji między przedsiębiorcami a państwem (w tym m.in. poprzez cyfryzację zamówień publicznych czy procesów budowlanych);
- c) Wprowadzenie zasady „tylko raz”, co oznacza, że obywatele i przedsiębiorstwa dostarczają swoje dane administracji publicznej tylko raz, a administracja publiczna następnie wewnętrznie udostępnia te dane pomiędzy instytucjami, unikając obciążania obywateli i przedsiębiorców.



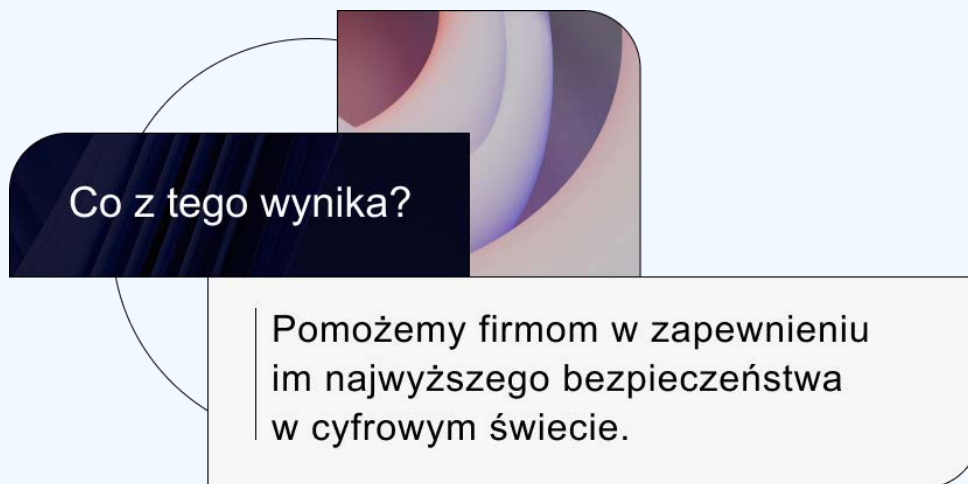
Co z tego wynika?

Kontakt firmy z administracją publiczną będzie ograniczony do niezbędnego minimum, a urzędy między sobą wymieniają się danymi. Firma nie będzie zmuszona do kilkukrotnego podawania tych samych danych różnym urządzeniom.

Cel 4: Przedsiębiorcy są świadomi cyberzagrożeń i sięgają po instrumenty zapobiegawcze.

Co umożliwi realizację celu:

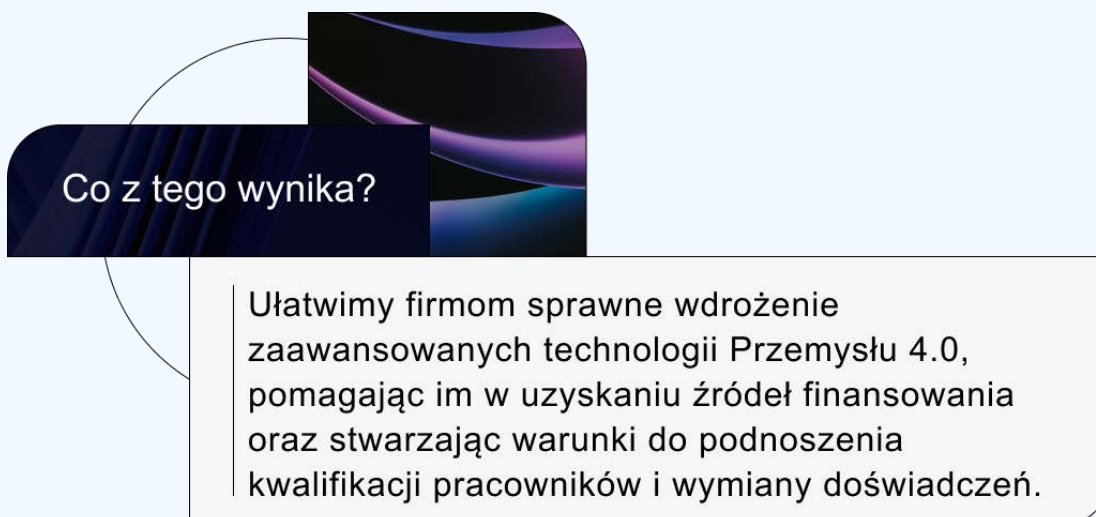
- a) Rozpowszechnianie podstawowych informacji z zakresu cyberbezpieczeństwa;
- b) Udostępnianie (również w ramach „Cyfrowego Startu dla Biznesu”) szkoleń i kursów obejmujących zakresem tematykę m.in. cyberzagrożeń i dezinformacji;
- c) Wprowadzenie systemu dobrowolnej certyfikacji cyberbezpieczeństwa w przedsiębiorstwach;
- d) Powiązanie systemu certyfikacji cyberbezpieczeństwa z ubezpieczeniami od ryzyk cyberbezpieczeństwa i uzależnienie wysokości składki z posiadany ubezpieczeniem.



Cel 5: Przedsiębiorcy z sektora przemysłu są świadomi korzyści wykorzystywania technologii Przemysłu 4.0 i wdrażają je w swoich firmach

Co umożliwi realizację celu:

- a) Wspieranie adopcji zaawansowanych technologii Przemysłu 4.0 poprzez stymulację współpracy międzyinstytucjonalnej, w tym współpraca z technicznymi ośrodkami akademickimi w celu opracowania programów podnoszących kwalifikacje pracowników przemysłowych, współpraca między sektorem publicznym a prywatnym w celu budowy nowoczesnych centrów danych i platform cyfrowych;
- b) Tworzenie platform wymiany wiedzy online, które umożliwiają przedsiębiorstwom dzielenie się doświadczeniami i przykładami najlepszych praktyk w zakresie Przemysłu 4.0;
- c) Ułatwianie przedsiębiorcom dotarcie do źródeł finansowania technologii Przemysłu 4.0, w tym ulg podatkowych i grantów na innowacje, kredytów technologicznych i programów pilotażowych wdrożeń.



4.2 Sztuczna inteligencja

Diagnoza – jak jest?

Implementacja najnowszych technologii oraz korzystanie z systemów opartych na zorientowanej na człowieka, zrównoważonej, godnej zaufania bezpiecznej i sprzyjającej włączeniu społecznemu sztucznej inteligencji (AI) są kluczowe dla rozwoju Polski.

Technologia ta może znacząco poprawić moce produkcyjne w przemyśle, efektywność i jakość świadczonych usług, a także wspierać procesy decyzyjne i zarządzanie zasobami.

AI jako technologia automatyzująca procesy jest również kluczowym narzędziem pozwalającym ograniczyć negatywne skutki trendów demograficznych. Wreszcie, technologia ta ma potencjał transformacyjny we współpracy z innymi przełomowymi technologiami, takimi jak chmura obliczeniowa czy internet rzeczy. Ten konglomerat, którego centralnym elementem jest AI, określany bywa jako AI+. Rośnie liczba i skala inwestycji w produkty i usługi AI⁴⁶. W tym wyścigu stawką jest udział w szybko rosnącym rynku AI i powiązanych z nim korzyści – eksportu ICT, wzrostu produktywności i innowacji. Dzisiejsze oszacowania wskazują, że do końca dekady korzyści te sięgną 10% globalnego produktu brutto, zaś wartość samego rynku AI przekroczy 1,3 bln USD. Kraje uczestniczą w tym wyścigu tworząc atrakcyjne warunki dla inwestorów i innowatorów. Polska jest w nim poza światową czołówką, wyprzedzają nas – prócz globalnych gigantów – kraje europejskie takie jak Wielka Brytania, Niemcy, Szwecja, Hiszpania⁴⁷. Jednak wyścig ten jest na wczesnym etapie i zmiana tego stanu rzeczy jest konieczna i możliwa.

W kontekście rozwoju AI przed Polską stoi szereg wyzwań strukturalnych. Budowa i rozwój przyjaznego ekosystemu AI w Polsce wymaga równoczesnej stymulacji tempa wzrostu inwestycji publicznych, jak i prywatnych w badania i innowacje, przy czym to drugie jest szczególnym wyzwaniem w odniesieniu do małych i średnich firm. Aby znaleźć się w gronie liderów konieczne jest również budowanie świadomości przedsiębiorców o korzyściach ze stosowania AI/AI+, zwiększenie dostępu do specjalistycznej wiedzy oraz mocy obliczeniowych.

Kluczowym potencjałem dla rozwoju sektora są specjaliści. Od początku 2020 r. do pierwszej połowy 2023 r. nadano w Polsce około 19 tys. stopni doktora, w tym 622 w dyscyplinach związanych z informatyką i 207 z tematyki sztucznej inteligencji. To wskaźniki, które plasują nas poza pierwszą 15. w Europie w kategorii absolwentów kierunków informatycznych, zarówno ilościowo jaki i w przeliczeniu na 100,000 mieszkańców⁴⁸.

46 <https://www.goldmansachs.com/insights/articles/ai-investment-forecast-to-approach-200-billion-globally-by-2025.html>

47 [https://www.europarl.europa.eu/RegData/etudes/ATAG/2024/760392/EPRS_ATA\(2024\)760392_EN.pdf](https://www.europarl.europa.eu/RegData/etudes/ATAG/2024/760392/EPRS_ATA(2024)760392_EN.pdf)

48 Stanford Institute for Human-Centered Artificial Intelligence, 2024 AI Index Report, Chapter Education, 2024

Konieczne jest przyjęcie i egzekwowanie spójnych ram prawnych, stosowania standardów i kodeksów dobrych praktyk, a także podniesienie poziomu dostępu do wysokiej jakości infrastruktury (teleinformatycznej, obliczeniowej, energetycznej). Polska ma obowiązek przeprowadzenia procesu legislacyjnego – wdrożenia uzgadniającego krajowy porządek prawny z unijnym AI Act i prawem międzynarodowym, czego efektem będzie obowiązywanie przepisów dotyczących sztucznej inteligencji w Polsce. Przed Polską stoi również wdrożenie zbieżnej z regulacjami unijnymi Konwencji Ramowej o sztucznej inteligencji, prawach człowieka, demokracji i praworządności przyjętej przez Komitet Ministrów Rady Europy.

Ważne jest wdrożenie tych regulacji w sposób sprzyjający innowacjom, równoważący troskę o godną zaufania, bezpieczną AI, z zadbaniami o rozwój i wdrażanie innowacji w przedsiębiorstwach.

Ta równowaga powinna przejawiać się zarówno w podejściu instytucjonalnym (rola i zakres działania polskich organów nadzoru współpracujących z europejskim Biurem ds. AI), jak i w systemie finansowania inwestycji. Jednocześnie, państwo nie może decydować się na wdrażanie konkretnej technologii bez przeprowadzania pogłębionych analiz dotyczących spodziewanych efektów i ryzyk wynikających z implementacji. Państwo powinno stosować AI tam, gdzie maksymalnie ułatwi życie obywatelom i realnie odpowie na potrzeby społeczne, a jednocześnie nie wygeneruje nadmiernych ryzyk.

Stąd też silna potrzeba aktualizacji polityki publicznej dotyczącej rozwoju sztucznej inteligencji w Polsce, w tym wskazanie obszarów strategicznych dla rozwoju gospodarki, w których AI powinna być wdrażana priorytetowo. Taka polityka musi uwzględniać aktualne trendy i wyzwania oraz zapewniać spójność i koordynację na szczeblu rządowym prowadzonym i międzynarodowym. Nowa polityka zostanie przygotowana w oparciu o cztery filary: innowacje, inwestycje, edukację oraz wdrożenia.

Polacy mają wysoką świadomość istnienia sztucznej inteligencji – 98,8 proc. osób deklaruje, że o niej słyszało⁴⁹. Połowa Polaków (51,1 proc.) uważa, że sztuczna inteligencja przyniesie społeczeństwu więcej korzyści niż szkód. Jednocześnie 25 proc. badanych było przekonanych, że szkody wyrządzone przez AI przewyższą korzyści. Polacy darzą AI sporym zaufaniem, 41 proc. badanych jest skłonnych polegać na informacjach dostarczanych przez sztuczną inteligencję. Mimo tego 40 proc. wskazuje na potrzebę zapewnienia nadzoru człowieka nad rozwojem AI.

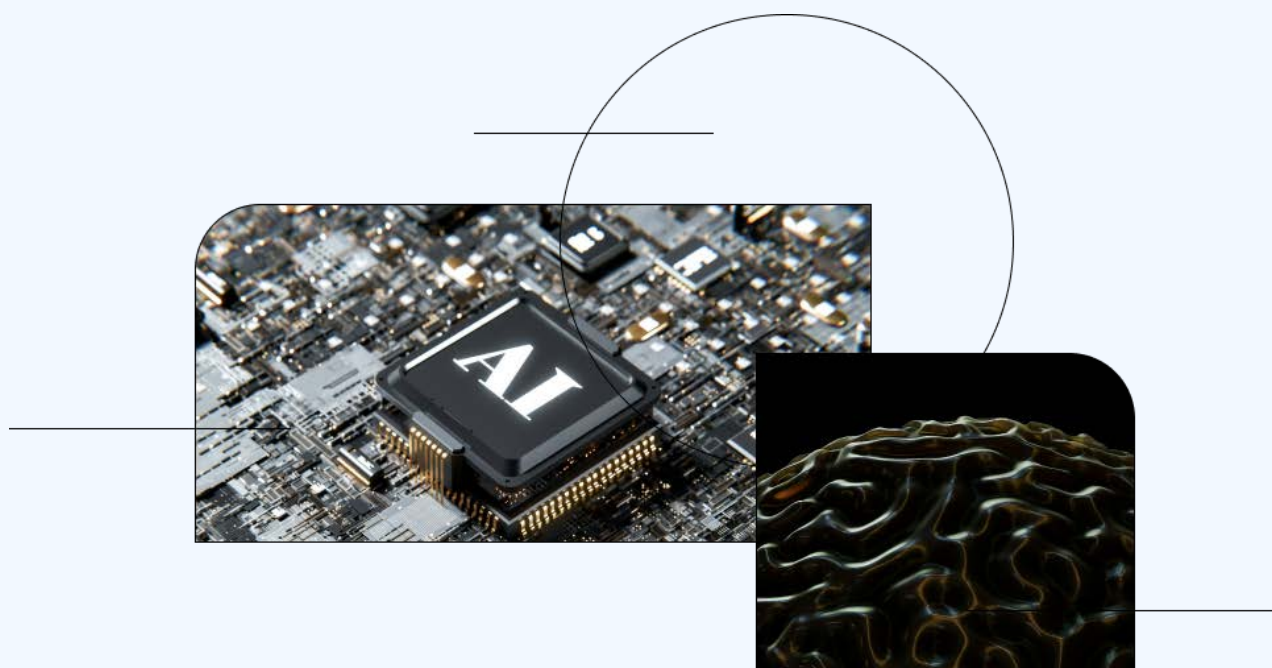
Polacy w dużej mierze⁵⁰ wyrażają poparcie dla wykorzystania AI przez państwo. Według 60,4 proc. sztuczna inteligencja powinna być wykorzystywana przy tworzeniu cyfrowych usług publicznych. Zdaniem 32 proc. badanych sztuczna inteligencja może przyspieszyć i zautomatyzować procesy administracyjne oraz skrócić czas realizacji usług publicznych. Inną często podnoszoną przez badanych nadzieją na wykorzystanie AI w usługach publicznych, jest zwiększenie ich dostępności dla osób z niepełnosprawnościami. Polacy są

49 <https://pie.net.pl/wp-content/uploads/2024/09/Sztuczna-inteligencja-w-administracji-publicznej.pdf>

50 <https://pie.net.pl/wp-content/uploads/2024/09/Sztuczna-inteligencja-w-administracji-publicznej.pdf>

niechętni wobec wykorzystania sztucznej inteligencji do zautomatyzowanego podejmowania decyzji administracyjnych, które mogą mieć wpływ na ich życie. Natomiast wyższym poparciem darzą możliwość automatyzacji prostych czynności administracyjnych, ostrzegania w sytuacjach nadzwyczajnych czy wykorzystania AI jako wsparcia dla obywateli przy wypełnianiu dokumentów.

Podsumowując, kluczowe dla rozwoju technologii jest stworzenie szerokiego ekosystemu AI+, który obejmuje współpracę publicznych i prywatnych podmiotów w zakresie edukacji, badań, innowacji, produkcji oraz bezpiecznego wdrażania rozwiązań z wykorzystaniem sztucznej inteligencji.



Cel 1: Rozwój gospodarki, przemysłu cyfrowego, dobrostanu społecznego i autonomii człowieka jest wspierany przez sprawny i skoordynowany ekosystem sztucznej inteligencji

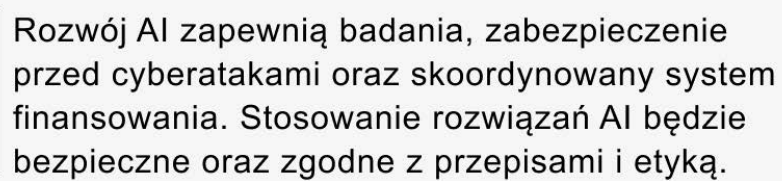
Co umożliwi realizację celu:

- a) Stworzenie zgodnego z przepisami unijnymi oraz przyjaznego dla przedsiębiorczości systemu nadzoru nad modelami i systemami AI, dzięki czemu obywatele, konsumenci i firmy będą miały świadomość oraz pewność, że rozwiązania AI używane na rynku i w administracji publicznej są bezpieczne, zgodne z przepisami i etyką;
- b) Wyłonienie instytucji wiodącej w zakresie badań nad AI oraz koordynacja współpracy instytucji badawczych zajmujących się badaniami w zakresie sztucznej inteligencji wchodzących w skład ekosystemu podmiotów zajmujących się tą tematyką;
- c) Zagwarantowanie przejrzystego, skoordynowanego i efektywnego finansowania rozwoju polskich firm w obszarze AI i innowacji cyfrowych, a także zwiększanie poziomu wsparcia (prywatnego, publicznego) dla przedsiębiorców rozwijających i wdrażających AI;
- d) Utworzenie zgodnych z podejściem unijnym piaskownic regulacyjnych (sandboxów) dla innowatorów;
- e) Stworzenie jednolitej, dostępnej publicznie listy systemów AI używanych w administracji publicznej wraz z opisem funkcji oraz podstawowych parametrów technicznych dostępnych dla obywateli w celu zwiększenia transparentności administracji publicznej. Opracowanie i egzekwowanie zasad stosowania AI w administracji publicznej;
- f) Stworzenie albo wyłonienie podmiotu odpowiedzialnego za bezpieczeństwo AI na światowym poziomie, którego zadaniem będzie badanie najnowszych zagrożeń związanych z szybkim rozwojem tej technologii, a także wsparcie w nadzorze nad bezpieczeństwem zastosowań AI. Jego działalność będzie wiązała się z jednej strony z bezpiecznym użytkowaniem i przyszłym rozwojem AI, z drugiej – z cyberbezpieczeństwem rozwiązań AI i zabezpieczeniem przed cyberatakami z wykorzystaniem tej technologii. Instytucja będzie prowadziła globalną współpracę z innymi instytucjami tego typu;
- g) Wypracowanie z partnerami (polskimi i międzynarodowymi) narzędzi oraz prowadzenie stosowanych regularnych badań w kreowaniu polityk publicznych poświęconych wpływowi technologii AI na rynek pracy, gospodarkę, środowisko oraz społeczeństwo uwzględniających zarówno potencjały, jak i zagrożenia, z uwzględnieniem sytuacji osób zagrożonych wykluczeniem;

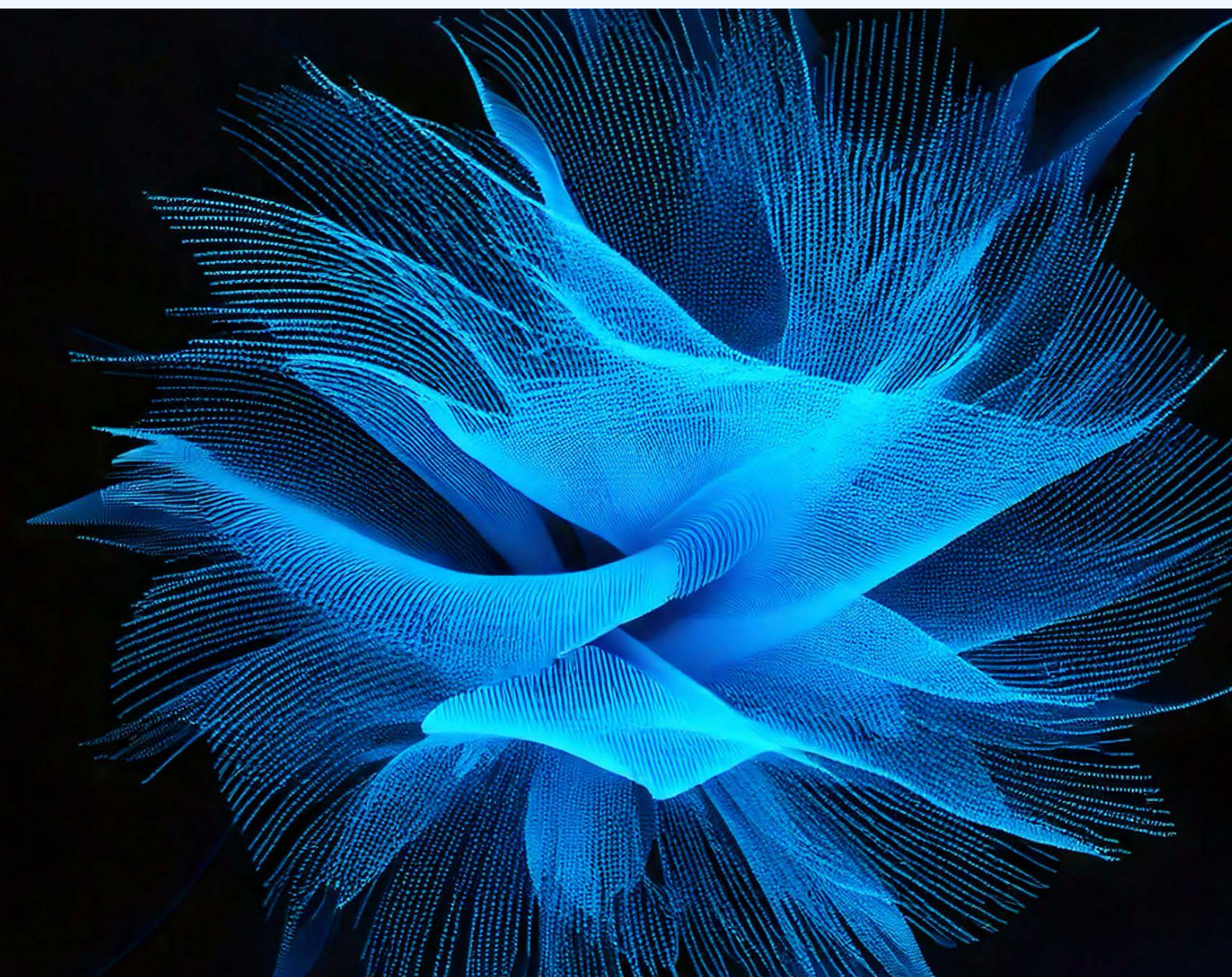
- h) Utworzenie cyfrowych standardów struktur danych zgodnych ze standardami ISO i IEC dla wszystkich gałęzi gospodarki w celu budowania i uczenia modeli AI



Co z tego wynika?



Rozwój AI zapewnią badania, zabezpieczenie przed cyberatakami oraz skoordynowany system finansowania. Stosowanie rozwiązań AI będzie bezpieczne oraz zgodne z przepisami i etyką.



Cel 2: Realizacja i finansowanie R&D oraz wdrożeń sztucznej inteligencji odbywa się w sposób efektywny i transparentny

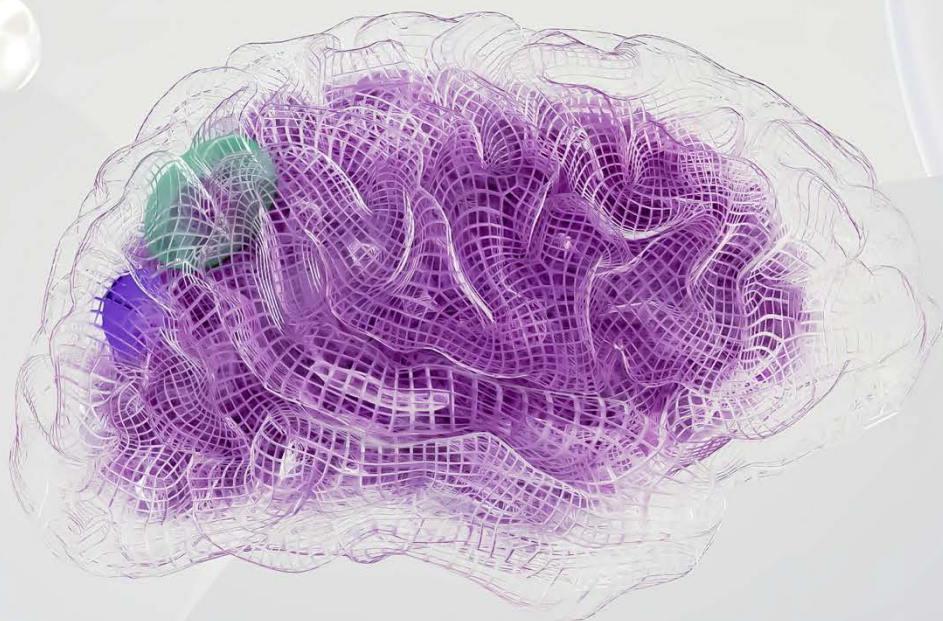
Co umożliwi realizację celu:

- a) Stworzenie i zarządzanie mechanizmem koordynacji obecnych funduszy, konkursów i sposobów ich realizacji, aby uniknąć duplikacji działań i nieefektywnego wydatkowania środków inwestycyjnych wraz z koniecznością centralizowania agendy badawczej, rozwojowej oraz wdrożeniowej;
- b) Priorytetyzacja w sfinansowaniu opracowywania, komercjalizacji i wdrażania innowacji, w tym adaptacji i wykorzystania technologii sztucznej inteligencji przez startupy, administrację publiczną, MŚP i duże przedsiębiorstwa;
- c) Utworzenie jednego miejsca dostępu do informacji o wszystkich źródłach finansowania projektów AI, w którym będzie możliwość znalezienia najbardziej odpowiedniego dla projektu funduszu;
- 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 zakresie AI;
- e) Zapewnienie 50% finansowania krajowego dla projektów związanych ze sztuczną inteligencją współfinansowanych z funduszy unijnych;
- f) Opracowanie i realizacja projektów AI o największym potencjale dla rozwoju gospodarczego i dobrostanu społecznego w Polsce o dużej wartości społecznej lub gospodarczej oraz o największym potencjale dla wejścia Polski do grona liczących się graczy na globalnym rynku sztucznej inteligencji;
- 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.

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 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.



4.3 Inne technologie przełomowe

Diagnoza – jak jest?

Technologie przełomowe w transformacji cyfrowej (niezależnie od wyodrębnionego osobno obszaru sztucznej inteligencji) to m.in. technologie kwantowe, przetwarzanie brzegowe, VR/AR i blockchain, technologie kosmiczne. Niezbędna lub oczekiwana interwencja państwa warunkuje zarówno w wymiarze polskim, jak i europejskim powodzenie szansy utrzymania strategicznej autonomii gospodarki i ograniczanie ryzyka zależności technologicznej od podmiotów zagranicznych. Zastosowanie różnych mechanizmów wsparcia inwestycji przemysłowych, sektora badań i rozwoju, ułatwienia dla startupów, inwestowanie w osiąganie twardych umiejętności w procesie kształcenia zawodowego, a także wdrażanie zastosowań technologii przełomowych w sektorze publicznym ma sprzyjać lokalizacji przedsięwzięć technologicznych w Polsce.

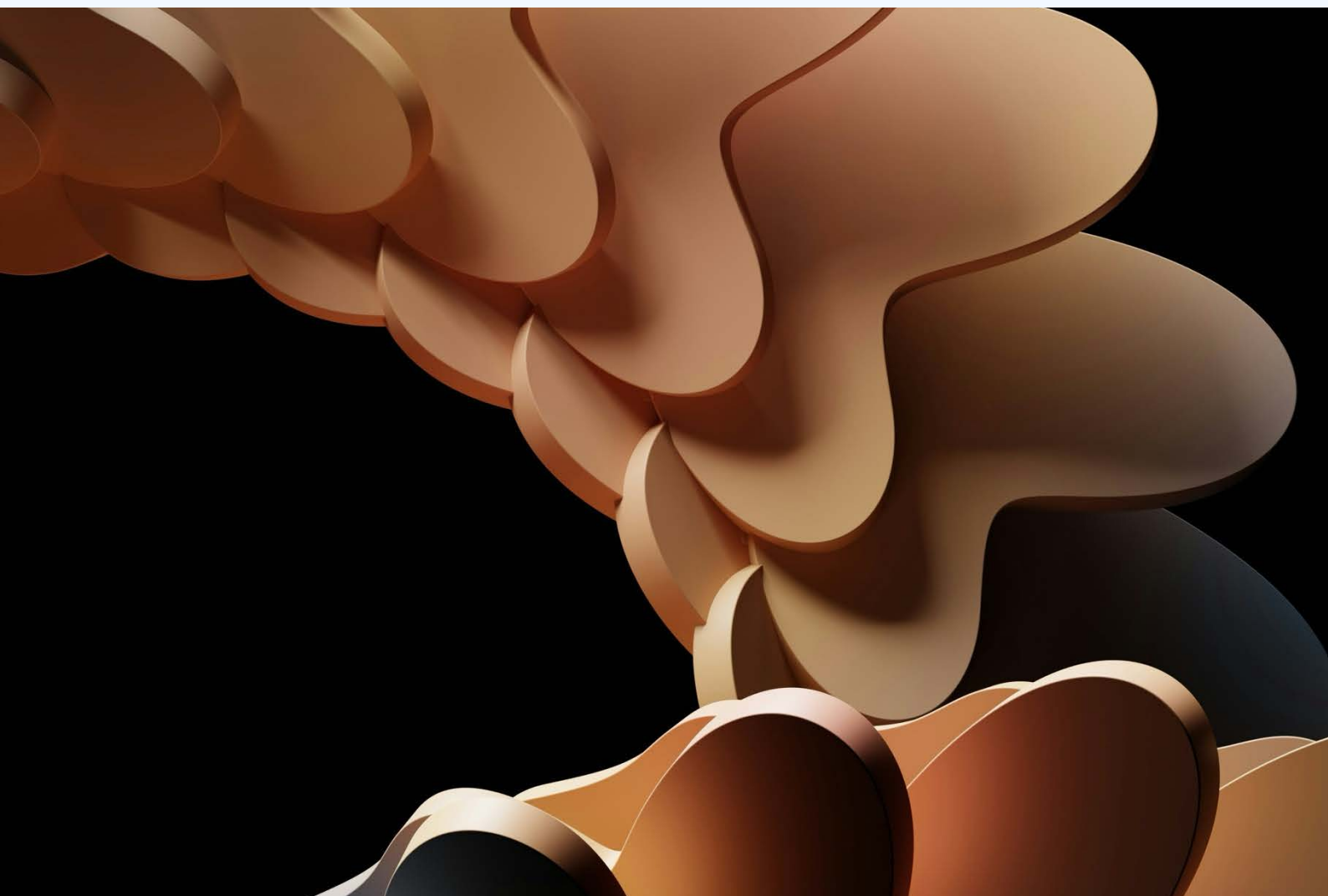
W przypadku najważniejszych trendów technologicznych działania rozwojowe są programowane na poziomie Unii Europejskiej. Polska angażuje się aktywnie w te przedsięwzięcia w projektach międzynarodowych, dających możliwość osiągnięcia ekonomii skali niezbędną w konkurencji globalnej, zarówno pod kątem efektywności łańcucha dostaw, jak i wprowadzania na rynek praktycznych zastosowań. Jest też sygnatariuszem Europejskiej Deklaracji w sprawie technologii kwantowych i przystąpiła do Grupy Koordynacyjnej ds. Technologii Kwantowych. Niektóre już realizowane projekty, jak sieć komunikacji kwantowej EuroQCI (European Quantum Communication Infrastructure) w światłowodowej części naziemnej i segmencie satelitarnym, czy budowa w Polsce komputera kwantowego w ramach europejskiej infrastruktury EuroHPCie nie miałyby szansy powodzenia bez współpracy wielu państw. Wyzwania wciąż obejmują zastosowania, metrologię (sensory), kryptografię postkwantową, czy produkcję mikroprocesorów ery postkwantowej.

Zwiększenie liczby węzłów w systemach przetwarzania brzegowego stało się jednym z celów polityki UE do 2030, dostarczających rynkowi bodźców do optymalizacji sieci przetwarzania danych. Co do zasady infrastruktura sieci przetwarzania danych jest obecnie budowana i utrzymywana głównie przez sektor prywatny, ale aspiracje planów rozwoju systemów AI, IoT, smart cities, sieci 5G nie zawsze idą w parze z planami inwestycji prywatnych. Zapewnienie energooszczędnego rozwoju i cyberbezpieczeństwa ma uzasadnienie w polityce publicznej.

Polska od 2018 roku uczestniczy w Europejskim Porozumieniu Blockchain. W roku 2024 budowana w ramach tego porozumienia europejska sieć blockchain EBSI zostanie przekazana do EUROPEUM-EDIC, nowego podmiotu utworzonego z udziałem Polski w nowych ramach prawnych dla projektów wielokrajowych. Również w tym obszarze współpraca europejska daje okazję do wdrażania wielkoskalowych projektów zastosowań technologii przełomowych w usługach sektora publicznego, które będą katalizować wdrożenia w innych dziedzinach.

Kluczowy dla rozwoju gospodarki cyfrowej przemysł półprzewodnikowy jest w Polsce rozwinięty w niewielkim stopniu – obecnie w Polsce nie prowadzi się masowej produkcji półprzewodników. Jest ona realizowana w skali pilotażowej, co najwyżej małoseryjnej. Są to głównie półprzewodniki do zastosowań specjalnych produkowane w sieci Łukasiewicz – Instytucie Mikroelektroniki i Fotoniki. Polską specyfiką jest także mała liczebność

wykwalifikowanych kadr, co rodzi obawy branży o ich odejście z polskich firm i ośrodków naukowych w sytuacji, gdy w Polsce pojawi się zagraniczny podmiot z dużą inwestycją w tym obszarze. Działalność dydaktyczna skoncentrowana jest w wąskiej grupie ośrodków akademickich takich jak Politechnika Warszawska czy Akademia Górniczo-Hutnicza; widoczne są też choćby obiecujące projekty współprowadzone przez Politechnikę Poznańską. Okazją na nadchodzące lata jest jednak dostrzeżenie wagi tematu na poziomie unijnym, wyrażone przez przyjęcie Aktu w Sprawie Chipów czy dążenie Unii do osiągnięcia poziomu 20 proc. światowej produkcji półprzewodników w 2030 r. Odnotować trzeba również powstanie Krajowych Ram Wspierania Strategicznych Inwestycji Półprzewodnikowych – programu, który ma zapewniać wsparcie lokowania w Polsce kosztownych, zaawansowanych zakładów produkcyjnych.



Cel 1: Rozbudowa ekosystemu badań i kompetencji wspiera rozwój w obszarze technologii przełomowych

Co umożliwi realizację celu:

- a) Stworzenie programu wieloletniego wspierania rozwoju technologii przełomowych w celu koordynacji agendy badawczej, konsolidacji wysiłków i zasobów oraz wyznaczenia wysokopoziomowych kierunków działań na najbliższe lata. Program będzie elastyczny i będzie umożliwiał dostosowanie do zmian technologicznych. Program umożliwi stabilizację pracy naukowej i finansowania interdyscyplinarnych zespołów badawczych. Musi zarazem stawiać na wysokojakościowe współpracy międzynarodowe i dostęp do najlepszego światowego know-how;
- b) Uspójnienie zarządzania agendą badawczą dookoła technologii przełomowych we współpracy ze środowiskiem naukowym, biznesowym i akademickim;
- c) Nawiązanie partnerskich relacji z wiodącymi światowymi ośrodkami badań w zakresie technologii przełomowych.



Cel 2: Technologie kwantowe są wykorzystywane w kluczowych gałęziach gospodarki i obszarach działalności państwa

Co umożliwi realizację celu:

- a) Identyfikowanie kluczowych obszarów, gdzie technologia kwantowa ma potencjał zwiększenia produktywności, bezpieczeństwa i wydajności w polskim kontekście;
- b) Zapewnienie dostępu do know-how i infrastruktury kwantowej ośrodkom akademickim i biznesowi;
- c) Wykorzystanie technologii kwantowych, między innymi w zakresie komunikacji i kryptografii kwantowej w ochronie infrastruktury krytycznej i zwiększaniu bezpieczeństwa państwa. Wykorzystanie technologii kwantowej w modelu podwójnego zastosowania w obronności;
- d) Wykorzystanie metrologii kwantowej w gospodarce, w szczególności przy badaniu i lokalizacji złóż surowców naturalnych;
- e) Wsparcie przedsiębiorczości opartej na produktach/usługach związanych z technologiami kwantowymi (np. akcelerator startupów, konkursy)




Co z tego wynika?

Wykorzystamy technologie kwantowe w najważniejszych obszarach działania państwa, zwiększając ich bezpieczeństwo, produktywność i wydajność.

Cel 3: Technologie internetu rzeczy są wykorzystywane w kluczowych sektorach gospodarki i w ośrodkach miejskich i wiejskich

Co umożliwi realizację celu:

- a) Opomiarowanie akwenów, w szczególności głównych rzek i jezior celem monitorowania jakości wody, poziomu wód i publiczne udostępnianie tych danych mieszkańcom i obywatelom;
- b) Rozwój sieci monitorowania poziomu smogu w miastach i miasteczkach w celu diagnozy jakości powietrza. Opomiarowanie głównych szlaków komunikacyjnych w celu monitorowania ruchu i optymalizacji transportu;
- c) Budowa farm demonstracyjnych zawierających najnowsze rozwiązania internetu rzeczy (IoT), na przykład czujniki wilgotności gleby w każdym województwie, celem edukacji i wdrożenia IoT w sektorze rolniczym;
- d) Zbudowanie 1000 węzłów przetwarzania brzegowego celem efektywnego przetwarzania danych zbieranych z urządzeń IoT;
- e) Zbudowanie platformy smart city w modelu open source dostępnej dla mniejszych miasteczek i wsi w celu popularyzacji rozwiązań inteligentnych miast i wsi w mniej skomunikowanych regionach, przy zapewnieniu ochrony prywatności mieszkańców.



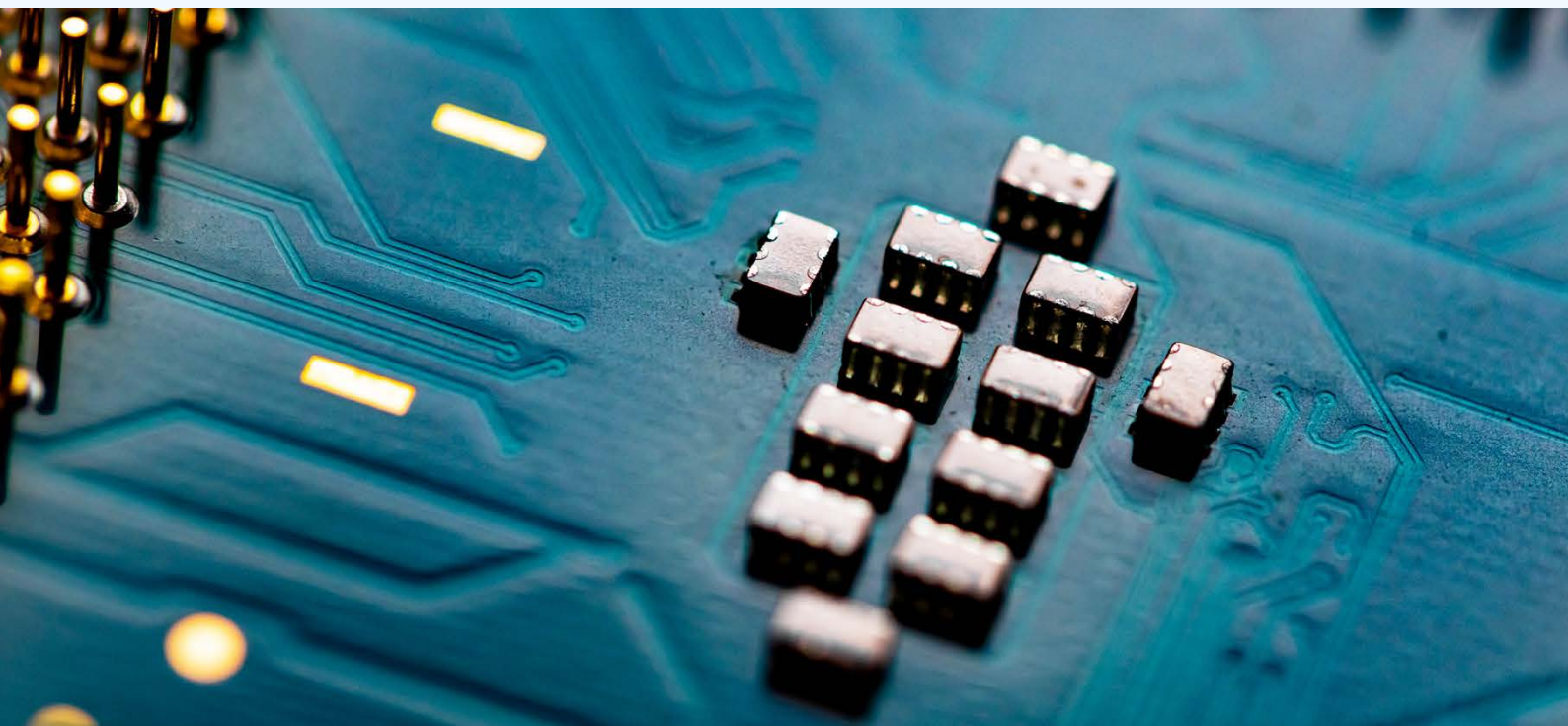
Co z tego wynika?

Wsie i miasta będą miały dostęp do wiedzy i rozwiązań smart city. Wykorzystanie technologii IoT usprawni działanie najważniejszych sektorów gospodarki m.in. umożliwi monitorowanie jakości wód i powietrza oraz monitorowanie ruchu i optymalizację transportu.

Cel 4: Polska rozwija sektor półprzewodników dzięki zwiększonym inwestycjom

Co umożliwi realizację celu:

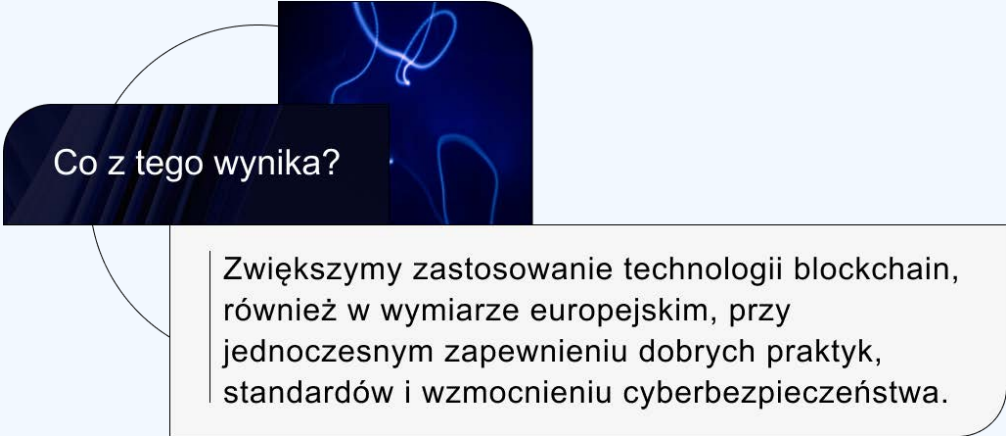
- a) Utworzenie szczegółowej polityki rozwoju sektora półprzewodników w Polsce, uwzględniającej kontekst międzynarodowy (w tym współpracę z państwami kluczowymi dla łańcucha dostaw i wsparcie unijne), zidentyfikowane bariery dla rozwoju i istniejące obszary polskich specjalizacji;
- b) Wsparcie rozbudowy polskiego ekosystemu w sektorze półprzewodników – z uwzględnieniem podmiotów ze wszystkich etapów łańcucha wartości – oraz włączania polskich firm i jednostek badawczych w rozwijający się w Europie łańcuch dostaw;
- c) Zapewnienie stałej współpracy między resortami i instytucjami kluczowymi dla rozwoju sektora półprzewodnikowego w celu zapewnienia synergii inwestycji, również w kontekście europejskim, budowy korzystnych warunków dla inwestorów i sprowadzania inwestycji zagranicznych;
- d) Utworzenie polskiego centrum kompetencji do spraw półprzewodników;
- e) Zabezpieczenie finansowania na pokrycie kosztów dostępu polskich firm (zwłaszcza MŚP) do platformy projektowania półprzewodników w chmurze oraz do pilotażowych linii produkcyjnych;
- f) Długofalowe utrzymanie programu Krajowe Ramy Wspierania Strategicznych Inwestycji Półprzewodnikowych;
- g) Wsparcie rozwoju pilotażowych i małoskalowych linii produkcyjnych w kraju, opartych o model foundry;
- h) Wsparcie tworzenia małej elektroniki opartej na technologii open-source.



Cel 5: Technologie blockchain są wykorzystywane i rozwijane, również w wymiarze europejskim

Co umożliwi realizację celu:

- a) Wdrażanie zastosowań technologii blockchain, gdzie kluczowym czynnikiem jest zwiększenie przejrzystości i rozliczalności wybranych procesów w administracji, sektorze publicznym i gospodarce, w tym likwidowanie pola do nadużyć lub manipulacji, wykorzystanie takich jakich środków jak weryfikowalne poświadczenia, suwerenna tożsamość, europejski portfel tożsamości, e-weksel, pieczęć elektroniczna, trwałe nośniki;
- b) Rozwijanie zdolności europejskiej sieci EBSI i zastosowań blockchain w usługach sektora publicznego poprzez współtworzony przez Polskę wielo-krajowy podmiot EUROPEUM EDIC. Wypracowanie dobrych praktyk we wszystkich testowanych i wdrażanych zastosowaniach technologii blockchain w usługach transgranicznych. Standaryzowanie procesów w usługach, interoperacyjności w rozproszonych systemach rejestrów i usługodawców usług, z zachowaniem ich lokalnej suwerenności, sprawiedliwego dostępu i możliwości użycia w ramach ekosystemu europejskiego;
- c) Integracja zastosowań technologii blockchain w infrastrukturze rynków finansowych i kapitałowych, obejmująca możliwość tokenizacji różnych kategorii papierów wartościowych oraz różnych kategorii praw posiadania, a także systemów płatności, rejestrów akcji;
- d) Wzmacnianie cyberbezpieczeństwa technologii blockchain, a także wykorzystywanie, technologii blockchain do rozwiązywania niektórych problemów z cyberbezpieczeństwem np. w systemach AI.



Co z tego wynika?

Zwiększymy zastosowanie technologii blockchain, również w wymiarze europejskim, przy jednoczesnym zapewnieniu dobrych praktyk, standardów i wzmocnieniu cyberbezpieczeństwa.

4.4 Technologie kosmiczne

Diagnoza – jak jest?

Mimo, iż przemysł kosmiczny wykorzystuje technologie cyfrowe i jest gotowy na wprowadzanie nowych, w dalszym ciągu napotyka problemy we współpracy między uczestnikami zaawansowanych projektów. Domena kosmiczna musi wdrażać cyfryzację w kontekście ograniczonym, wynikającym z procesów, organizacji i doświadczenia technologicznego. Polega to na zapewnieniu realizacji potrzeb interoperacyjności wszystkich narzędzi, między dyscyplinami, w całym cyklu życia i w całym łańcuchu dostaw. W tym kontekście, Europejska Agencja Kosmiczna (ESA) w swoim dokumencie „ESA AGENDA 2025: Make space for Europe”, dokonała harmonizacji niezbędnych przedsięwzięć wskazując społeczności sektora kosmicznego, a w szczególności Delegacjom Państw Członkowskich ESA, kierunki rozwoju i wdrażania wspólnie z przemysłem, złożonych i ambitnych misji i programów kosmicznych. ESA zapewniła również, że dokona pełnej cyfryzacji zarządzania projektami, umożliwiając rozwój możliwych do powielania kopii cyfrowych (digital twins), zarówno poprzez wykorzystanie inżynierii systemów opartych na modelach, jak i zamówień publicznych i finansów, osiągając pełną kompatybilność cyfrową z przemysłem.

Polska, podobnie jak inne państwa, traktuje rozwój rodzimego sektora kosmicznego jako zasób strategiczny i biznesowy, który zyskuje coraz większe znaczenie dla gospodarki krajowej i jest motorem coraz szerszej współpracy międzynarodowej.

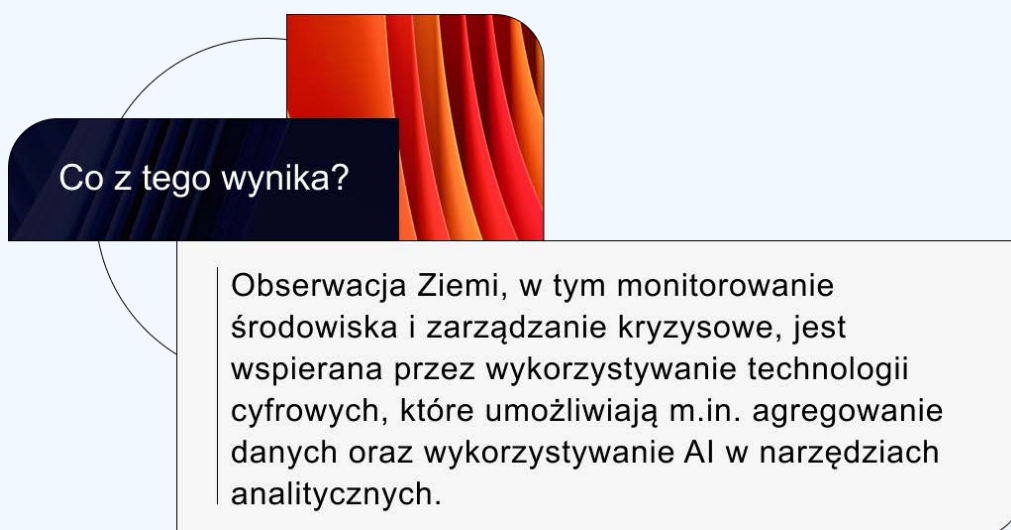
Wstąpienie Polski do ESA umożliwiło jeszcze większy postęp w rozwoju technologii kosmicznych i technik satelitarnych przez polski przemysł, a zwiększenie poziomu inwestycji z budżetu państwa, zarówno w programy opcjonalne jak i obowiązkowe, umożliwia zapewnienie administracji państwowej danych satelitarnych, wsparcie polskich podmiotów w zakresie pozyskiwania doświadczenia kosmicznego, inwestycje w dedykowaną infrastrukturę laboratoryjną i testową, rozwój zdolności w wybranych obszarach technologii kosmicznych, które mają wpływ na zwiększenie szeroko rozumianego bezpieczeństwa naszego kraju.

Ale członkostwo Polski, udział polskich firm kosmicznych w projektach ESA, to także ścisła realizacja wytycznych, wynikających z przepisów, norm, i innych dokumentów obejmujących m.in. konieczność cyfryzacji w dziedzinie inżynierii. Dzięki temu, polskie podmioty zdobywają nieocenione doświadczenie wymagane w sektorze kosmicznym. Pozwala ono inżynierom systemów i zespołom projektowym opanować złożoność systemu kosmicznego, zrozumiałe wyrażać koncepcję operacji, strukturyzować wymagania i śledzić je od projektowania i produkcji aż do testowania. Te praktyczne umiejętności wyraźnie wskazują, że Polska wpisuje się w cele cyfryzacji wskazane przez ESA, jednocześnie sprzyjając postępowi technologicznemu w kraju i przyczyniając się do zaspokajania potrzeb krajowych, jak również zwiększaniu potencjału konkurencyjności polskiego przemysłu kosmicznego na rynkach globalnych.

Cel 1: Technologie obserwacji Ziemi są udoskonalane na potrzeby monitorowania środowiska i zarządzania katastrofami

Co umożliwi realizację celu:

- a) Stworzenie scentralizowanej platformy do agregowania danych z różnych misji kosmicznych, satelitów i czujników;
- b) Wdrażanie zaawansowanych narzędzi analitycznych wykorzystujących AI do przetwarzania i interpretacji danych w celu prognozowania i wspierania decyzji w czasie rzeczywistym np. w zarządzaniu kryzysowym;
- c) Wykorzystywanie technologii cyfrowych bliźniaków satelitów w celu optymalizacji ich działania, predykcji usterek oraz zarządzania cyklem życia.



Cel 2: Infrastruktura kosmiczna jest cyberbezpieczna

Co umożliwi realizację celu:

- a) Wdrożenie kompleksowych środków cyberbezpieczeństwa w celu ochrony systemów kosmicznych i danych przed zagrożeniami, zapewniając ciągłość operacyjną;
- b) Wdrożenie systemów komunikacji kwantowej dla bezpiecznej transmisji danych;
- c) Opracowywanie i wdrażanie zaawansowanych systemów zarządzania ruchem kosmicznym - technologii śledzenia śmieci kosmicznych i kolizji satelitów oraz zarządzania nimi;
- d) Wsparcie rozwoju AI, automatyki i robotyki na potrzeby autonomicznych operacji satelitarnych, wykrywania anomalii, serwisowania, napraw i montażu na orbicie.
- e) Opracowywanie i wdrażanie narzędzi informatycznych dla sterowania systemami wynoszenia i pojazdami kosmicznymi oraz zapewnienia ich bezpieczeństwa lotu;
- f) Komputery pokładowe (ACOS) – algorytmy sterowania do manewrów rakiet, manewrów zbliżania na orbicie, optymalizacji zużycia paliwa pojazdów kosmicznych, itd.;
- g) Rozwój oprogramowania do kalkulacji manewrów pojazdów kosmicznych: liczenie trajektorii lotu rakiety, strefy upadku, modelowanie aerodynamiczne i gazodynamiczne, specjalne moduły do podwójnego zastosowania.



Co z tego wynika?

Zapewnimy ciągłość operacyjną systemów kosmicznych i zabezpieczymy je przed cyberzagrożeniami, wykorzystując najnowsze technologie cyfrowe.

4.5 Finansowanie i wsparcie innowacji

Diagnoza – jak jest?

W 2023 r. Polska zajęła dalekie, 17. miejsce w Unii Europejskiej oraz 20. w Europie pod względem kapitału zainwestowanego w startupy na różnych fazach wzrostu. Mimo zwiększenia skali finansowania nieznacznie spadł procentowy udział Polski w całkowitym kapitale zainwestowanym przez fundusze venture capital/private equity (VC/PE) w Europie w ciągu ostatnich trzech lat (2021-2023) w stosunku do trzech poprzednich lat (2018-2020). Największe wzrosty odnotowały Holandia, Norwegia, Estonia, Austria i Niemcy. W 2023 r. Warszawa zajęła wysokie 3. miejsce w wśród miast z regionu Europy Środkowo-Wschodniej pod względem nominalnej wartości zainwestowanego kapitału, ale sam region EŚW nadal pozostaje na poziomie o 70% niższym np. w stosunku do regionu DACH (Niemcy, Austria, Szwajcaria), pod względem procentowego udziału finansowania startupów w PKB. W ostatnich latach wzrosła w Polsce skala finansowania startupów na etapie pre-seed (przedzależkowym) oraz seed (zależkowym), jednak nadal występuje problem finansowania na kolejnych etapach rozwoju.

Na szczeblu krajowym w ostatnich latach podjęto szereg działań mających zwiększyć finansowanie, do których można przede wszystkim zaliczyć wzrost aktywności Polskiego Funduszu Rozwoju. Odegrał on kluczową rolę w zwiększeniu finansowania, wspierając ponad 60 funduszy w formule funduszy funduszy poprzez PFR Ventures. Działalność PFR przyciągnęła do Polski szereg zagranicznych funduszy VC.

Do zdiagnozowanych problemów z obszaru finansowania zaliczyć można brak możliwości finansowania startupów przez fundusze emerytalne, brak efektywnej współpracy banków komercyjnych z BGK, szereg barier prawnych w sektorze bankowym w zakresie finansowania startupów poprzez instrumenty dłużne czy niedostatecznie skuteczne działania akceleratorów finansowanych ze środków publicznych. Dane wskazują na stosunkowo wysoką liczbę startupów w Polsce, jednak wynika to z faktu, że polska gospodarka jest jedną z największych w UE.

Pod względem liczby wszystkich startupów, również tych bez zapewnionego finansowania, Polska zajmuje w Unii 9. miejsce oraz 11. w Europie. Jednak pod względem liczby startupów jakie uzyskały finansowanie przypadających na mieszkańca, Polska jest dopiero 23. w Unii. Podobnie jest w przypadku tzw. jednorożców (innowacyjnych firm o wycenie powyżej 1 mld USD) – nominalnie Polska zajmuje 9. miejsce, ale per capita – już 22.

W ostatnich pięciu latach udział regionu EŚW w całkowitej wartości startupów w Europie wzrósł z 4,9% w roku 2019 do 5,7% w roku 2023. Pod względem wzrostu całkowitej wartości startupów za okres ostatnich pięciu lat Polska zajęła 6. miejsce w regionie EŚW (wzrost o 240 proc., w porównaniu do 740 proc. w Chorwacji). Pod względem udziału Polski w całkowitej wartości TOP100 największych spółek technologicznych regionu EŚW Polska zajmuje 1. miejsce z udziałem 38%.

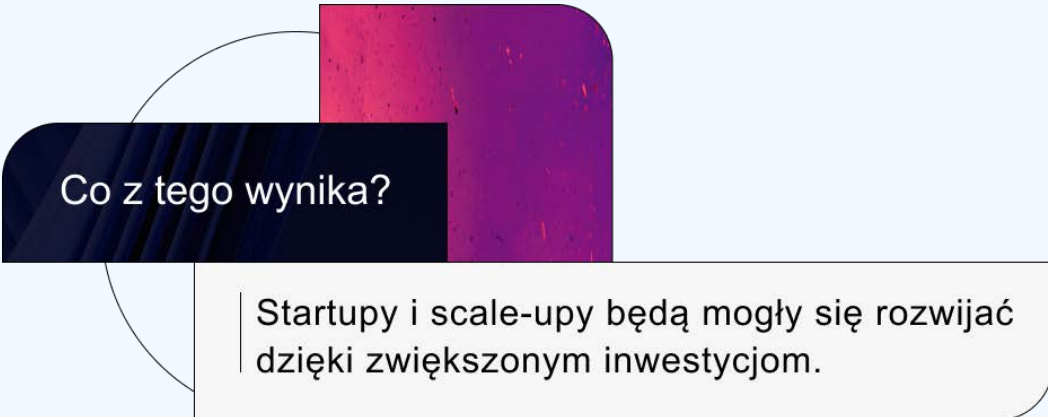
Porównując polski ekosystem startupowy z ekosystemami wiodących krajów w UE można zaobserwować szereg różnic, do których można zaliczyć: brak kompleksowego programu ułatwiającego współpracę spółek skarbu państwa (SSP) ze startupami, niedostatecznie

efektywne wsparcie dla rozwoju ekosystemu innowacji, i niedostatecznie skuteczną promocję Polski jako centrum innowacji.

Cel 1: Istnieje zintegrowany i sprawny system finansowania dla startupów i scale-upów

Co umożliwi realizację celu:

- a) Zintegrowanie środowiska finansowego (fundusze VC, BGK, GPW, banki prywatne) w celu intensyfikacji współpracy oraz wypracowania rozwiązań na rzecz mobilizacji kapitału dla startupów;
- b) Wprowadzenie zachęt fiskalnych dla krajowych i zagranicznych inwestorów instytucjonalnych i prywatnych (w tym duże przedsiębiorstwa) z tytułu inwestycji w startupy;
- c) Usprawnienie ekosystemu akceleratorów finansowanych ze środków publicznych, we współpracy z prywatnymi inwestorami i poszukiwanie możliwości koinwestycji z wiodącymi światowymi akceleratorami.



Co z tego wynika?

Startupy i scale-upy będą mogły się rozwijać dzięki zwiększonym inwestycjom.

Cel 2: Startupy i scale-upy rozwijają się bez barier inwestycyjnych

Co umożliwi realizację celu:

- a) Identyfikacja i zniesienie barier prawnych dla wzrostu startupów i ich skalowania;
- b) Umożliwienie tworzenia celowych wehikułów inwestycyjnych (SPV) do inwestycji w fundusze lub startupy;
- c) Dostosowanie procedur administracyjnych w celu zwiększenia zainteresowania prowadzeniem innowacyjnych firm i inwestowania w Polsce przez podmioty z zagranicy;
- d) Wypracowanie rozwiązań prawnych przyciągających talenty z zagranicy.



Co z tego wynika?

Ułatwimy działalność startupów i scale-upów zmieniając prawo i dostosowując procedury administracyjne do ich specyfiki.

Cel 3: Państwo zwiększa pulę talentów i liczebność podmiotów ekosystemu w Polsce

Co umożliwi realizację celu:

- a) Uznanie tzw. cyfrowych nomadów ICT pochodzących spoza UE za preferowanych z punktu widzenia polityki migracyjnej; stworzenie programu przedstawiającego im zalety stałego osiedlenia się w Polsce;
- b) Rozwinięcie wsparcia w administracji publicznej dla pewnej puli zagranicznych talentów ICT przed przybyciem do Polski we współpracy z agencjami pracy i wspierającymi relokację. Jego zakres obejmować będzie procedury administracyjne i wsparcie logistyczne.

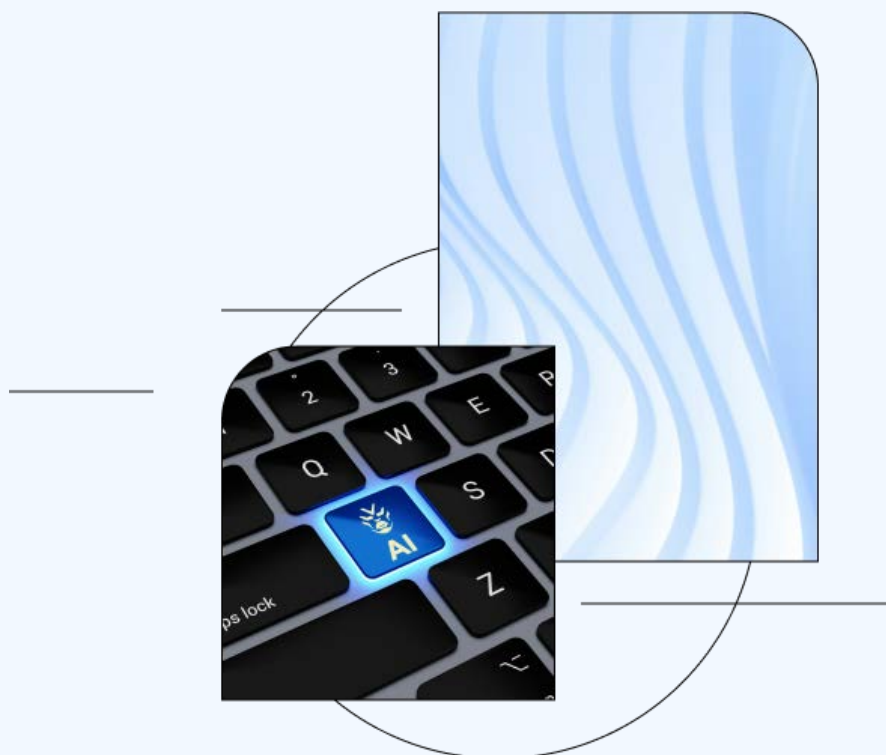


4.6 Open source

Diagnoza – jak jest?

Polska jest państwem o silnym sektorze IT, który jednak w niewielkim stopniu wykorzystuje potencjał otwartego oprogramowania. Jako jedno z nielicznych państw UE, nie posiada strategii rozwoju i wspierania otwartego oprogramowania⁵¹. Jest ono w niewielkim stopniu wykorzystywane w administracji publicznej, mimo że otwarte oprogramowanie jest komplementarne do rozwoju ekosystemu otwartych danych, które są w Polsce na wysokim poziomie.

Równocześnie, tworzenie i wykorzystywanie otwartego oprogramowania jest ważnym narzędziem pozwalającym zapewnić suwerenność cyfrową. Pozwala zmniejszać zależność od określonego, komercyjnego oprogramowania; zwiększa przejrzystość i kontrolę nad wykorzystywanymi technologiami, jest też bardziej efektywne kosztowo. Otwarte oprogramowanie pozwala też budować powiązania między sektorem IT oraz różnorodnymi środowiskami rozwijającymi i korzystającymi z technologii. W ostatnich latach przykładem takiego podejścia jest rozwój polskich, otwartych modeli językowych.

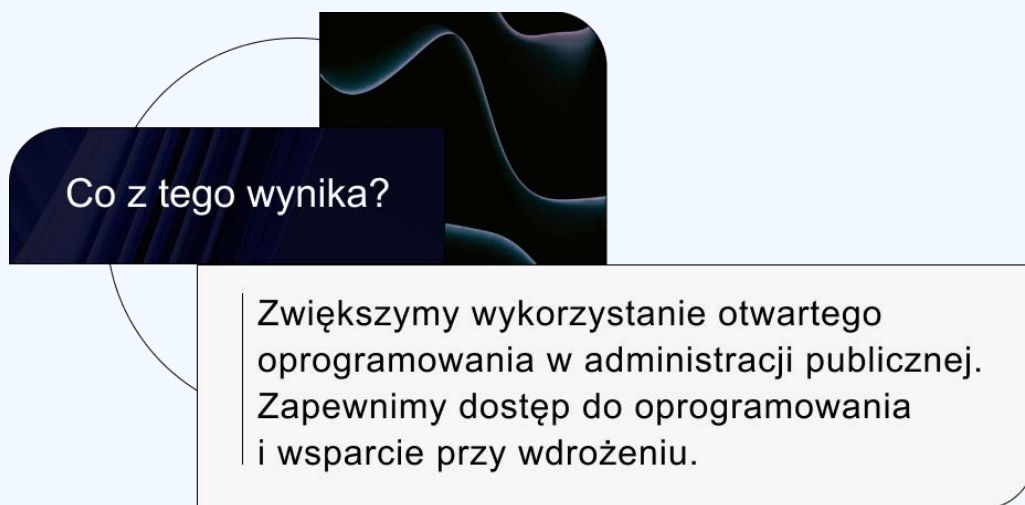


⁵¹ Blind, K.; Böhm, M., Grzegorzewska, P., Katz, A., Muto, S., Pätsch, S., Schubert, T. (2021). The impact of Open Source Software and Hardware on technological independence, competitiveness and innovation in the EU economy, Final Study Report. Brussels, s. 226.

Cel 1: Polska administracja publiczna w większym stopniu wykorzystuje otwarte oprogramowanie.

Co umożliwi realizację celu:

- a) Wskazanie podmiotu odpowiedzialnego za koordynację rozwoju i wdrażania otwartego oprogramowania w polskiej administracji publicznej, a także rozwoju kompetencji w tym zakresie;
- b) Opracowanie programu wdrażania otwartego oprogramowania w polskiej administracji, obejmującego standardy wykorzystania oprogramowania oraz projekty pilotażowe;
- c) Określanie zasad prowadzenia przetargów na wdrożenia IT w administracji publicznej, które będą wspierać wykorzystanie otwartego oprogramowania;
- d) Utworzenie repozytorium otwartego oprogramowania dla polskiej administracji.



Cel 2. Poziom tworzenia i wykorzystania otwartego oprogramowania przez polskie firmy i polskich programistów jest wyższy.

Co umożliwi realizację celu:

- a) Wprowadzenie instrumentu finansowania dla firm i programistów na tworzenie otwartego oprogramowania;
- b) Wsparcie rozwoju otwartych systemów sztucznej inteligencji oraz ich wdrażania w administracji publicznej;
- c) Wsparcie rozwoju otwartych rozwiązań dla administracji samorządowej - połączone wsparcie dla lokalnych firm i gmin wdrażających oprogramowanie.



Co z tego wynika?

Firmy i programiści tworzący otwarte oprogramowanie otrzymają zwiększone finansowanie. Proces wdrażania otwartego oprogramowania będzie rozwijany i wspierany.

4.7 Cyfrowa i zielona transformacja

Diagnoza – jak jest?

Obecnie w Polsce realizowanie inicjatyw na rzecz zielonej i cyfrowej transformacji wynika głównie z unijnych wymogów regulacyjnych i wytycznych w zakresie finansowania projektów z funduszy europejskich, nie zaś z obranej przez państwo ambitnej strategii w zakresie tzw. „bliźniaczej przemiany”. Zaproponowane w Krajowym planie do programu polityki „Droga ku cyfrowej dekadzie” działania w tym obszarze skupiają się przede wszystkim na tworzeniu sandboxów dla rozwiązań AI, uczestnictwie w inicjatywie Komisji Europejskiej Earth Destination, inwestycjach i wymogach związanych z wdrażaniem innowacji środowiskowych (przede wszystkim gospodarki obiegu zamkniętego). Dotychczas niewiele uwagi poświęcono także wpływowi państwowych rozwiązań cyfrowych na środowisko i zmiany klimatu. Równocześnie wiadome jest, że ślad węglowy generowany wskutek produkcji i użytkowania rozwiązań cyfrowych stale rośnie w Polsce i na świecie. Szacuje się, że globalne emisje sektora ICT wynoszą od 4% do 10%⁵² i są większe niż te generowane przez przemysł lotniczy.

Niezbędne jest więc bardziej kompleksowe niż dotychczas podejście do cyfrowej i zielonej transformacji

oraz współpraca międzyresortowa, która obejmie wątki zarówno energochłonności narzędzi cyfrowych, potencjału technologii w walce ze zmianami klimatu i ograniczeniem emisji, jak również ekologii cyfrowej.

Wśród polskiego biznesu rośnie świadomość wpływu nowych technologii na środowisko i klimat. Zgodnie z ostatnimi danymi⁵³, ponad 64% firm z sektora ICT zwraca uwagę na kwestie takie jak zużycie energii czy możliwość łatwej wymiany części przy wyborze sprzętu lub dostawcy usług. Równocześnie brakuje systemów monitorowania wpływu technologii cyfrowych wykorzystywanych przez firmy na środowisko. Obowiązek raportowania kwestii związanych z ryzykiem klimatycznym, wynikający z dyrektywy ws. sprawozdawczości przedsiębiorstw w zakresie zrównoważonego rozwoju (tzw. CSRD – The Corporate Sustainability Reporting Directive), na ten moment dotyczy jedynie największych spółek giełdowych. To natomiast może prowadzić do ograniczonego raportowania bądź też greenwashingu (fałszywego przedstawiania produktów lub usług jako ekologicznych) w przypadku podmiotów mniejszych oraz tych nienotowanych na giełdzie. W zakresie certyfikacji, istnieją unijne systemy weryfikacji technologii, jak chociażby ETV⁵⁴ (Environmental Technology Verification – Program weryfikacji technologii środowiskowych

52 <https://www.sciencedirect.com/science/article/pii/S2666389921001884>

53 https://ec.europa.eu/eurostat/statistics-explained/index.php?title=ICT_in_enterprises_and_the_environment.

54 <https://lifeproetv.eu/pl/strona-glowna/>

Unii Europejskiej). Jednak odnoszą się one przede wszystkim do technologii środowiskowych (tj. mających na celu redukcję emisji gazów cieplarnianych, ograniczenie zużycia zasobów takich jak woda czy surowce), nie zaś do produktów sektora ICT, które w coraz większym stopniu odpowiadają za zużycie energii. Ponadto są one dobrowolne, co może stawać pod znakiem zapytania ich skuteczność.

Pierwsze polskie badania⁵⁵ sugerują, że świadomość obywateli na temat ekologii cyfrowej jest niska.

Terminy takie jak “cyfrowy ślad węglowy” i “ekologia cyfrowa” są jasne jedynie dla odpowiednio 19% i 12% osób niezwiązanych z sektorem ICT. Odsetek ten był wyższy wśród osób związanych z branżą IT, jednak wciąż wynosił tylko 25%. Hasło “ekologia cyfrowa” okazało się jeszcze mniej popularne, ponieważ znało je 23% specjalistów IT i 12% pozostałych respondentów.



⁵⁵ <https://blog.theprotocol.it/artikol/cyfrowa-ekologia-w-pracy-i-zyciu-polakow-raport-theprotocol>

Cel 1: Dane z obszaru energetyki, środowiska i klimatu są dostępne i ponownie wykorzystywane zarówno przez organy administracji publicznej, jak i zewnętrzne podmioty w celu prowadzenia analiz i badań na rzecz optymalizacji sektora energetycznego

Co umożliwi realizację celu:

- a) Reforma modelu prowadzenia badań statystycznych w obszarach takich jak: stan i ochrona środowiska, rynek materiałowy i paliwowo-energetyczny, leśnictwo i łowiectwo. Dostęp do wyników badań statystycznych prowadzonych na zlecenie ministra właściwego powinien być, w myśl zasady 3R⁵⁶, równoprawny, równorzędny i równoczesny, a do tego nieodpłatny. Aby to osiągnąć, konieczna jest likwidacja barier w zakresie dostępności danych takich jak systemy płatności za dostęp do treści publikowanych przez podmioty realizujące badania z obszaru statystyki oraz egzekwowanie wysokich standardów otwartości danych (eliminację formatów plików blokujących maszynowy odczyt danych). Kluczowe jest także zapewnienie zgodności raportowanych danych i spójności metodologii wykorzystywanej przez instytucje współodpowiedzialne za prowadzenie badań statystycznych;
- b) Zmobilizowanie państwowego sektora energetycznego i wydobywczego do dobrowolnej publikacji danych o istotnej społecznej wartości, np. informacji o zanieczyszczeniu i wykorzystaniu środowiska, zatrudnieniu i oddziaływaniu lokalnym. Opracowanie i wdrożenie planu udostępniania danych i modelu zarządzania (data governance) zgodnego z założeniami unijnego aktu w sprawie zarządzania danymi (DGA) oraz skupionego na regularnym zwiększaniu zestawu udostępnianych danych w oparciu o zapotrzebowanie administracji rządowej i samorządowej, społeczeństwa obywatelskiego, sektora prywatnego i środowiska eksperckiego.

56

https://bip.stat.gov.pl/files/gfx/bip/pl/defaultstronaopisowa/566/1/1/zasady_postepowania_z_danymi_statystycznymi_streszczenie.docx



Co z tego wynika?

Organy administracji publicznej i zewnętrzne podmioty mogą przeprowadzać badania sektora energetycznego, przy wykorzystaniu danych. Wyniki badań będą publikowane, w sposób nieodpłatny i umożliwiający maszynowy odczyt danych.



Cel 2: Systemy energetyczne, w tym ciepłownicze, opierają się na innowacyjnych systemach zarządzania i optymalizacji

Co umożliwi realizację celu:

- a) Wzmacnianie cyberbezpieczeństwa oraz zapewnienie infrastruktury cyfrowej wspierającej innowacje, takie jak chociażby zaawansowane magazynowanie energii, sztuczna inteligencja w energetyce i urządzenia grid-edge, które pozwolą na integrację energii z OZE z istniejącymi mocami wytwórczymi, sieciami dystrybucji i przesyłu energii oraz zapewnią ciągłość dostaw i sprawne funkcjonowanie systemu energetycznego;
- b) Współpracę międzyresortową w zakresie aktualizacji i wdrażania dokumentów strategicznych w zakresie transformacji sektora energetycznego (takich, jak chociażby Krajowy Plan na rzecz Energii i Klimatu [KPEiK] na lata 2021-2030) w celu wszechstronnego uwzględnienia kwestii digitalizacji systemu energetycznego;
- c) Dalszy rozwój inteligentnych sieci (smart grids) zgodny z unijnymi zasadami interoperacyjności, wytycznymi Grupy Roboczej "Clean Energy Package"⁵⁷ oraz założeniami projektu KPEiK. Dzięki coraz bardziej powszechnemu zastosowaniu inteligentnych liczników, rozbudowa smart grids i digitalizacja systemu energetycznego (zwiększania jego opomiarowania, sprawności, inteligentnego sterowania) jest możliwa. W przyszłości kluczowe będzie także wdrażanie coraz to bardziej zaawansowanych narzędzi AI, które pozwolą na przetwarzanie na bieżąco wiedzy o kształcie lokalnego i krajowego rynku energetycznego - analizowanie coraz większych ilości danych rosnącego grona prosumentów, zjawisk atmosferycznych w celu prognozowania zużycia energii, danych z czujników i urządzeń IoT mówiących o nawykach odbiorców energii;
- d) Wspieranie, równolegle z cyfryzacją systemu elektroenergetycznego, rozwoju podobnych rozwiązań w ciepłownictwie. Rozwiązania pozwolą na zmapowanie całej sieci ciepłowniczej czy stworzenie pełnego cyfrowego modelu sieci, zintegrowanego z innymi systemami działającymi w przedsiębiorstwie ciepłowniczym;
- e) Wspieranie innowacji w sektorze energetycznym poprzez inwestycje w prace badawczo-rozwojowe (R&D) oraz szkolenia specjalistów ICT skupione na tworzeniu rozwiązań cyfrowych dla sektora energetycznego.

⁵⁷ [https://www.cencenelec.eu/media/CEN-CENELEC/AreasOfWork/CEN-CENELEC_Topics/Smart Grids and Meters/Smart Grids/finalreportwg-cep_2019.pdf](https://www.cencenelec.eu/media/CEN-CENELEC/AreasOfWork/CEN-CENELEC_Topics/Smart%20Grids%20and%20Meters/Smart%20Grids/finalreportwg-cep_2019.pdf)



Co z tego wynika?

Usprawnimy funkcjonowanie sektora energetycznego, zwiększając zastosowanie rozwiązań cyfrowych, inwestując w prace badawczo-rozwojowe i zapewniając rozwój specjalistów ICT.



Cel 3: Wpływ technologii ICT wykorzystywanych przez administrację publiczną na środowisko jest weryfikowany i ograniczany

Co umożliwi realizację celu:

- a) Mierzenie cyfrowego śladu węglowego administracji publicznej generowanego na skutek korzystania z urządzeń elektronicznych i internetu w sektorze publicznym, a także zużycia energii niezbędnej do utrzymania państwowej infrastruktury (centrów danych, serwerów);
- b) Mapowanie i monitorowanie łańcucha dostaw systemów i usług ICT wykorzystywanych w administracji publicznej. Opracowanie norm zużycia energii dla systemów i usług ICT, które są brane pod uwagę przy realizacji zamówień publicznych oraz premiowanie dostawców systemów i usług ICT, którzy zobowiązali się do osiągnięcia neutralności klimatycznej do 2050 r. (zgodnie z Porozumieniem paryskim) bądź wcześniej, przedstawiając rzetelny plan działania i wykazując udokumentowane postępy w realizacji celów;
- c) Zaprojektowanie zasad zrównoważonego rozwoju ICT i ekologii cyfrowej w organach administracji publicznej oraz uwzględnianie ich przy projektowaniu krajowych polityk publicznych i strategii.



Cel 4: Przyjazny środowisku sektor ICT

Co umożliwi realizację celu:

- a) Promowanie rozwoju i wykorzystania energooszczędnych rozwiązań wśród operatorów telekomunikacyjnych. Dążenie do zapewnienia większej efektywności energetycznej w projektowaniu, budowie i eksploatacji sieci, w tym dbanie o wymianę urządzeń sieciowych na bardziej energooszczędne, włączanie funkcji oszczędzania energii w nieużywanych komponentach, optymalizację z wykorzystaniem sztucznej inteligencji;
- b) Przygotowanie we współpracy z sektorem ICT, przedsiębiorstwami przemysłu technologicznego, instytucjami szkolnictwa wyższego, instytucjami badawczymi, wytycznych i najlepszych praktyk dot. zrównoważonego rozwoju w projektowaniu produktów i usług cyfrowych;
- c) Zachęcanie operatorów centrów przetwarzania danych do uwzględnienia dobrych praktyk, o których mowa w europejskim kodeksie postępowania w sprawie efektywności energetycznej centrów danych⁵⁸;
- d) Zachęcanie do tworzenia narzędzi przyjaznych środowisku narzędzi cyfrowych generującego rozwiązania poprzez konkursy tematyczne i „hackathony”.



⁵⁸https://joint-research-centre.ec.europa.eu/scientific-activities-z/energy-efficiency/energy-efficiency-products/code-conduct-ict/european-code-conduct-energy-efficiency-data-centres_en

Cel 5: Obywatele są świadomi wpływu technologii ICT na środowisko i dysponują podstawową wiedzą w zakresie ekologii cyfrowej

Co umożliwi realizację celu:

- a) Uwzględnianie w programach kształcenia kwestii wpływu korzystania z usług ICT na środowisko oraz edukowanie na temat tego, jak korzystać z technologii w sposób bardziej zrównoważony. Prowadzenie kampanii społeczno-edukacyjnych podnoszących świadomość w ww. obszarach;
- b) Podnoszenie świadomości znaczenia przekazywania urządzeń do recyklingu, zwiększanie dostępności punktów odbioru elektrośmieci;
- c) Propagowanie norm i oznakowań dotyczących zrównoważonego rozwoju w odniesieniu do produktów i usług cyfrowych.

Co z tego wynika?

Umożliwimy Ci zwiększenie wiedzy o wpływie technologii ICT na środowisko oraz pokażemy, jak korzystać z niej zgodnie z zasadami ekologii cyfrowej.

System wdrażania



Ministerstwo
Cyfryzacji

Tu tworzymy przyszłość

System wdrażania

Koordinacja

Organem odpowiedzialnym za koordynację działań mających na celu realizację Strategii będzie minister właściwy ds. informatyzacji.

Cyfryzacja jest procesem przekrojowym i wielowymiarowym, co znajduje odzwierciedlenie w bardzo szerokim zakresie przedmiotowym Strategii. Realizacja głównego jej celu, jakim jest podnoszenie jakości życia przez cyfryzację, wymaga zaangażowania i ścisłej współpracy wielu jednostek sektora publicznego. Niemniej, interwencja nie ogranicza się jedynie do sfery funkcjonowania państwa, ale zakłada również inspirowanie działań na rzecz transformacji cyfrowej przy zaangażowaniu sektora prywatnego.

Szczególną rolę w procesie wdrażania Strategii odegrają pełnomocnicy ds. informatyzacji, powoływani obligatoryjnie w urzędach obsługujących ministrów kierujących działami administracji rządowej oraz w Kancelarii Prezesa Rady Ministrów (fakultatywnie natomiast w pozostałych urzędach). Działania pełnomocników skoncentrowane będą na sprawach należących do właściwości działu administracji rządowej, kierowanego przez właściwego ministra, w tym na sprawach należących do właściwości jednostek organizacyjnych lub organów podległych temu ministrowi i przez niego nadzorowanych. Głównym ich zadaniem będzie koordynowanie realizacji strategii, w tym przygotowywanie aktualnych informacji na temat postępów w jej realizacji oraz ryzyk z tym związanych, a także diagnozowanie obszarów koniecznych zmian dla dalszego wdrażania Strategii oraz wprowadzania nowych technologii cyfrowych.

Realizacja Strategii wymaga spójnych, zharmonizowanych i konsekwentnych działań, niejednokrotnie jednak przecinających tradycyjny podział obszarów działalności państwa oraz wertykalnych względem działów administracji rządowej. Służyć ma temu bieżące współdziałanie powołanych pełnomocników ds. informatyzacji, a w wymiarze instytucjonalnym możliwe będzie dzięki roli Komitetu do spraw Cyfryzacji.

Zadaniem Komitetu do spraw Cyfryzacji będzie zapewnienie koordynacji działań państwa związanych z informatyzacją oraz wsparcie rozwoju cyfrowego państwa, co ma kluczowe znaczenie dla wdrażania Strategii. Działalność Komitetu ds. Cyfryzacji polegająca na opiniowaniu i monitorowaniu przedsięwzięć informatycznych o publicznym zastosowaniu wpłynie na wzmocnienie ich koordynacji poprzez zapewnienie ich spójności z działaniami strategicznymi państwa, w tym zgodności ze Strategią oraz z założeniami AIP. Natomiast uzależnienie możliwości finansowania ze środków publicznych przedsięwzięć informatycznych o publicznym zastosowaniu od pozytywnej oceny Komitetu do spraw Cyfryzacji wpłynie pozytywnie na zwiększenie interoperacyjności i komplementarności rozwiązań informatycznych funkcjonujących w państwie, a także na zwiększenie efektywności gospodarowania środkami publicznymi.

Realizacja głównego celu Strategii wymaga, aby to zaangażowanie wielu jednostek sektora publicznego, o którym mowa powyżej, odbywało się wielokierunkowo i na wielu

plaszczynach. Działania, służące realizacji celu, będą realizowane bowiem w formie programów, projektów, aktów prawnych i przepisów technicznych.

Przegląd

Z uwagi na potrzebę dobrego planowania, spójności i ciągłości procesów cyfryzacji państwa, Strategia obejmuje wieloletnią perspektywę. Jednak tempo rozwoju technologicznego i trudność w przewidzeniu jego długofalowych kierunków sprawia, że niezbędny jest jej regularny przegląd i ewentualna aktualizacja. Minister właściwy do spraw informatyzacji we współpracy z członkami Rady Ministrów, będzie dokonywał przeglądu Strategii co 2 lata, a sprawozdanie z przeglądu będzie przedkładane Radzie Ministrów w terminie 2 miesięcy od jego zakończenia. Do opracowywania informacji z realizacji strategii w celu dokonania przeglądu zobowiązani będą pełnomocnicy ds. informatyzacji.

Monitorowanie

Minister właściwy do spraw informatyzacji monitoruje realizację Strategii raz w roku. System monitorowania obejmuje badanie postępu zaplanowanych działań w ramach celów horyzontalnych i kierunkowych oraz badanie ilościowe dotyczące stopnia realizacji przyjętych wskaźników efektywności ujętych w tabeli nr 1. Wyniki z przeprowadzonego monitoringu realizacji Strategii będą przedstawiane Komitetowi do spraw Cyfryzacji w formie sprawozdania oraz publikowane na stronie internetowej Ministerstwa Cyfryzacji, w terminie 3 miesięcy od zakończenia roku kalendarzowego.

Sprawozdanie będzie sporządzane przez ministra właściwego do spraw informatyzacji w szczególności na podstawie:

- a) przekazanych przez pełnomocników ds. informatyzacji informacji na temat każdego z zaplanowanych w Strategii działań i danych statystycznych w odniesieniu do przyjętych wskaźników, zgodnie z właściwością poszczególnych członków Rady Ministrów
- b) analizy źródeł danych dla kluczowych wskaźników efektywności określonych w tabeli nr 1.

W sprawozdaniu będą zawarte: opisy podjętych działań zaplanowanych w Strategii wraz z oceną stopnia ich zaawansowania, ewentualne zdiagnozowane problemy z ich wdrażaniem oraz rekomendacje dla poszczególnych członków Komitetu do spraw Cyfryzacji na kolejny okres.

Integralnym elementem monitoringu Strategii będzie zestaw wskaźników efektywności, odnoszących się do celów wyznaczonych w poszczególnych obszarach, ze wskazaniem wartości bazowej oraz docelowej. Źródłem danych dla pomiaru wskaźników będzie przede wszystkim krajowa statystyka publiczna, ale również System Inwentaryzacji Systemów Teleinformatycznych (SIST), raporty z działalności Komitetu do spraw Cyfryzacji, dane własne podmiotów odpowiedzialnych za realizację poszczególnych działań oraz dostępne, cykliczne raporty i badania rynku.

Poniższa tabela prezentuje wskaźniki określone dla Strategii.

Tabela 1 – wskaźniki efektywności

Lp.	Obszar	Nazwa wskaźnika	Wartość bazowa	Wartość docelowa	Rok, do kiedy wskaźnik ma zostać osiągnięty	Źródło danych
1	Koordynacja cyfrowej transformacji kraju	Udział urzędów obsługujących ministrów kierujących działami administracji rządowej, w których powołany został pełnomocnik ds. informatyzacji w ogólnej liczbie urzędów obsługujących ministrów kierujących działami administracji publicznej i KPRM	0%	100%	2026	Dane własne MC/KdsC
2		Udział przedsięwzięć informatycznych o publicznym zastosowaniu, których założenia są zgodne z pryncypiami, standardami, wytycznymi i rekomendacjami architektonicznymi AIP w ogólnej liczbie przedsięwzięć informatycznych o publicznym zastosowaniu, których założenia są opiniowane przez Komitet do spraw Cyfryzacji.	0%	100%	2035	MonaLiza/KdsC
3	Komunikacja elektroniczna	Powszechny dostęp do mobilnych usług telekomunikacyjnych o przepustowości co najmniej 100 Mb/s	57%	100% powierzchni kraju	2035	UKE

4	Kompetencje cyfrowe	Odsetek osób, które posiadają co najmniej podstawowe umiejętności cyfrowe	44,3% (dane za 2023 r.)	85% osób w wieku 16-74 lata	2035	GUS
5		Odsetek osób, które posiadają ponadpodstawowe kompetencje cyfrowe	20,1% (dane za 2023 r.)	50% osób w wieku 16-74 lata	2035	GUS
6		Udział specjalistów ICT wśród pracujących	4,3%	10% pracujących	2035	GUS
7		Udział kobiet wśród specjalistów ICT	19,1%	35%	2035	GUS
8	Cyberbezpieczeństwo	Powołanie centralnej instytucji odpowiedzialnej za cyberbezpieczeństwo na poziomie krajowym	0	1	2025/2026	Dane własne MC
9		Stworzenie chmury niejawnej – osiągnięcie pełnej zdolności operacyjnej	0	1	2029	Dane własne MC
10		Wdrożenie mechanizmu umożliwiającego wykluczanie dostawców wysokiego ryzyka.	0	1	2026	Dane własne MC
11		Odsetek terminowo zgłoszonych incydentów do zespołów CSIRT przez zobowiązane ustawowe podmioty Krajowego Systemu Cyberbezpieczeństwa	Wartość bazowa do określenia na późniejszym etapie.	100%	2035	Zespoły CSIRT
12	E-usługi publiczne	Wszystkie kluczowe e-usługi są dostępne przez aplikację mObywatel	Wartość bazowa do określenia na późniejszym etapie.	100%	2035	Dane własne COI
13		Odsetek spraw w realizowanych elektronicznie przez podmioty realizujące działania publiczne w stosunku do wszystkich spraw	Wartość bazowa do określenia na późniejszym etapie.	100%	2035	
14		Integracja z usługą ePłatności minimum jednej instytucji/urzędu w obszarach JST w Polsce	2%	100%	2035	Dane własne COI

15	Cyfryzacja procesów administracyjnych i postępowań sądowych	Udział liczby podmiotów realizujących zadania publiczne korzystających z systemu klasy EZD w stosunku do liczby podmiotów publicznych ogółem	86% (dane za 2022 r.)	100%	2035	Raport GUS
16		Odsetek urzędów administracji publicznej wykorzystujących technologie sztucznej inteligencji	Wartość bazowa do określenia na późniejszym etapie.	80%	2035	
17	Systemy i rejestry	Udział liczby publicznych systemów teleinformatycznych, dla których w repozytorium interoperacyjności udostępniono opisy API, w stosunku do liczby publicznych systemów teleinformatycznych monitorowanych w SIST.	0%	100%	2035	SIST
18		Umocowanie prawne referencyjnych rejestrów publicznych	0	1	2027	Dane własne MC
19	Cyfrowa tożsamość	Liczba wydanych środków identyfikacji elektronicznej dla osób prawnych i osób fizycznych reprezentujących osoby prawne (czy na dany podmiot uprawniony przypada osoba reprezentująca posiadająca taki środek)	0%	50% podmiotów uprawnionych	2035	Dane własne COI
20		Liczba aktywowanych europejskich portfeli tożsamości cyfrowej	0	20 mln użytkowników	2035	Dane własne COI
21	Chmura obliczeniowa	Minimum 70% systemów wykorzystywanych do realizacji cyfrowych usług publicznych korzysta ze współdzielonej infrastruktury	0	70%	2035	Dane własne COI

		obliczeniowej (chmury obliczeniowej).				
22	Otwarte dane i wymiana danych	Liczba udostępnionych danych w portalu dane.gov.pl	41500 (wartość na koniec 2024 r.)	100 000	2035	dane.gov.pl
23	Bezpieczna przestrzeń cyfrowa	Stworzenie i wprowadzenie systemu oceny wymiaru etycznego narzędzi SI stosowanych przez państwo	0	1	2025	Dane własne MC
24		Ustalenie organu odpowiedzialnego za nadzorowanie i integrowanie działań różnych podmiotów zajmujących się przeciwdziałaniem dezinformacji.	0	1	2026	Dane własne MC
25	Cyfrowe zdrowie	Odsetek PWDL prowadzących EDM, podłączonych do systemu P1 i wymieniających się dokumentacją w sposób elektroniczny	18%	100%	2035	Centrum e-Zdrowia
26		Liczba badań naukowych i projektów badawczych, które zostały zrealizowane na podstawie dostępnych danych rzeczywistych przez pierwsze 3 lata funkcjonowania rozwiniętego systemu udostępniania danych	0	3500	2035	Centrum e-Zdrowia
27		Wprowadzenie narzędzi predykcyjnych i screeningowych w systemie centralnym	0	Narzędzia wdrożone dla co najmniej 100 jednostek chorobowych	2035	Centrum e-Zdrowia

28	Branże kreatywne	Wzrost wartości polskiego rynku gier wideo	1286 mln USD (2022)	3669 mln USD ⁵⁹ (10% wzrostu rocznie)	2035	PARP	
29	Cyfrowa akademia	Liczba absolwentów kierunków kształcących w obszarze ICT (dyscypliny wg klasyfikacji ISCED 0610, 0611, 0612, 0613, 0618, 0619, 0688) ⁶⁰	15279 (koniec 2023)	20 000	2035	MNiSW System POL_on	
30		Ilość mocy obliczeniowej dla obliczeń HPC dostępnej w PLGrid	70 petaflopsów	1 eksaflops	2035	Raport PLGrid	
31		Ilość mocy obliczeniowej dla obliczeń AI dostępnej w PLGrid:	3 eksaflopsy	40 eksaflopsów	2035	Raport PLGrid	
32	Cyfrowa transformacja przedsiębiorstw	Udział przedsiębiorstw sektora MŚP wykorzystujących na co najmniej podstawowym poziomie technologie cyfrowe	50% (2023)	92%	2035	GUS	
33		Odsetek przedsiębiorstw sektora MŚP wykorzystujących technologie sztucznej inteligencji	3,7% (2023)	50%	2035	GUS	
34	Sztuczna inteligencja	Stworzenie mechanizmu koordynacji wdrożenia i finansowania projektów AI w administracji publicznej		0	1	2026	Dane własne MC

⁵⁹ W cenach z 2022 r.

⁶⁰ ISCED - Międzynarodowa Standardowa Klasyfikacja Edukacji to system służący do gromadzenia, zestawiania i analizowania statystyk dotyczących edukacji, porównywalnych na szczeblu międzynarodowym. Dyscypliny brane pod uwagę przy badaniu wskaźnika: 0610 Technologie teleinformacyjne nieokreślone dalej, 0611 Obsługa i użytkowanie komputerów, 0612 Projektowanie i administrowanie baz danych i sieci, 0613 Tworzenie i analiza oprogramowania i aplikacji, 0618 Interdyscyplinarne programy i kwalifikacje związane z technologiami informacyjno-komunikacyjnymi, 0619 Technologie teleinformacyjne gdzie indziej niesklasyfikowane, 0688 Interdyscyplinarne programy i kwalifikacje obejmujące technologie informacyjno-komunikacyjne.

35	Inne technologie przełomowe	Stworzenie programu wieloletniego wspierania rozwoju technologii przełomowych	0	1	2026	Dane własne MC
36	Open source	Utworzenie Biura Programów Otwartego Oprogramowania	0	1	2035	Dane własne MC
37	Cyfrowa i zielona transformacja	Odsetek gospodarstw domowych wyposażonych w inteligentne liczniki	33%	100%	2031	Monitoring realizacji PEP 2040

Finansowanie

Działania zebrane i zaproponowane w strategii mają charakter przekrojowy i wpływają na wiele obszarów, takich jak bezpieczeństwo państwa, utrzymanie konkurencyjności gospodarki, edukację czy postęp naukowy i technologiczny. Zaplanowane działania będą realizowane przez różne podmioty, z udziałem nakładów finansowych pochodzących, w szczególności z następujących źródeł:

- budżet państwa – cele strategii będą realizowane poprzez interwencje publiczne finansowane z części budżetu państwa poszczególnych ministrów. Ponadto, z budżetu państwa będą pochodziły środki na współfinansowanie dla projektów realizowanych ze źródeł zagranicznych;
- budżety jednostek samorządu terytorialnego;
- środki innych podmiotów realizujących zadania publiczne;
- fundusze celowe m.in.: Fundusz Szerokopasmowy, Fundusz Cyberbezpieczeństwa, CEPIK;
- Instrument na rzecz Odbudowy i Zwiększania Odporności (RRF): Krajowy Plan Odbudowy i Zwiększania Odporności;
- fundusze europejskie przeznaczone na realizację Polityki spójności (w tym Program Fundusze Europejskie na Rozwój Cyfrowy 2021-2027, Program Fundusze Europejskie dla Rozwoju Społecznego 2021-2027, Fundusze Europejskie dla Nowoczesnej Gospodarki) oraz Wspólnej polityki rolnej w perspektywie 2021–2027 oraz 2028-2034;
- inne instrumenty i programy europejskie m.in.: Instrument „Łącząc Europę” (Connecting Europe Facility), Program „Cyfrowa Europa”, Program „Horyzont Europa”, Program „Obywatele, Równość, Prawa i Wartości” (Citizens, Equality, Rights And Values Programme, CERV);
- inne środki publiczne, w tym środki ze źródeł zagranicznych (np. z Norweski Mechanizm Finansowy), inne instrumenty funkcjonujące w oparciu o środki publiczne, jak np. instrumenty BGK w ramach oferty Grupy Polskiego Funduszu Rozwoju;
- instrumenty finansowe międzynarodowych instytucji finansowych (z kredytów, gwarancji, obejmowania udziałów, fundusze Venture Capital);
- środki prywatne – realizacja celów Strategii będzie wymagała również zaangażowania środków prywatnych, w szczególności w zakresie zapewnienia współfinansowania projektom współfinansowanym ze środków UE;
- Narodowy Fundusz Zdrowia (NFZ), a także współpłacenie pacjentów za świadczenia zdrowotne (np. w refundacji aptecznej) oraz współpłacenie przez dostawców technologii (np. instrumenty dzielenia ryzyka, podmioty zainteresowane dostępem do danych);

Koszty realizacji zadań i utrzymania efektów strategii zostaną sfinansowane w ramach corocznie ustalanego limitu wydatków dla poszczególnych części budżetowych. Ostateczna wysokość środków przewidzianych do realizacji poszczególnych projektów będzie planowana corocznie przez Radę Ministrów w trakcie prac nad ustawą budżetową.

Wsparciem dla wydatków krajowych będą środki europejskie w perspektywie finansowej 2021-2027 oraz 2028-2035. Przewiduje się, że w perspektywie finansowej 2028-2035 znaczenie środków UE będzie nadal istotne, choć stanie się relatywnie mniejsze. Interwencje publiczne będą w większym stopniu finansowane w oparciu o krajowe środki publiczne. Istotne będzie skoncentrowanie środków UE na projektach o najwyższej wartości dodanej i pozytywnych efektach zewnętrznych. Jednocześnie, biorąc pod uwagę potrzebę przeznaczenia znacznych środków na cyfryzację, konieczna może być zmiana struktury finansowania rozwoju branży, która w dużej mierze opiera się o kontrybucje sektora telekomunikacyjnego, a pomija innych graczy, korzystających ze wspólnej infrastruktury.

Słownik

- Architektura Informacyjna Państwa (AIP) – metoda zarządzania informatyzacją państwa, oparta na modelach architektonicznych i obejmująca zasady podstawowe (pryncypia), standardy, wytyczne i rekomendacje architektoniczne;
- Blockchain - złożona kombinacja technologii kryptograficznych i technologii systemów rozproszonych, pozwalająca potwierdzać prawdziwość danych w różnych procesach transakcyjnych. Pozwala stronom, które się nie znają, zaufać procesom, procedurom lub pomiarom, bez potrzeby angażowania pośredników, którzy mieliby takie zaufanie gwarantować. Niekiedy kojarzona również z pojęciem WEB 3.0.;
- Centra Wymiany i Analizy Informacji (ang. Information Sharing and Analysis Center, ISAC) - centra wymiany wiedzy i doświadczeń dotyczących incydentów cyberbezpieczeństwa w danym sektorze gospodarki;
- Chmura obliczeniowa (ang. cloud computing) - nowoczesna technologia służąca do przechowywania, przetwarzania i zarządzania danymi. Opiera się na współdzielonych zasobach (oprogramowaniu i infrastrukturze). Dostarcza ją dostawca z danej organizacji lub też zewnętrzny dostawca. Dostęp do zasobów odbywa się przez internet;
- CSRD (ang. Corporate Sustainability Reporting Directive) – Dyrektywa Parlamentu Europejskiego i Rady (UE) 2022/2464 z dnia 14 grudnia 2022 r. w sprawie zmiany rozporządzenia (UE) nr 537/2014, dyrektywy 2004/109/WE, dyrektywy 2006/43/WE oraz dyrektywy 2013/34/UE w odniesieniu do sprawozdawczości przedsiębiorstw w zakresie zrównoważonego rozwoju. Dyrektywa nakłada obowiązek raportowania kwestii związanych z ryzykiem klimatycznym;
- DESI (ang. Digital Economy and Society Index) – indeks gospodarki cyfrowej i społeczeństwa cyfrowego, został stworzony na zlecenie Komisji Europejskiej jako narzędzie monitorujące wskaźniki postępu cyfrowego państw członkowskich UE;
- E-Doręczenia – elektroniczny odpowiednik listu poleconego za potwierdzeniem odbioru. Dzięki tej usłudze podmioty publiczne, obywatele i firmy mogą korzystać z wygodnych i bezpiecznych doręczeń elektronicznych. Są one równoważne prawnie tradycyjnej przesyłce poleconej za potwierdzeniem odbioru.
- Elektroniczna platforma usług administracji publicznej (ePUAP) - system teleinformatyczny, w którym instytucje publiczne udostępniają usługi przez pojedynczy punkt dostępowy w internecie (art. 3 pkt 13 ustawy z dnia 17 lutego 2005 r. o informatyzacji działalności podmiotów realizujących zadania publiczne (Dz. U. z 2024 r. poz. 304, 1222));
- Europejskie Ramy Interoperacyjności (ang. European Interoperability Framework, EIF) – unijne wspólnie uzgodnione podejście do świadczenia europejskich usług użyteczności publicznej w sposób interoperacyjny. Określono w nich podstawowe wytyczne dotyczące interoperacyjności w formie wspólnych zasad, modeli i zaleceń;

- Europejskie Wspólne Przedsięwzięcie w dziedzinie Obliczeń Wielkiej Skali (ang. European High Performance Computing Joint Undertaking, EuroHPC JU) – wspólna inicjatywa UE, krajów europejskich i partnerów prywatnych mająca na celu rozwój ekosystemu superkomputerów światowej klasy w Europie;
- Fundusze Venture Capital (Fundusze VC) – model finansowania inwestycji w przedsięwzięcia biznesowe na wczesnym etapie rozwoju, charakteryzujący się wysoką stopą ryzyka. Fundusze VC z reguły inwestują w przedsięwzięcia innowacyjne, tworzone przez niewielkie firmy, licząc na wysoką stopę zwrotu;
- Fundusze Private Equity (Fundusze PE)- model finansowania, w ramach którego gromadzone środki inwestowane są w przedsiębiorstwa o dużym potencjale wzrostu wartości. W odróżnieniu od funduszy VC, fundusze PE inwestują także w firmy na późniejszych etapach rozwoju;
- Generatywna sztuczna inteligencja (GenAI) - technologia, która za pomocą poleceń, pozwala użytkownikom tworzyć nowe treści. Algorytmy GenAI działają w oparciu o dane dostarczone zarówno na etapie tworzenia narzędzia jak i te wprowadzone w trakcie użytkowania;
- Hackaton - wydarzenie, podczas którego programiści, projektanci i inni specjaliści współpracują intensywnie w celu rozwiązania określonego problemu lub stworzenia nowego produktu w krótkim czasie, zazwyczaj od 24 do 72 godzin;
- ICT (ang. Information and Communication Technologies) - rodzina technologii umożliwiających przetwarzanie, gromadzenie i przesyłanie informacji w formie elektronicznej;
- Inteligentne miasto (ang. smart city) - obszar miejski, w którym technologia i gromadzenie danych pomagają poprawić jakość życia, a także zrównoważony rozwój i wydajność działania miasta. Jedną z technologii wykorzystywanych w ramach inteligentnych miast jest Internet Rzeczy (IoT);
- Inteligentna wieś (ang. smart village) – obszar wiejski, który wykorzystuje nowoczesne technologie w celu zrównoważonego i innowacyjnego rozwoju oraz celu poprawy jakości i poziomu życia jej mieszkańców;
- Interfejs programistyczny aplikacji (ang. application programming interface, API) – zbiór technicznych funkcji umożliwiających połączenie i wzajemną wymianę danych lub metadanych między programami komputerowymi lub systemami teleinformatycznymi (art. 2 pkt 9 ustawy z dnia 11 sierpnia 2021 r. o otwartych danych i ponownym wykorzystywaniu informacji sektora publicznego (Dz. U. z 2023 r. poz. 1524));
- Internet Rzeczy (ang. Internet of Things, IoT) – systemy, składające się z połączonych urządzeń często nazywanych "inteligentnymi". Urządzenia te zbierają i wymieniają między sobą dane oraz mogą być sterowane i monitorowane przez Internet;
- MŚP - mikroprzedsiębiorstwo lub małe lub średnie przedsiębiorstwo w rozumieniu art. 2 załącznika do zalecenia Komisji 2003/361/WE⁶¹;

⁶¹ Zalecenie Komisji 2003/361/WE z dnia 6 maja 2003 r. dotyczące definicji mikroprzedsiębiorstw oraz małych i średnich przedsiębiorstw (Dz.U. L 124 z 20.5.2003, s. 36).

- Ogólnopolska Sieć Edukacyjna (OSE) - program publicznej sieci telekomunikacyjnej dającej szkołom dostęp do szybkiego (100 Mb/s), bezpłatnego i bezpiecznego internetu;
- Otwarte oprogramowanie (ang. open-source) – rodzaj oprogramowania, którego kod źródłowy jest publicznie dostępny i może być swobodnie modyfikowany oraz dystrybuowany przez użytkowników;
- PLGrid - ogólnopolska infrastruktura obliczeniowa zbudowana w celu wsparcia badań naukowych i prac rozwojowych dla wielu dziedzin nauki i gospodarki. W ramach PLGrid możliwy jest dostęp do superkomputerów, komputerów kwantowych, specjalizowanych akceleratorów dla sztucznej inteligencji, chmury obliczeniowej, pamięci dyskowych, zoptymalizowanego oprogramowania obliczeniowego oraz wsparcia ekspertów z całej Polski;
- Przemysł 4.0 – termin odnoszący się do czwartej rewolucji przemysłowej, która oznacza integrację inteligentnych maszyn, systemów oraz wprowadzanie zmian w procesach produkcyjnych mających w celu zwiększenia wydajności wytwarzania oraz wprowadzenie możliwości elastycznych zmian asortymentu. Przemysł 4.0 dotyczy nie tylko technologii, ale też nowych sposobów pracy i roli ludzi w przemyśle;
- Rejestr publiczny - uporządkowany zbiór danych służący do realizacji zadań publicznych, prowadzony na podstawie przepisów ustawowych, przez podmiot realizujący zadania publiczne;
- Rozporządzenie eIDAS 2.0 – rozporządzenie Parlamentu Europejskiego i Rady (UE) 2024/1183 z dnia 11 kwietnia 2024 r. w sprawie zmiany rozporządzenia (UE) nr 910/2014 w odniesieniu do ustanowienia europejskich ram tożsamości cyfrowej (Dz. Urz. UE L 2024/ 1183 z 30.04.2024);
- Rozporządzenie GIA (ang. Gigabit Infrastructure Act) - unijne rozporządzenie o infrastrukturze gigabitowej, które ma na celu usprawnienie i przyspieszenie wdrażania sieci o bardzo wysokiej pojemności (VHCN), takich jak światłowody i 5G, w całej Europie;
- Rzeczywistość rozszerzona (ang. Augmented Reality, AR) - technologia, która łączy wirtualne elementy z rzeczywistym światem, tworząc interaktywne i wzbogacone doświadczenia dla użytkowników;
- Srebrna gospodarka, również gospodarka senioralna - sektor gospodarki ukierunkowany na osoby starsze;
- Startup - dynamiczna, zazwyczaj młoda firma lub projekt, który ma na celu wprowadzenie innowacyjnego produktu, usługi lub rozwiązania na rynek, poszukująca modelu biznesowego, który zapewniłby jej zyskowy rozwój;
- STEM (ang. science, technology, engineering, mathematics) – skrót oznaczający naukę, technologię, inżynierię, matematykę. Jest to termin używany do określenia tych czterech dziedzin, które są ze sobą powiązane i mają kluczowe znaczenie w kontekście edukacji oraz rozwoju zawodowego;
- System EZD – system teleinformatyczny do elektronicznego zarządzania dokumentacją umożliwiający wykonywanie w nim czynności kancelaryjnych, dokumentowanie przebiegu załatwiania spraw oraz gromadzenie i tworzenie dokumentów elektronicznych (§ 2 pkt 13 rozporządzenia Prezesa Rady Ministrów z dnia 18 stycznia 2011 r. w sprawie instrukcji kancelaryjnej, jednolitych rzeczowych

wykazów akt oraz instrukcji w sprawie organizacji i zakresu działania archiwów zakładowych);

- System EZD RP - system klasy EZD, którego możliwości, budowa i oferowane funkcje realizują rzeczywiste potrzeby biznesowe polskiej administracji publicznej. EZD RP powstał w ramach projektu realizowanego przez NASK w partnerstwie z Wojewodą Podlaskim. Jest wdrażany w środowiskach produkcyjnych kolejnych jednostek administracji publicznej i usprawnia ich funkcjonowanie poprzez udostępnienie nowoczesnych i uniwersalnych rozwiązań cyfrowych back-office w obszarze elektronicznego zarządzania dokumentacją;
- System Inwentaryzacji Systemów Teleinformatycznych (SIST) — system teleinformatyczny służący do zbierania informacji o planowanych, istniejących i wycofanych systemach teleinformatycznych, współpracy pomiędzy nimi, rejestrach prowadzonych przez administrację publiczną oraz możliwościach wykorzystania zbieranych w nich informacji;
- System teleinformatyczny - zespół współpracujących ze sobą urządzeń informatycznych i oprogramowania zapewniający przetwarzanie, przechowywanie, a także wysyłanie i odbieranie danych przez sieci telekomunikacyjne za pomocą właściwego dla danego rodzaju sieci telekomunikacyjnego urządzenia końcowego w rozumieniu przepisów ustawy z dnia 16 lipca 2004 r. – Prawo telekomunikacyjne (Dz. U. z 2016 r. poz. 1489, 1579, 1823, 1948, 1954 i 2003) (art. 3 pkt 3 ustawy z dnia 17 lutego 2005 r. o informatyzacji działalności podmiotów realizujących zadania publiczne (Dz. U. z 2024 r. poz. 304, 1222);
- System zarządzania cyberbezpieczeństwem S46 – system teleinformatyczny, który wspiera zgłaszanie i obsługę incydentów, wymianę informacji i współpracę pomiędzy uczestnikami krajowego systemu cyberbezpieczeństwa (KSC). Zapewnia również szacowanie ryzyka na poziomie krajowym i ostrzeżenie o zagrożeniach cyberbezpieczeństwa;
- Sztuczna Inteligencja (ang. Artificial Intelligence, AI/SL) - dziedzina wiedzy obejmująca m.in. sieci neuronowe, robotykę i tworzenie modeli zachowań inteligentnych oraz programów komputerowych symulujących te zachowania, włączając w to również uczenie maszynowe (ang. machine learning), głębokie uczenie (ang. deep learning) oraz uczenie wzmocnione (ang. reinforcement learning);
- Wirtualna rzeczywistość (ang. Virtual Reality, VR) – stworzony za pomocą technologii informatycznej trójwymiarowy obraz, który imituje świat realny lub stanowi wizję świata fikcyjnego (wygenerowane komputerowo otoczenie);
- Wysokowydajne przetwarzanie komputerowe (ang. High-performance computing, HPC) – zaawansowana infrastruktura obliczeniowa przeznaczona do realizacji najbardziej wymagających zadań naukowych, inżynierskich oraz komercyjnych;
- Zasada bezpieczeństwa w fazie projektowania (ang. security by design) - podejście, które zakłada, że bezpieczeństwo systemów informatycznych powinno być integralną częścią procesu projektowania i tworzenia;
- Zasada etyki na etapie projektowania (ang. ethics by design) - podejście, które integruje kwestie etyczne na etapie projektowania technologii, w szczególności w kontekście sztucznej inteligencji (AI) i innych nowoczesnych rozwiązań technologicznych;

- Zasada otwartości w fazie projektowania i otwartości domyślnej – podejście, które promuje dostępność danych i informacji w sposób umożliwiający ich swobodne wykorzystanie i ponowne wykorzystywanie, już na etapie projektowania;
- Zasada prywatności w fazie projektowania (ang. privacy by design) - podejście, które zakłada, że kwestie związane z prywatnością (ochroną danych osobowych) powinny być integralną częścią procesu projektowania systemów, aplikacji i usług;
- Zespół Reagowania na Incydenty Bezpieczeństwa Komputerowego (ang. Computer Security Incident Response Team, CSIRT) – zespół odpowiadający za koordynację procesu reagowania na incydenty komputerowe występujące w obszarze wskazanym w art. 26 ust. 7 ustawy z dnia 5 lipca 2018 roku o krajowym systemie cyberbezpieczeństwa (Dz.U.2018 poz.1560).