KONFEDERACJA LEWIATAN

STANOWISKO KONFEDERACJI LEWIATAN
W SPRAWIE HORYZONTALNEGO UWZGLĘDNIENIA CYFRYZACJI I CYBERBEZPIECZEŃSTWA W PLANIE PARTNERSTWA KRAJOWEGO I REGIONALNEGO NA LATA 2028–2034

Konfederacja Lewiatan postuluje, aby transformacja cyfrowa i cyberbezpieczeństwo zostały potraktowane w Planie Partnerstwa Krajowego i Regionalnego na lata 2028–2034 jako horyzontalne czynniki konkurencyjności, odporności i sprawności państwa, obecne we wszystkich priorytetach oraz właściwych dla nich reformach i inwestycjach.

Cyfryzacja nie powinna zostać ograniczona do jednego kierunku interwencji ani utożsamiona wyłącznie z zakupem sprzętu, oprogramowania lub uruchamianiem kolejnych e-usług. Powinna obejmować zmianę procesów, wykorzystanie danych, automatyzację, sztuczną inteligencję, rozwój infrastruktury cyfrowej, kompetencje oraz zdolność organizacji do bezpiecznego wykorzystywania technologii.

Cyberbezpieczeństwo powinno natomiast stanowić obowiązkowy element projektowania każdej inwestycji cyfrowej oraz cyfryzacji poszczególnych sektorów. Dotyczy to zarówno przedsiębiorstw, jak i administracji publicznej, ochrony zdrowia, transportu, energetyki oraz infrastruktury krytycznej.

Postulaty Konfederacji Lewiatan odnoszą się do wszystkich czterech priorytetów PPKR.

I. Priorytet 1 – Konkurencyjność międzynarodowa Polski

Kierunek A.1 – Wzmocnienie współpracy nauki i biznesu oraz transferu technologii

Współpraca nauki i biznesu powinna zostać silnie ukierunkowana na testowanie, rozwój i wdrażanie technologii cyfrowych, w szczególności rozwiązań z zakresu sztucznej inteligencji, automatyzacji, robotyzacji, analityki danych i Przemysłu 4.0.

Przedsiębiorstwa powinny mieć możliwość korzystania z infrastruktury uczelni i instytucji badawczych w celu pilotażowego testowania technologii przed rozpoczęciem pełnoskalowej inwestycji. Dotyczy to m.in. laboratoriów cyfrowych, środowisk symulacyjnych, infrastruktury obliczeniowej, centrów danych.

PPKR powinien określić przejrzyste zasady finansowania dostępu przedsiębiorstw do infrastruktury badawczej i cyfrowej. Instrument powinien być dostępny zarówno dla MŚP, jak i dużych przedsiębiorstw, ponieważ ryzyko technologiczne związane z cyfryzacją występuje niezależnie od wielkości firmy.

Kierunek A.3 – Transformacja cyfrowa przedsiębiorstw

Kierunek A.3 powinien być jednym z kluczowych obszarów interwencji PPKR. Jego zakres należy jednak rozszerzyć tak, aby odpowiadał całemu procesowi transformacji cyfrowej przedsiębiorstw, a nie jedynie zakupowi podstawowych narzędzi informatycznych.

Opis wyzwania powinien uwzględniać globalną konkurencję technologiczną, rosnące znaczenie sztucznej inteligencji, konieczność zwiększenia produktywności przedsiębiorstw, znaczenie danych, automatyzację i robotyzację, rosnące zagrożenia dla bezpieczeństwa systemów, danych i łańcuchów dostaw.

PPKR powinien być spójny ze Strategią Cyfryzacji Państwa oraz wspierać rozwój i wykorzystanie technologii oferowanych przez polskich i europejskich dostawców.

Cyberbezpieczeństwo powinno zostać bezpośrednio wpisane do zakresu kierunku A.3. Nie może być traktowane jako odrębny lub fakultatywny dodatek do inwestycji cyfrowych. Każdy projekt transformacji cyfrowej powinien uwzględniać analizę ryzyka cyberbezpieczeństwa. Wsparcie powinno obejmować trzy powiązane wymiary:

- organizacyjny – zarządzanie ryzykiem, polityki bezpieczeństwa, procedury reagowania na incydenty, bezpieczeństwo dostawców, plany ciągłości działania i odtwarzania po awarii,
- techniczny – sprzęt, oprogramowanie, zabezpieczenia systemów IT i OT, monitoring, systemy wykrywania incydentów, rozwiązania do tworzenia odpornych kopii zapasowych i ochrony danych,
- kompetencyjny – szkolenia zarządów, kadry kierowniczej, specjalistów oraz wszystkich pracowników korzystających z systemów cyfrowych.

Instrumenty cyfryzacji nie powinny być ograniczone wyłącznie do MŚP. Duże przedsiębiorstwa i mid-capy także ponoszą wysokie koszty wdrażania złożonych systemów cyfrowych i rozwijają rozwiązania wykorzystywane przez całe łańcuchy dostaw. Ponadto wpływają na standardy technologiczne i cyberbezpieczeństwo mniejszych partnerów oraz tworzą zapotrzebowanie na usługi polskich firm technologicznych.

Wsparcie nie powinno być również kierowane jedynie do firm znajdujących się na podstawowym poziomie dojrzałości cyfrowej. Interwencja powinna obejmować zarówno podstawową cyfryzację, jak i przechodzenie przedsiębiorstw na kolejne poziomy zaawansowania technologicznego.

Warto przewidzieć instrument umożliwiający testowanie rozwiązań z zakresu sztucznej inteligencji, Przemysłu 4.0, automatyzacji, robotyzacji, analizy danych, Internetu rzeczy, rozwiązań chmurowych, cyberbezpieczeństwa. Przedsiębiorstwo powinno mieć możliwość przeprowadzenia pilotażu, testu integracyjnego lub proof of concept przed rozpoczęciem pełnej inwestycji. Instrument powinien finansować również testy bezpieczeństwa oraz ocenę zgodności technologii z wymaganiami organizacyjnymi, technicznymi i regulacyjnymi.

Zakres wsparcia powinien obejmować także dostęp przedsiębiorstw do infrastruktury obliczeniowej, rozwiązań chmurowych, modeli sztucznej inteligencji, narzędzi do trenowania i dostosowywania modeli, bezpiecznych środowisk przetwarzania danych i wysokiej jakości zbiorów danych treningowych. Wsparciem powinny zostać objęte także podmioty tworzące i porządkujące sektorowe zbiory danych, w tym rozwiązania typu „data lakes for Industry". Bez dostępu do odpowiednio przygotowanych, interoperacyjnych i bezpiecznych danych rozwój sztucznej inteligencji w przedsiębiorstwach będzie ograniczony.

Doświadczenia z regionalnymi instrumentami cyfryzacji wskazują na ryzyko długiego procesu oceny, nadmiernej liczby załączników i różnic interpretacyjnych. Zasadne jest zatem wdrażanie podstawowego instrumentu transformacji cyfrowej przedsiębiorstw na poziomie krajowym,

z możliwością uzupełnienia go działaniami regionalnymi odpowiadającymi na specyficzne potrzeby terytorialne.

Kierunek A.5 – Rozwój infrastruktury transportowej i logistycznej

Cyfryzacja powinna być jednym z komponentów modernizacji transportu i logistyki. Inwestycje infrastrukturalne powinny być łączone z wdrażaniem interoperacyjnych systemów cyfrowych umożliwiających sprawne zarządzanie ruchem, przepływem towarów, dokumentacją i informacją.

Wsparcie powinno obejmować np. systemy zarządzania slotami w terminalach i portach, cyfrową awizację pojazdów, elektroniczną wymianę danych między uczestnikami łańcuchów dostaw, narzędzia do planowania przewozów intermodalnych, cyfrowe systemy zarządzania terminalami, systemy zarządzania ruchem i informacją pasażerską.

Cyberbezpieczeństwo musi być obowiązkowym elementem tych inwestycji. Dotyczy to zarówno systemów transportu publicznego, jak i infrastruktury logistycznej oraz portowej. Porty morskie, terminale i systemy zarządzania transportem są elementami infrastruktury o strategicznym znaczeniu.

II. Priorytet 2 – Spójność i rozwój terytorialny

Kierunek B.1 – Rozwój gospodarczy regionów

Rozwój regionalny w coraz większym stopniu zależy od działalności usługowej, technologicznej i cyfrowej. Regionalne specjalizacje mogą obejmować m.in.: usługi cyfrowe, technologie informacyjne, sztuczną inteligencję, cyberbezpieczeństwo, rozwiązania dla gospodarki cyfrowej, usługi świadczone zdalnie. PPKR powinien umożliwiać wspieranie tych działalności, jeżeli generują wysoką wartość dodaną, zwiększają odporność gospodarczą regionów i tworzą atrakcyjne miejsca pracy.

Kierunek B.3 – Rozwój obszarów zmarginalizowanych i dostęp do usług

Cyfryzacja powinna być wykorzystywana jako narzędzie ograniczania różnic rozwojowych. Interwencja nie może jednak ograniczać się do budowy infrastruktury. Musi obejmować również dostępność usług, kompetencje, bezpieczeństwo oraz zdolność przedsiębiorstw i instytucji do wykorzystywania technologii.

Programy rozwoju przedsiębiorczości na obszarach zmarginalizowanych powinny obejmować wsparcie cyberbezpieczeństwa firm. Podobnie wsparcie infrastruktury wodno-kanalizacyjnej powinno obejmować cyfrowe systemy monitorowania, sterowania i zarządzania zasobami. Jednocześnie konieczne jest finansowanie cyberbezpieczeństwa takich systemów, w szczególności zabezpieczenia infrastruktury OT, kontroli dostępu, tworzenia kopii zapasowych oraz zdolności reagowania na incydenty.

Należy rozważyć instrument voucherowy umożliwiający korzystanie z nowoczesnych usług łączności osobom znajdującym się w mniej korzystnej sytuacji, w szczególności mieszkańcom obszarów trudnodostępnych, mieszkańcom terenów słabo zurbanizowanych, osobom starszym, osobom o niższych dochodach, grupom zagrożonym wykluczeniem cyfrowym. Budowa sieci bez zapewnienia ekonomicznej dostępności usług nie pozwoli na pełne wykorzystanie potencjału infrastruktury.

Kierunek B.6 – Odporność obszarów przygranicznych

Odporność obszarów przygranicznych powinna obejmować kompleksowy komponent cyfrowy. Regiony te mogą być szczególnie narażone na cyberataki, działania dezinformacyjne, zakłócenia łączności. Wsparcie powinno obejmować cyberbezpieczeństwo przedsiębiorstw, administracji i infrastruktury krytycznej, jak również rozwój odpornych systemów komunikacji i zarządzania kryzysowego.

Kierunek B.7 – Ochrona zdrowia

W PPKR powinien zostać wyodrębniony czytelny obszar poświęcony cyfrowej transformacji ochrony zdrowia, obejmujący cały ekosystem podmiotów leczniczych, a nie wyłącznie centralne systemy administracji. Wsparcie powinno obejmować m.in. modernizację infrastruktury IT, interoperacyjność systemów, bezpieczną wymianę danych, wykorzystanie sztucznej inteligencji, telemedycynę, rozwój kompetencji cyfrowych personelu.

Każdy projekt cyfryzacji ochrony zdrowia powinien obejmować zagadnienia związane z cyberbezpieczeństwem. Cyberbezpieczeństwo jest warunkiem bezpiecznego wdrażania Europejskiej Przestrzeni Danych Zdrowotnych oraz dalszego rozwoju usług opartych na danych.

W obliczu wyzwań demograficznych wsparcie powinno obejmować oprogramowanie i urządzenia umożliwiające prowadzenie zdalnej opieki długoterminowej w modelu domowo-ambulatoryjnym. Dotyczy to w szczególności zdalnego monitorowania parametrów pacjenta, systemów kontaktu pacjenta z personelem czy cyfrowej koordynacji opieki.

III. Priorytet 3 – Transformacja energetyczna, odporność i bezpieczeństwo

Kierunki C.1, C.3 i C.6 – Cyfryzacja sektora energetycznego

Transformacja energetyczna wymaga równoległej transformacji cyfrowej. Rozwój rozproszonych źródeł energii, magazynów, elektromobilności i usług elastyczności nie będzie możliwy bez zaawansowanych systemów zarządzania danymi i infrastrukturą.

PPKR powinien wspierać inteligentne sieci energetyczne, cyfrowe systemy zarządzania siecią, wirtualne elektrownie, systemy zarządzania popytem, automatyzację bilansowania, cyfrową integrację magazynów energii i źródeł OZE, rozwiązania Vehicle-to-Grid i Vehicle-to-Home, platformy wymiany danych energetycznych, systemy prognozowania produkcji i zużycia energii.

Cyfryzacja energetyki musi być bezpośrednio powiązana z cyberbezpieczeństwem. Rozwój inteligentnych i rozproszonych systemów zwiększa liczbę punktów potencjalnego ataku i wymaga finansowania ochrony infrastruktury IT i OT, bezpiecznej komunikacji oraz monitorowania incydentów.

Kierunek C.6 – Wzmocnienie odporności na zagrożenia związane z bezpieczeństwem państwa i obywateli

W PPKR należy wyraźnie wskazać, że odporność państwa obejmuje także odporność cyfrową gospodarki i systemów łączności. Bez nowoczesnej, bezpiecznej i odpornej infrastruktury telekomunikacyjnej niemożliwa będzie realizacja wielu pozostałych celów planu.

Cyberbezpieczeństwo powinno zostać uwzględnione zarówno w instrumentach horyzontalnych, jak i w działaniach sektorowych skierowanych do poszczególnych branż. Warto dodać rezultat strategiczny dotyczący zwiększenia odporności cyfrowej przedsiębiorstw, w tym MŚP. Powinna mu odpowiadać inwestycja wspierająca diagnozę poziomu cyberbezpieczeństwa przedsiębiorstw, budowę kompetencji, zakup i wdrażanie rozwiązań technicznych, bezpieczeństwo systemów IT i OT, monitoring zagrożeń, wykrywanie i obsługę incydentów, ciągłość działania, bezpieczeństwo łańcuchów dostaw.

Warto dodać także cel szczegółowy dotyczący odpornej i bezpiecznej infrastruktury łączności cyfrowej oraz inwestycję skierowaną do operatorów telekomunikacyjnych. Wsparcie powinno obejmować systemy awaryjnego zasilania stacji bazowych, instalacje OZE i nowoczesne baterie podtrzymujące, cyfrowe systemy zarządzania energią, zabezpieczenia obiektów telekomunikacyjnych, rozwiązania antydronowe, sensory wykrywające zagrożenia, monitoring wizyjny, kontrolę dostępu, systemy automatycznego powiadamiania służb.

Interwencja powinna obejmować także urządzenia zwiększające zasięg i odporność sieci mobilnych, w tym mobilne stacje bazowe i wzmacniacze sygnału. Rozwiązania te powinny wspierać utrzymanie łączności mieszkańców, administracji, przedsiębiorstw i służb w sytuacjach kryzysowych.

IV. Priorytet 4 – Sprawne państwo i ochrona wartości Unii Europejskiej

Kierunek D.1 – Dialog społeczny, społeczeństwo obywatelskie i zdolności partnerów społecznych

Wsparcie partnerów społecznych powinno mieć wyraźny i rozbudowany wymiar cyfrowy. Cyfryzacja jest nie tylko jednym z obszarów, który powinien być przedmiotem dialogu społecznego, ale również narzędziem zwiększającym jakość, zasięg i efektywność samego dialogu.

Partnerzy społeczni powinni uzyskać finansowanie pozwalające im korzystać z nowoczesnych narzędzi cyfrowych w procesie przygotowywania stanowisk, prowadzenia konsultacji, gromadzenia danych od organizacji członkowskich. Należy umożliwić budowę cyfrowych platform konsultacji, które pozwolą zwiększyć transparentność dialogu, skrócić czas konsultacji, dokumentować potrzeby reprezentowanych grup.

Partnerzy społeczni powinni prowadzić analizy dotyczące wpływu sztucznej inteligencji, automatyzacji, pracy zdalnej i hybrydowej, cyberzagrożeń na warunki pracy, zatrudnienie, produktywność, zdrowie pracowników i konkurencyjność przedsiębiorstw. Powinni także uczestniczyć w tworzeniu rekomendacji dotyczących bezpiecznego, odpowiedzialnego i społecznie akceptowalnego wdrażania nowych technologii.

Kierunek D.2 – Sprawny wymiar sprawiedliwości

Cyfryzacja sądów i prokuratury powinna obejmować nie tylko uruchamianie e-usług, ale kompleksową zmianę sposobu prowadzenia postępowań, zarządzania dokumentacją i komunikacji z użytkownikami. Wsparcie powinno obejmować interoperacyjność systemów, cyfrowy obieg dokumentów, bezpieczne udostępnianie akt.

Kierunek D.3 – Sprawna administracja publiczna

Cyfryzacja administracji powinna prowadzić do rzeczywistego przeprojektowania usług i procesów, a nie jedynie do elektronicznego odwzorowania dotychczasowych procedur. Interwencja powinna obejmować projektowanie usług wokół potrzeb użytkownika, integrację rejestrów i systemów, bezpieczną wymianę danych, automatyzację procesów.

Warto rozważyć wzmocnienie działań związanych z cyberbezpieczeństwem administracji publicznej, ze szczególnym uwzględnieniem jednostek samorządu terytorialnego. Ze względu na zróżnicowane potrzeby i poziom dojrzałości cyfrowej jednostek samorządu terytorialnego inwestycja nie powinna być wdrażana wyłącznie centralnie. Zasadne jest zastosowanie poziomu krajowego i regionalnego, z odpowiednią rolą ministra właściwego do spraw cyfryzacji oraz samorządów województw.

Podsumowanie

W ocenie Konfederacji Lewiatan cyfryzacja i cyberbezpieczeństwo powinny być widoczne we wszystkich priorytetach PPKR oraz na każdym etapie projektowania i realizacji interwencji.

Postulujemy w szczególności:

- wyraźne włączenie cyberbezpieczeństwa do inwestycji cyfrowych,
- uwzględnianie komponentów cyfrowych w działaniach sektorowych,
- zapewnienie wsparcia dla cyfryzacji przedsiębiorstw niezależnie od ich wielkości,
- rozwój infrastruktury AI, danych i mocy obliczeniowej,
- finansowanie pilotażowego testowania technologii,
- cyfrową transformację ochrony zdrowia, transportu, energetyki i administracji,
- utworzenie instrumentów cyberbezpieczeństwa przedsiębiorstw i administracji,
- rozwój odpornej infrastruktury telekomunikacyjnej,
- wsparcie cyfrowych platform dialogu społecznego;
- zapewnienie interoperacyjności, trwałości cyfrowej i bezpieczeństwa finansowanych systemów.

Tak zaprojektowany PPKR pozwoli wykorzystać technologie cyfrowe jako rzeczywisty czynnik wzrostu produktywności, poprawy usług publicznych i zwiększenia odporności państwa. Jednocześnie zapewni, że transformacja cyfrowa będzie bezpieczna, inkluzywna i prowadzona z udziałem przedsiębiorstw, administracji, partnerów społecznych oraz innych podmiotów bezpośrednio doświadczających jej skutków.