Rzecznik Małych i Średnich Przedsiębiorców | Samodzielny Organ Ochrony Prawa

Warszawa, dnia 24 lipca 2025 r.

WPL.279.2025.GG

Pan
Dr n. hum. Krzysztof Gawkowski
Wiceprezes Rady Ministrów
Minister Cyfryzacji
Pełnomocnik Rządu ds. Cyberbezpieczeństwa
ul. Królewska 27, 00-060 Warszawa
e-mail: sekretariat.bm@cyfra.gov.pl
sekretariat.dp@cyfra.gov.pl
kancelaria@cyfra.gov.pl

Szanowny Panie Premierze,

w związku z przekazaniem do konsultacji Projektu uchwały Rady Ministrów w sprawie Strategii Cyberbezpieczeństwa Rzeczypospolitej Polskiej na lata 2025–2029[1], uprzejmie proszę o przyjęcie poniższych uwag.

Strategia cyberbezpieczeństwa ma charakter strategiczno-operacyjny, ale zawiera również istotne elementy prawne poprzez odniesienie do obowiązujących aktów normatywnych i wytyczne, które powinny być uwzględniane w procesie tworzenia prawa związanego z cyberbezpieczeństwem. Zgodnie z art. 93 ust. 1 Konstytucji Rzeczpospolitej Polskiej[2] uchwały Rady Ministrów oraz zarządzenia Prezesa Rady Ministrów i Ministrów mają charakter wewnętrzny i obowiązują tylko jednostki organizacyjnie podległe organowi wydającemu te akty, jednak należy zwrócić uwagę na praktyczne znaczenia oraz skutki dla przedsiębiorców, jakie może nieść Strategia.

[1] Nr wykazu: ID131, dalej: „Strategia".
[2] Konstytucja Rzeczypospolitej Polskiej z dnia 2 kwietnia 1997 r., Dz. U. Nr 78, poz. 483 z późn. zm., dalej: „Konstytucja RP".

Biuro Rzecznika Małych i Średnich Przedsiębiorców, ul. Wilcza 46, 00-679 Warszawa, NIP: 7010832846, REGON: 380779546,
tel. +48 22 1237070, fax: +48 22 1237071, epuap: /RzecznikMSP/kancelaria, e-mail: biuro@rzecznikmsp.gov.pl

Administratorem danych osobowych jest Rzecznik Małych i Średnich Przedsiębiorców z siedzibą w Warszawie. Dane przetwarzane są w celu prowadzenia korespondencji, wypełnienia obowiązków prawnych (art. 6 ust. 1 lit. c RODO), realizacji zadań publicznych (art. 6 ust. 1 lit. e RODO) oraz archiwizacji i celów dowodowych (art. 6 ust. 1 lit. f RODO). Odbiorcami mogą być podmioty uprawnione na podstawie przepisów prawa. Dane będą przechowywane zgodnie z przepisami o archiwizacji. Przysługuje Państwu prawo dostępu do danych, ich sprostowania, ograniczenia przetwarzania oraz wniesienia skargi do Prezesa UODO. Więcej informacji: https://rzecznikmsp.gov.pl/kontakt/#rodo.
https://www.facebook.com/BiuroRzecznikaMSP/ https://rzecznikmsp.gov.pl/
https://x.com/RzecznikMSP https://rzecznikmsp.gov.pl/kontakt/newsletter/
https://www.youtube.com/rzecznikmsp https://naukaibiznes.rzecznikmsp.gov.pl/

Mając powyższe na względzie, podczas analizy projektu Strategii dostrzeżono następujące wątpliwości:

1. Realizacja głównego celu Strategii (ppkt 4.2 Strategii), powinna odbywać się z uwzględnianiem zasady proporcjonalności w zakresie wymogu stosowania środków technicznych, operacyjnych i organizacyjnych w celu zarządzania ryzykiem dla bezpieczeństwa sieci i systemów informatycznych wykorzystywanych przez podmioty kluczowe i podmioty ważne, do których zaliczani są również przedsiębiorcy, niezależnie od ich wielkości.[3] (ppkt. 5.1. Strategii). Doskonalenie i rozwój krajowego systemu cyberbezpieczeństwa wiąże się z ponoszeniem znacznych nakładów na dostosowanie lub wymianę różnego rodzaju infrastruktury technologicznej, dlatego w procesie opracowywania regulacji, w szczególności wymogów oraz obowiązków nakładanych na mikroprzedsiebiorców, małych i średnich przedsiębiorców[4], z tego powodu zasada proporcjonalności ma dla nich charakter gwarancyjny.

   Ponadto w razie zamiaru wprowadzenia istotnych zmian procedur, ograniczeń czy też konieczności wymiany produktów, usług lub procesów ICT, obligatoryjne powinno być szacowanie kosztów takich operacji dla krajowej gospodarki (np. w przypadku instytucji uznania dostawcy za dostawcę wysokiego ryzyka), zwłaszcza w kontekście stosunkowo niewielkiej liczby krajowych dostawców tego rodzaju produktów i powiązanych z nimi usług i procesów oraz uprzednie badanie dostępności na rynku alternatywnych rozwiązań w świetle niewielkiej liczby dostawców produktów, usług i procesów ICT, a także spodziewanych problemów z zaopatrzeniem. Weryfikacja taka może następnie stanowić podstawę do przygotowania i wdrożenia środków rekompensujących obowiązkowa wymianę elementów posiadanej infrastruktury,

[3] „Jako podstawowy obowiązek należy wskazać stosowanie odpowiednich i proporcjonalnych środków technicznych, operacyjnych i organizacyjnych w celu zarządzania ryzykiem dla bezpieczeństwa sieci i systemów informatycznych wykorzystywanych przez te podmioty do prowadzenia działalności lub świadczenia usług oraz w celu zapobiegania wpływowi incydentów na odbiorców ich usług lub na inne usługi bweryfikacji bądź minimalizowania takiego wpływu.” – str. 14 Strategii.
[4] Dalej: „sektor MŚP”.

przynajmniej dla przedsiębiorców sektora MŚP. Rozważenia wymagają również możliwości dodatkowego wsparcia dla krajowych producentów i dostawców tego rodzaju sprzętu, usług i procesów.

Deklaracja konieczności wzmocnienia podstawowego poziomu cyberodporności i higieny cyfrowej ma fundamentalne znaczenie, jednak z punktu widzenia sektora MŚP mechanizmy wsparcia, o których mowa w Strategii[5], w kontekście zamiaru wprowadzenia niektórych regulacji i ograniczeń (np. instytucji dostawy wysokiego ryzyka) powinny mieć charakter obowiązkowy. Przedsiębiorcy i ich organizacje podczas prac Zespołów Roboczych powołanych w ramach Rady Przedsiębiorców przy Rzeczniku Małych i Średnich Przedsiębiorców wskazują, że ze względu na wąski międzynarodowy rynek dostawców nowoczesnych technologii oraz niewielu producentów krajowych i unijnych, branża ICT jest bardzo wrażliwa na wszelkie działania regulacyjne.

Strategia powinna również zwracać uwagę na uwzględnianie w ewentualnych pracach legislacyjnych art. 66 ustawy z dnia 6 marca 2018 r. Prawa przedsiębiorców[6], który stanowi, że przed rozpoczęciem prac nad opracowaniem projektu aktu normatywnego określającego zasady podejmowania, wykonywania lub zakończenia działalności gospodarczej dokonuje się: oceny jego wpływu na mikroprzedsiębiorców, małych i średnich przedsiębiorców oraz analizy zgodności projektowanych regulacji z przepisami tej ustawy.

2. Analiza Strategii wskazuje na potrzebę uporządkowania kluczowych pojęć oraz ich wzajemnej relacji. Zgodnie z art. 4 pkt 3 Dyrektywy Parlamentu Europejskiego i Rady (UE) 2016/1148 z dnia 6 lipca 2016 r. w sprawie środków na rzecz wysokiego wspólnego poziomu bezpieczeństwa sieci i systemów informatycznych na terytorium Unii[7], do którego odsyła definicja zawarta w art. 2 pkt. 3 Rozporządzenia Parlamentu

[5] Strategia, s. 28.
[6] T.j. Dz. U. z 2024 r. poz. 236 z późn. zm.
[7] Dz. U. UE. L. z 2016 r. Nr 194, str. 1, z późn, zm., dalej: „Dyrektywa (UE) 2016/1148".

Europejskiego i Rady (UE) 2019/881 z dnia 17 kwietnia 2019 r. w sprawie ENISA (Agencji Unii Europejskiej ds. Cyberbezpieczeństwa) oraz certyfikacji cyberbezpieczeństwa w zakresie technologii informacyjno-komunikacyjnych oraz uchylenia rozporządzenia (UE) nr 526/2013 (tzw. akt o cyberbezpieczeństwie)[8] – krajowa strategia w zakresie bezpieczeństwa sieci i systemów informatycznych oznacza ramy zapewniające strategiczne cele i priorytety w zakresie bezpieczeństwa sieci i systemów informatycznych na poziomie krajowym. Należy jednak zwrócić uwagę, iż w chwili obecnej trwają prace nad projektem ustawy o zmianie ustawy o krajowym systemie cyberbezpieczeństwa oraz niektórych innych ustaw[9], w którym planowane są istotne zmiany, jednak do czasu ich zakończenia w mocy pozostają przepisy Rozdziału 13 Strategia ustawy z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa[10], względnie definicje zawarte we wspomnianym Rozporządzeniu (UE) 2019/881, jako akcie bezpośrednio obowiązującym.

W tych okolicznościach cel główny Strategii wydaje się być sformułowany w sposób niewystarczająco dokładny oraz nieuwzględniający wszystkich ważnych elementów, takich jak np. zapobieganie zagrożeniom, którego znaczenie jest równie istotne jak ich wykrywanie i adekwatna reakcja.

Z przytoczonych powodów warto rozważyć usystematyzowanie najistotniejszych pojęć w kontekście możliwej zmiany ich znaczenia w najbliższym czasie.

3. Strategia, ze względu na specyfikę dziedziny, której dotyczy, odnosi się do szerokiego kręgu organów, zróżnicowanego rodzaju procedur, także sądowo-administracyjnych oraz licznej grupy przedsiębiorców, w tym z sektora MŚP.

   W takich okolicznościach wymagane wydaje się, aby decyzje o znacznym zasięgu oddziaływania podlegały możliwie szerokiej konsultacji między organami właściwymi,

[8] Dz. U. UE. L. z 2019 r. Nr 151, str. 15 z późn. zm., dalej: „Rozporządzenie (UE) 2019/881.
[9] Nr w wykazie prac legislacyjnych Rady Ministrów: UC 32, dalej „nowelizacja ustawy o KSC".
[10] T.j. Dz. U. z 2024 r. poz. 1077, z późn. zm., dalej: „ustawa o KSC".

z udziałem przedstawicieli organów ochrony prawa, w tym praw przedsiębiorców (Rzecznik Małych i Średnich Przedsiębiorców). Stosowne uzupełnienie strategii w tym zakresie może być niezbędne.

4. Biorąc pod uwagę znaczenie przedmiotu Strategii, ponownej analizy może wymagać podniesienie priorytetu zadań o charakterze stymulowanie badań, rozwoju i innowacji w obszarze cyberbezpieczeństwa (ppkt 8.2 Strategii), w szczególności przez wspieranie i stymulowanie rozwoju polskiego potencjału przemysłowego, technologicznego i naukowego w zakresie cyberbezpieczeństwa. W tym kontekście zasadny jawi się postulat, by działania opisane w ppkt 8.2 Strategii zostały uznane za priorytetowe w ramach: „Celu szczegółowego 4. Zwiększanie potencjału krajowej bazy technologiczno-przemysłowej oraz wzmocnienie suwerenności technologicznej Rzeczypospolitej Polskiej w obszarze cyberbezpieczeństwa” (pkt 8 Strategii).

Mając na względzie dostrzeżone wątpliwości oraz doniosłość Strategii Cyberbezpieczeństwa Rzeczypospolitej Polskiej, wyrażam nadzieję, że załączone uwagi spotkają się z aprobatą projektodawcy, a ich uwzględnienie pozwoli na dalej idące wzmocnienie bezpieczeństwa państwa oraz przedsiębiorców sektora MŚP i zwracam się z prośbą o ich rozważenie w ramach dalszych prac nad projektem Strategii.

Z wyrazami szacunku

Agnieszka Maria Majewska

Elektronicznie podpisany przez Agnieszka Maria Majewska
Data: 2025.07.25 21:15:10 +02'00'

Agnieszka Majewska
Rzecznik
Małych i Średnich Przedsiębiorców