PROJEKT STANOWISKA RZĄDU

przygotowany w związku z art. 6 ust. 1 pkt 2 ustawy z dnia 11 marca 2004 r. o współpracy Rady Ministrów z Sejmem i Senatem w sprawach związanych z członkostwem Rzeczypospolitej Polskiej w Unii Europejskiej (Dz. U. nr 52, poz. 515 z późn. zm.)

Dotyczy	Proposal for a Regulation of the European Parliament and of the Council concerning the European Network and Information Security Agency (ENISA)

Data przekazania dokumentu Polsce przez SG Rady UE	1 października 2010 r.

Sygnatura dokumentu	Komisja Europejska	COM(2010) 521
	Rada UE	14358/10
	Numer międzyinstytucjonalny	2010/0275 (COD)

Procedura decyzyjna	Zwykła procedura prawodawcza

Tryb głosowania w Radzie UE	Większość kwalifikowana

Instytucja wiodąca	Ministerstwo Spraw Wewnętrznych i Administracji

Instytucje współpracujące	Ministerstwo Infrastruktury Urząd Komunikacji Elektronicznej

Data przyjęcia przez KSE	29 grudnia 2010 r.

I. Cel projektu aktu prawnego

We wniosku w sprawie rozporządzenia Parlamentu Europejskiego i Rady w sprawie Europejskiej Agencji ds. Bezpieczeństwa Sieci i Informacji (ENISA) Komisja Europejska przedstawia propozycję modernizacji Agencji ENISA – COM(2010)521. Zgodnie z założeniami KE wymienione rozporządzenie towarzyszy innemu wnioskowi w sprawie rozporządzenia Parlamentu Europejskiego i Rady zmieniającego rozporządzenie (WE) nr 460/2004 ustanawiające Europejską Agencję ds. Bezpieczeństwa Sieci i Informacji (ENISA) w zakresie okresu jej działania do dnia 13 września 2013 roku – COM(2010)520.
Celem wniosku w sprawie Europejskiej Agencji ds. Bezpieczeństwa Sieci i Informacji (ENISA) – COM(2010)521 jest gruntowna zmiana przepisów dotyczących Agencji i jej funkcjonowania. Wniosek stanowi realizację takiego wariantu modernizacji Agencji, który zakłada rozszerzenie zadań ENISA poprzez włączenie organów odpowiedzialnych za egzekwowanie prawa i ochronę prywatności jako pełnoprawnych zainteresowanych stron.

Po przeprowadzonych konsultacjach społecznych w sprawie przyszłości kwestii związanych z problematyką bezpieczeństwa sieci i informacji KE zleciła wykonanie studium możliwości analizującego warianty dalszych działań wobec Agencji – dok. SEC(2010)1126, gdzie przedstawiono 5 wariantów dalszej polityki. Z punktu widzenia dalszej dyskusji najważniejsze były wariant nr 2 z mandatem dotychczasowym, wariant nr 3 przewidujący rozszerzenie zadań ENISA poprzez włączenie organów odpowiedzialnych za egzekwowanie prawa i ochronę prywatności jako pełnoprawnych zainteresowanych stron oraz wariant nr 4 zakładający dodanie do zakresu zadań Agencji funkcji w zakresie zwalczania ataków cybernetycznych i reagowania na incydenty cybernetyczne. Jakkolwiek panuje zgodność wśród państw członkowskich odnośnie do konieczności wzmocnienia agencji, kontrowersje budzi nadanie agencji nowych uprawnień, dlatego też jako projekt rozporządzenia procedowany jest wariant nr 3. Wniosek w sprawie modernizacji Agencji o sygnaturze COM(2010)521, podobnie jak wniosek w sprawie tymczasowego przedłużenia mandatu Agencji, był przedmiotem dyskusji Grupy Roboczej H5 UE ds. Telekomunikacji i Społeczeństwa Informacyjnego w dniach 13 i 20 października 2010 r., czego rezultatem było przedłożenie przez Prezydencję belgijską na posiedzeniu w dniu 3 listopada 2010 r. nowych zapisów rozporządzenia „tymczasowego" (dok. 15610/10) oraz „modernizującego" (dok. 15611/10) uwzględniającego uwagi Państw Członkowskich. Zmiany rozporządzenia „tymczasowego" mają charakter formalny związany z przedłużeniem mandatu, natomiast kilka zmian wprowadzonych do art. 2 i 3 dotyczących celów i zadań Agencji ENISA w rozporządzeniu „modernizującym" ma zaakcentować zachowawcze elementy wariantu modernizacji Agencji tj. uwzględnienie funkcjonowania w niektórych krajach silnych narodowych struktur odpowiadających za bezpieczeństwo sieci i informacji.
Możliwe są dwa scenariusze dalszych prac, a mianowicie zakończenie procedowania sprawy przez Prezydencję węgierską, bądź też procedowanie przez Prezydencję polską procesu II czytania rozporządzenia modernizującego. W pierwszym przypadku Polsce przypadłyby zadania o charakterze protokolarnym takie jak podpisanie rozporządzenia, w drugim prowadzenie negocjacji z Parlementem Europejskim ze strony Rady nad kształtem rozporządzenia. Drugi scenariusz jest bardziej prawdopodobny z uwagi na przedstawione przez państwa członkowskie zastrzeżenia, które zostały zaprezentowane przez Prezydencję belgijską w sprawozdaniu z postępów prac – dok. 16835/10 na posiedzeniu Rady UE ds. Transportu, Telekomunikacji i Energii w dniach 2-3 grudnia 2010 r. Za tym scenariuszem przemawia również zauważalne po wejściu w życiu Traktatu lizbońskiego korzystanie przez PE z rozszerzonych uprawnień.

Jak sygnalizuje sprawozdanie z postępów prac w większości państwa członkowskie sprzeciwiają się nadaniu agencji uprawnień o charakterze operacyjnym, sugerując jednocześnie przejrzyste określenie relacji agencji w stosunku do problematyki zwalczania przestępczości. Rozbieżności występują w kwestii stopnia precyzyjności definiowania zadań (duże państwa chcą konkretnego określenia zadań), elastyczności i długości mandatu (np. Grecja popiera mandat bezterminowy), roli Stałej Grupy Przedstawicieli Zainteresowanych Stron, relacji agencja – Komisja Europejska (państwa nie chcą większych uprawnień KE w procedurze wyboru dyrektora wykonawczego), niezależności członków zarządu, finansowania.

Polityka w zakresie bezpieczeństwa sieci i informacji odgrywa podstawową rolę w Europejskiej Agendzie Cyfrowej [1], flagowej inicjatywie realizowanej w ramach unijnej strategii „Europa 2020", której celem jest wykorzystanie i rozwój potencjału technologii teleinformatycznych oraz przełożenie tego potencjału na zrównoważony rozwój i innowacje. Wśród priorytetów służących rozwojowi społeczeństwa informacyjnego i otoczenia usług elektronicznych w UE znalazły się priorytety ukierunkowane na zwiększenie zaufania i poprawę bezpieczeństwa użytkowników tych usług. W związku z tym Europejska Agenda Cyfrowa wskazuje na potrzebę reformy Agencji ENISA, aby umożliwić Unii Europejskiej, państwom członkowskim i zainteresowanym stronom uzyskanie wysokiego poziomu zdolności i gotowości do zapobiegania problemom w zakresie bezpieczeństwa sieci i informacji, wykrywania ich oraz bardziej skutecznej reakcji na zaistniałe incydenty.

II. Stanowisko Rządu

Z uwagi na wzrost zagrożeń wobec użytkowników sieci publicznych Rząd Rzeczpospolitej Polskiej uznaje za zasadne inicjatywę prowadzenia przez Komisję Europejską na wysokim szczeblu polityki w zakresie bezpieczeństwa sieci i informacji za zasadną. Rząd polski popiera również intensyfikację działań wykonawczych w zakresie Europejskiej Agencji ds. Bezpieczeństwa Sieci i Informacji ukierunkowanych na jej gruntowną modernizację.
Mając na uwadze znaczenie problematyki bezpieczeństwa sieci i informacji bardzo ważne jest zapewnienie trwałości mandatu Agencji, dlatego też Rząd RP stoi na stanowisku, że mandat pięcioletni może się okazać zbyt krótki. Przyjęcie mandatu pięcioletniego oznacza, że już pod koniec trzeciego roku działalności musi być przygotowana ocena działalności agencji pod kątem jej przydatności dla procesu zwiększania poziomu świadomości i bezpieczeństwa systemów teleinformatycznych w Europie. Oznacza to, że „de facto" na działania, które są przedmiotem oceny KE zostają zaledwie dwa lata, co może być okresem zbyt krótkim dla przeprowadzenia rzetelnej oceny.
Mając na uwadze zgłaszane przez państwa członkowskie zastrzeżenia do precyzyjności zadań agencji, przedmiotem szczególnego zainteresowania Rządu RP jest art. 3 pkt. 1b oraz fakt czy ten artykuł jest podstawą prawną do ustanowienia zespołu reagowania na incydenty komputerowe (CERT) dla instytucji UE. Jeśli tak czy byłby to wówczas jeden zespół, który działałby w różnorodnym środowisku instytucji unijnych o bardzo różnej misji i niekiedy specyfice działania systemów teleinformatycznych, czy też powinna to być sieć kilku - kilkunastu zespołów dedykowanych w poszczególnych instytucjach współpracujących ze sobą w modelu podobnym do sieci współpracy krajowych czy branżowych zespołów CERT w Europie.
Rząd RP podziela zastrzeżenia niektórych państw członkowskich odnośnie do przepisów regulujących kompetencje dyrektora wykonawczego w zakresie opracowywania programu

[1] COM(2010) 245 z 19.5.2010.

pracy agencji (art. 12.pkt 2). W proponowanym rozporządzeniu dyrektor przedstawia gotowy program do akceptacji zarządu, który to zarząd odpowiada za zgodność programu z wyznaczonymi celami działania agencji. Wskazane jest, aby dyrektor wykonawczy w trakcie opracowywania programu - tak jak obecnie - konsultował się z zarządem. Zapewni to sprawność procesu i ograniczy praktyki wprowadzania istotnych zmian w fazie akceptacji lub odrzucania przygotowywanego programu.

III. Uzasadnienie stanowiska Rządu

Należy podkreślić, że wniosek w sprawie rozporządzenia COM(2010)521 ma charakter reformujący, dlatego też stanowisko Rządu uwzględnia wyniki analizy korzyści i kosztów wprowadzenia rozwiązań modernizujących Europejską Agencję ds. Bezpieczeństwa Sieci i Informacji (ENISA) w korelacji z rozwiązaniami i działaniami krajowymi dotyczącymi zapewnienia bezpieczeństwa sieci i informacji, ochrony danych osobowych, a zwłaszcza ich skuteczności z punktu widzenia porządku prawnego w kraju oraz dostępności zasobów osobowych i finansowych. W szczególności poddano analizie przedmiot działalności interesariuszy problematyki bezpieczeństwa sieci i informacji oraz problematyki cyberprzestępczości, którzy są wymienieni m.in. w projekcie „*Rządowego Programu Ochrony Cyberprzestrzeni RP na lata 2011-2016”*, sektora bankowego oraz tych objętych Narodowym Programem Ochrony Infrastruktury Krytycznej, Rządowy Zespół Zarządzania Kryzysowego oraz przedmiot działalności Rządowego Centrum Bezpieczeństwa. Wynika z niej potrzeba wyrażenia poparcia dla wzmocnionego zakresu i skuteczności działania Agencji ENISA. Popierane przez Rząd Rzeczpospolitej Polskiej zmiany dotyczące organizacji pracy Agencji ENISA tj. kwestie dotyczące długości mandatu, roli dyrektora generalnego i zarządu uwzględniają uwagi zgłaszane przez reprezentantów Polski w Radzie Zarządzającej ENISA, którymi są przedstawiciele Naukowej i Akademickiej Sieci Komputerowej (NASK) oraz Agencji Bezpieczeństwa Wewnętrznego w randze reprezentanta i zastępcy reprezentanta.

Z uwagi na fakt, że wymienione rozporządzenie może być procedowane podczas polskiej Prezydencji w Radzie ważne jest zapewnienie odpowiednich procedur organizacyjnych oraz polityki w zakresie prac nad rozporządzeniami ws. nowego mandatu działania Agencji ENISA. W tym celu Ministerstwo Spraw Wewnętrznych i Administracji, które zgodnie z przepisami prawa odpowiada za realizację zobowiązań międzynarodowych Rzeczypospolitej Polskiej w dziedzinie informatyzacji, we współpracy z instytucjami krajowymi pełniącymi istotne role w obszarze bezpieczeństwa sieci i informacji, przedstawiło propozycję w sprawie szerokiej i wąskiej grupy interesariuszy tej problematyki. Propozycja, która została zaakceptowana przez kierownictwa instytucji właściwych w sprawach ENISA tj. kierownictwa MSWiA, NASK, ABW, MI, UKE, Komendy Głównej Policji[2] oraz członków grupy ekspertów, zakłada prowadzenie bieżącej komunikacji i współpracy przy wykorzystaniu poczty elektronicznej w zakresie tej problematyki z możliwością wpisania zadań do zakresów obowiązków służbowych. Decyzje co do kształtu projektów stanowisk, instrukcji, notatek informacyjnych związanych z procesem legislacyjnym dotyczącym agencji ENISA przekazywanych do akceptacji przez Komitet Spraw Europejskich podejmuje wąska grupa 3 ekspertów z NASK, ABW i MSWiA.

Projekt stanowiska Rządu RP został przekazany do konsultacji z Krajową Izbą Gospodarczą

[2] W pracach szerokiej grupy ekspertów na zasadach obserwatora uczestniczy przedstawiciel Generalnego Inspektora Ochrony Danych Osobowych.

Elektroniki i Telekomunikacji, Polską Izbą Informatyki i Telekomunikacji, Polskim Towarzystwem Informatycznym, Naukową i Akademicką Siecią Komputerową, Polską Izbą Komunikacji Elektronicznej, fundacjami Panoptykon, Bezpieczna Cyberprzestrzeń.
Polska Izba Informatyki i Telekomunikacji oraz Naukowa i Akademicka Sieć Komputerowa nie wniosły uwag do dokumentu.
Fundacja Bezpieczna Cyberprzestrzeń pozytywnie ocenia prowadzenie i intensyfikację przez Komisję Europejską polityki w zakresie bezpieczeństwa sieci i informacji. Fundacja podziela opinię, że przewidywany 5-letni mandat dla Agencji ENISA może się okazać zbyt krótki. Sugeruje jednocześnie, że ewaluacja skuteczności działań Agencji powinna się odbywać w oparciu o z góry zdefiniowany zestaw wskaźników, podlegający okresowej ocenie i modyfikacji z uwagi na dynamikę zmian obszaru bezpieczeństwa teleinformatycznego. W kontekście potencjalnego powołania zespołu CERT dla instytucji europejskich, zdaniem fundacji powinien być to jeden zespół CERT dla wszystkich instytucji. Fundacja podkreśla również, że ważnym zadaniem zmodernizowanej Agencji ENISA jest regularna ocena stanu bezpieczeństwa sieci i informacji w Europie.
Polskie Towarzystwo Informatyczne sceptycznie oceniło proponowaną w rozporządzeniu modernizującym koncepcję rozszerzenia uprawnień Agencji ENISA. Wątpliwości PTI budzi możliwość ustanowienia przy współpracy Agencji z organami traktatowymi UE ram prawnych dla gromadzenia wiarygodnych danych o bezpieczeństwie teleinformatycznym i jego naruszeniach. Zastrzeżenia PTI budzi też brak koncentracji przyszłych działań Agencji na krajach, które są potencjalnym źródłem zagrożeń bezpieczeństwa teleinformatycznego. Ponadto pełnienie przez Agencję funkcji ośrodka wsparcia w zakresie opracowywania i realizacji polityki bezpieczeństwa sieci i informacji może prowadzić do tworzenia własnych standardów oraz praktyki konkurowania z firmami doradczymi i audytorskimi.

1. Ocena skutków prawnych

Zgodnie z prawodawstwem Unii Europejskiej rozporządzenie jest aktem normatywnym o charakterze generalnym i jest bezpośrednio stosowane, a więc staje się częścią krajowego porządku prawnego bez konieczności implementacji i wywiera natychmiastowe skutki prawne od momentu wejścia w życie na poziomie krajowym.

2. Ocena skutków społecznych

Spodziewane skutki społeczne modernizacji Agencji zostały przedstawione w ocenie skutków dotyczących wniosku w sprawie modernizacji Agencji (dokument o sygnaturze SEC(2010)1126) oraz skrótowo w przedstawionym przez Prezydencję belgijską sprawozdaniu z postępów prac na rozporządzeniami (dokument o sygnaturze 16835/10). Zgodnie z tymi ocenami Agencja ENISA obecnie najczęściej oferuje usługi dla Komisji Europejskiej i Państw Członkowskich. Kontakty z innymi interesariuszami tj. przedsiębiorstwami, obywatelami, izbami gospodarczymi i stowarzyszeniami konsumenckimi były znacznie rzadsze i raczej na zasadzie ad hoc, a sama praktyczna codzienna przydatność Agencji w obszarze bezpieczeństwa sieci i informacji ograniczona. Zgodnie z wnioskowanym wariantem modernizacji Agencja będzie mogła rozszerzyć swoją działalność w celu podniesienia świadomości wszystkich zainteresowanych stron w obszarze wyzwań związanych z bezpieczeństwem sieci i informacji. Będzie swego rodzaju „łącznikiem" pomiędzy cywilnymi ekspertami z zakresu bezpieczeństwa a organami państw członkowskich odpowiedzialnymi za walkę z cyberprzestępczością. Agencja będzie też działać jako centrum kompetencyjne w zakresie problematyki bezpieczeństwa sieci i informacji oraz będzie oferować wsparcie dla rozwoju i wdrażania polityki, w szczególności w odniesieniu do

ochrony prywatności, podpisu elektronicznego, eID i standardów informatycznych np. w obszarze zamówień publicznych. Zakłada się, że Agencja opracuje ramy badawcze dla gromadzenia danych statystycznych z obszaru bezpieczeństwa sieci i informacji.

3. Ocena skutków gospodarczych

Spodziewane skutki gospodarcze modernizacji Agencji zostały przedstawione w ocenie skutków dotyczących wniosku w sprawie modernizacji Agencji (dokument o sygnaturze SEC(2010)1126) oraz skrótowo w przedstawionym przez Prezydencję belgijską raporcie z postępów prac na rozporządzeniami (dokument o sygnaturze 16835/10).

Należy zwrócić uwagę, że jakkolwiek ENISA nie będzie prowadzić działań operacyjnych w zakresie zwalczania cyberprzestępczości, zgodnie z oczekiwaniami wnioskodawców Agencja powinna pełnić ważną rolę doradczą w budowanym na zasadzie partnertwa publiczno-prywatnego europejskim centrum ds. walki z cyberprzestępczością. Agencja będąc jednym z partnerów przedsięwzięcia mogłaby wypracować modelowe zasady współpracy, które byłyby wykorzystane jako dobra praktyka dla budowania partnerstw na poziomie państw i regionów w UE. Agencja miałaby też pełnić rolę centrum kompetencyjnego dla organizowania przez Państwa Członkowskie symulacji ataków cybernetycznych na dużą skalę w wymiarze dwustronnym i regionalnym. Pondato, zakłada się, że Agencja będzie konsultować opracowywanie skryptów i scenariuszy testowych oraz wspierać organizację takich ćwiczeń (ostatnie odbyły się w dniach 3-4 listopada 2010 r.). Przewidziane jest również pełnienie przez Agencję centrum kompetencyjnego dla tworzenia narodowych CERT-ów. Wymienione powyżej rozwiązania są bardzo korzystne dla krajów, które nie prowadzą takich działań, bądź przewidują finansowanie krajowe.

4. Ocena skutków finansowych

Spodziewane skutki finansowe modernizacji Agencji zostały przedstawione w ocenie skutków dotyczących wniosku w sprawie modernizacji Agencji (dokument o sygnaturze SEC(2010)1126).
Proponowane przepisy zwiększają obciążenia finansowe Rzeczpospolitej Polskiej wynikające z członkostwa w Unii Europejskiej w wyniku modernizacji Agencji dla okresu 1 stycznia 2012 r. – 31 grudnia 2016 r. w wysokości ok. 1 946 tys. euro za okres 5 letni (3% z ogólnej kwoty 64,892 mln), w stosunku do kosztów w wysokości ok. 1 314 tys. euro, gdyby mandat był utrzymany w takiej samej formule jak mandat dotychczasowy.

IV. Członek kierownictwa ministerstwa wiodącego upoważniony do prezentowania stanowiska Rządu

Piotr Kołodziejczyk,
Podsekretarz Stanu w Ministerstwie Spraw Wewnętrznych i Administracji
sekretariat: tel.: (22) 60 148 58 e-mail: Kolodziejczyk.Sekretariat@mswia.gov.pl