Rada
Unii Europejskiej

Bruksela, 18 grudnia 2020 r.
(OR. en)

Międzyinstytucjonalny numer referencyjny:
2020/0365 (COD)

14262/20
ADD 3

PROCIV 105	**ECOFIN 1182**
JAI 1132	**ENV 832**
COSI 258	**SAN 490**
ENFOPOL 354	**CHIMIE 69**
CT 121	**RECH 539**
COTER 120	**DENLEG 90**
ENER 512	**RELEX 1037**
TRANS 621	**HYBRID 49**
TELECOM 277	**CYBER 283**
ATO 91	**ESPACE 85**

PISMO PRZEWODNIE

Od:	Sekretarz generalna Komisji Europejskiej (podpisała dyrektor Martine DEPREZ)
Data otrzymania:	16 grudnia 2020 r.
Do:	Jeppe TRANHOLM-MIKKELSEN, sekretarz generalny Rady Unii Europejskiej
Nr dok. Kom.:	SWD(2020) 359 final
Dotyczy:	DOKUMENT ROBOCZY SŁUŻB KOMISJI - SPRAWOZDANIE ZE STRESZCZENIA OCENY SKUTKÓW - towarzyszący dokumentowi: Wniosek dotyczący DYREKTYWY PARLAMENTU EUROPEJSKIEGO I RADY w sprawie odporności podmiotów krytycznych

Delegacje otrzymują w załączeniu dokument SWD(2020) 359 final.

Zał.: SWD(2020) 359 final

KOMISJA
EUROPEJSKA

Bruksela, dnia 16.12.2020 r.
SWD(2020) 359 final

DOKUMENT ROBOCZY SŁUŻB KOMISJI

SPRAWOZDANIE ZE STRESZCZENIA OCENY SKUTKÓW

Towarzyszący dokumentowi:

Wniosek dotyczący
DYREKTYWY PARLAMENTU EUROPEJSKIEGO I RADY

w sprawie odporności podmiotów krytycznych

{COM(2020) 829 final} - {SEC(2020) 433 final} - {SWD(2020) 358 final}

Streszczenie oceny skutków

Ocena skutków dodatkowych środków zapewniających odporność infrastruktury krytycznej (pozycja programu prac Komisji na 2020 r.)

A. Zasadność działań

Dlaczego należy podjąć działania? Na czym polega problem?

Świadczenie usług kluczowych z wykorzystaniem infrastruktury krytycznej, która stanowi podstawę niezbędnych funkcji społecznych lub działalności gospodarczej w Unii, wymaga, aby usługi te były świadczone w sposób niezawodny, co oznacza, że właściwi operatorzy muszą być odporni na obecne i przewidywane w przyszłości ryzyko (takie jak zagrożenia naturalne, działania hybrydowe, terroryzm, incydenty wewnętrzne, stany zagrożenia zdrowia publicznego lub wypadki związane ze zdrowiem publicznym). Istniejące obecnie ramy europejskie nie są w pełni dostosowane ani do potrzeb, ani do przyszłych wyzwań. Pomimo dyrektywy w sprawie europejskiej infrastruktury krytycznej z 2008 r. oraz wprowadzonych od tego czasu innych środków na szczeblu unijnym i krajowym operatorzy nie zawsze są odpowiednio przygotowani, aby zmierzyć się z ryzykiem związanym z coraz bardziej złożonym kontekstem operacyjnym ukształtowanym między innymi przez dynamiczny krajobraz ryzyka i głębsze współzależności między sektorami. Dyrektywa w sprawie europejskiej infrastruktury krytycznej, w której skoncentrowano się bardziej na ochronie składników infrastruktury niż na odporności operatorów, dotyczy niewielkiej części europejskiej infrastruktury krytycznej o zidentyfikowanych skutkach transgranicznych w dwóch sektorach (energetycznym i transportowym). Ponadto na szczeblu krajowym występują rozbieżne podejścia i niedociągnięcia dotyczące zasięgu sektorowego, kryteriów, oceny ryzyka, wymiany informacji itp. Przeszkadza to w prawidłowym funkcjonowaniu rynku wewnętrznego i znacząco ogranicza zdolność operatorów do świadczenia przedmiotowych usług na terenie całej Unii w sposób niezawodny i niezakłócony bezzasadnymi restrykcjami.

Jaki jest cel inicjatywy?

Celem ogólnym inicjatywy jest zapewnienie nieprzerwanego świadczenia usług kluczowych na rynku wewnętrznym dzięki zwiększeniu odporności operatorów infrastruktury krytycznej (określonych we wniosku jako „podmioty krytyczne") w państwach członkowskich. Osiągnięcie tego celu ogólnego zapewni realizacja następujących celów szczegółowych:

- zapewnienie lepszego zrozumienia ryzyka i współzależności oraz środków pozwalających na zmierzenie się z nimi;
- zapewnienie, aby organy państw członkowskich określiły jako krytyczne wszystkie odpowiednie podmioty we wszystkich głównych sektorach;
- zapewnienie, aby zarówno polityka publiczna, jak i praktyka operacyjna uwzględniały szeroką gamę działań zwiększających odporność; oraz
- zwiększenie zdolności oraz poprawa współpracy i komunikacji między zainteresowanymi stronami.

Na czym polega wartość dodana podjęcia działań na poziomie UE?

Interwencja UE jest uzasadniona ze względu na wspólny charakter wielu rodzajów ryzyka, na które są narażeni operatorzy infrastruktury krytycznej w Europie, którzy są w coraz większym stopniu współzależni między sobą, a także na zróżnicowanie przepisów krajowych w tej dziedzinie, co ogranicza zdolność operatorów do świadczenia swoich usług na rynku wewnętrznym. Transnarodowy charakter świadczenia usług kluczowych oznacza, że nawet zakłócenia na szczeblu lokalnym mogą mieć dalekosiężne skutki europejskie, i nie można racjonalnie oczekiwać, iż same działania krajowe będą w stanie je zminimalizować. Dzięki spójnemu ogólnounijnemu podejściu do zarządzania ryzykiem, obejmującemu wszystkie zagrożenia w tej dziedzinie, wszyscy właściwi operatorzy wprowadziliby odpowiednie środki zwiększające odporność. To z kolei zapewniłoby większą niezawodność świadczenia usług kluczowych, ale przyczyniłoby się również do stworzenia równiejszych warunków działania na rynku wewnętrznym.

B. Rozwiązania

Jakie warianty legislacyjne i nielegislacyjne rozważono? Czy wskazano preferowany wariant? Jak

uzasadniono ten wybór lub jego brak?

Rozważono cztery warianty strategiczne:

Wariant strategiczny 1 przewiduje dobrowolne środki o charakterze nielegislacyjnym, które mają zachęcać do stosowania bardziej spójnego podejścia i wymiany informacji, jako uzupełnienie obowiązującej dyrektywy w sprawie europejskiej infrastruktury krytycznej.

Wariant strategiczny 2 wiąże się z rewizją obowiązującej dyrektywy w sprawie europejskiej infrastruktury krytycznej w celu dostosowania jej zasięgu sektorowego do zasięgu obowiązującej dyrektywy w sprawie bezpieczeństwa sieci i informacji oraz w celu uściślenia kryteriów wyboru i wymogów dotyczących operatorów europejskiej infrastruktury krytycznej, np. utrzymania planów odporności operatorów. Zarówno państwa członkowskie, jak i wyznaczeni operatorzy europejskiej infrastruktury krytycznej mieliby również obowiązek przeprowadzania ocen ryzyka.

Wariant strategiczny 3 zakłada natomiast zastąpienie obowiązującej dyrektywy w sprawie europejskiej infrastruktury krytycznej nadrzędnym ramowym instrumentem prawnym w celu zwiększenia odporności podmiotów krytycznych co najmniej w sektorach objętych obowiązującą dyrektywą w sprawie bezpieczeństwa sieci i informacji oraz poprawy funkcjonowania rynku wewnętrznego w tym zakresie. Wsparciem we wdrażaniu tego wariantu byłoby centrum wiedzy w strukturach Komisji. Państwa członkowskie miałyby obowiązek określenia, na podstawie oceny ryzyka, podmiotów krytycznych, które byłyby objęte różnymi wymogami dotyczącymi zwiększania odporności. Zarówno państwa członkowskie, jak i podmioty krytyczne miałyby obowiązek przeprowadzania ocen ryzyka. Wariant ten obejmowałby również procedurę wskazywania podmiotów krytycznych o szczególnym znaczeniu europejskim oraz niektóre przepisy szczególne mające zastosowanie do tych podmiotów.

Wariant strategiczny 4 obejmuje wszystkie elementy określone w wariancie 3. Ponadto Komisja odgrywałaby aktywniejszą rolę w wyznaczaniu podmiotów krytycznych i utworzona zostałaby unijna agencja ds. odporności infrastruktury krytycznej.

Po uwzględnieniu przewidywanych skutków oraz wartości każdego wariantu preferowanym wariantem jest wariant 3, który zapewniłby bardziej kompleksowe ramy odporności uwzględniające istniejące środki unijne i specyfikę krajową.

Jak kształtuje się poparcie dla poszczególnych wariantów?

Ograniczona liczba państw członkowskich i operatorów stwierdziła, że obecne ramy są wystarczające, i opowiedziała się za dobrowolnymi środkami przewidzianymi w wariancie 1. Jeżeli chodzi o wariant 2, jedno państwo członkowskie opowiedziało się za zachowaniem obecnego kształtu europejskiej infrastruktury krytycznej, natomiast inne państwa były za przeglądem koncepcji europejskiej infrastruktury krytycznej, tak aby obejmowała ona infrastrukturę o wyraźnym wymiarze ogólnoeuropejskim. Większość państw członkowskich wybrała wariant 3. Operatorzy poparli przede wszystkim warianty 2 i 3. Wariant 4 był najmniej preferowanym wariantem ze wszystkich zarówno wśród państw członkowskich, jak i wśród operatorów; wariant ten uznano za zbyt inwazyjny i nieelastyczny, tj. niepozwalający na uwzględnienie specyfiki sektorów.

C. Skutki wdrożenia preferowanego wariantu

Jakie korzyści przyniesie wdrożenie preferowanych wariantów lub – jeśli ich nie wskazano – głównych wariantów?

Biorąc pod uwagę istotną rolę, jaką usługi kluczowe odgrywają w życiu obywateli UE i w unijnej gospodarce, większa odporność operatorów przyniosłaby korzyści podmiotom we wszystkich sektorach gospodarki, w tym małym, średnim i dużym przedsiębiorstwom. Podejmowane na szczeblu UE starania na rzecz zapewnienia nieprzerwanego świadczenia usług kluczowych – poza tym, że mają pozytywny wpływ na poszczególne przedsiębiorstwa – pomogłyby również zwiększyć ogólną stabilność gospodarczą i jeszcze bardziej poprawić atrakcyjność rynku UE dla inwestorów.

Poza skutkami gospodarczymi środki zwiększające odporność przewidziane w wariancie 3 ograniczyłyby zakłócenia i zapewniłyby obywatelom UE bezpieczniejsze warunki pracy oraz wyższą jakość życia i zdrowia. Wraz ze wzrostem niezawodności świadczenia usług kluczowych zwiększa się bowiem prawdopodobieństwo

wystąpienia pozytywnych skutków gospodarczych, społecznych, edukacyjnych, zawodowych i rekreacyjnych w życiu obywateli. Ponadto dodatkowe starania na rzecz ograniczenia częstotliwości i wagi zakłóceń świadczenia usług kluczowych miałyby również pozytywny wpływ na środowisko, ponieważ zagwarantowałyby bardziej efektywne wykorzystanie zasobów, a także bardziej zrównoważone wzory konsumpcji i produkcji w UE.

Jakie są koszty wdrożenia preferowanych wariantów lub – jeśli ich nie wskazano – głównych wariantów?

Główne koszty dla państw członkowskich byłyby związane z opracowaniem strategii krajowych, przeprowadzaniem ocen ryzyka oraz wskazywaniem podmiotów krytycznych, a także nadzorem i egzekwowaniem. Właściwe organy mogłyby jednak wykorzystać w tym celu istniejące polityki i procesy – w tym dokumenty dotyczące strategii, ustalenia dotyczące oceny ryzyka oraz procedury wyznaczania przewidziane w dyrektywie w sprawie bezpieczeństwa sieci i informacji – jako podstawę wspierającą wdrażanie, ograniczając tym samym ogólne koszty. Natomiast koszty bezpośrednie ponoszone przez wskazane podmioty krytyczne byłyby związane z przeprowadzeniem ocen ryzyka na poziomie operatora – w razie potrzeby lub jeśli nie są jeszcze prowadzone – z wprowadzeniem odpowiednich środków organizacyjnych lub technicznych mających na celu zwiększenie odporności operatorów, a także ze zgłaszaniem incydentów właściwym organom.

Jakie będą skutki dla przedsiębiorstw, MŚP i mikroprzedsiębiorstw?

Oczekuje się, że spośród operatorów, których dotyczą poszczególne warianty, liczba MŚP, na które warianty te miałyby wpływ, będzie niewielka. Chociaż w sektorach takich jak transport, energia lub woda podmiotami, które zostaną prawdopodobnie wyznaczone na podmioty krytyczne, są zwykle średnie lub duże przedsiębiorstwa zatrudniające tysiące pracowników, w innych sektorach podmioty krytyczne mogą być mniejsze. Na przykład można przyjąć, że w sektorze zdrowia MŚP mogą świadczyć konkretne, zaawansowane technicznie lub specjalistyczne usługi. MŚP znajdujące się w takiej sytuacji prawdopodobnie zachęca się jednak do zapewnienia wysokiego poziomu odporności we własnym zakresie lub są one objęte szczególnymi wymogami na szczeblu krajowym lub unijnym, co zmniejsza dodatkowe koszty związane z preferowanym wariantem.

Czy przewiduje się znaczące skutki dla budżetów i administracji krajowych?

Przewiduje się pewne skutki dla właściwych organów państw członkowskich wynikające z konkretnych zobowiązań, np. regularnych ocen ryzyka na szczeblu krajowym, strategii krajowych oraz działań nadzorczych i środków egzekucyjnych. Ponadto z pewnymi kosztami wiązałaby się potrzeba zapewnienia dodatkowego wsparcia operatorom wskazanym jako podmioty krytyczne w wypełnianiu zobowiązań wynikających z prawodawstwa.

Czy wystąpią inne znaczące skutki?

Nie dotyczy

D. Działania następcze

Kiedy nastąpi przegląd przyjętej polityki?

Ocena skutków aktu ustawodawczego zostanie przeprowadzona cztery lata po upływie terminu na wdrożenie tego aktu, aby zapewnić wystarczająco długi okres na ocenę skutków inicjatywy po jej pełnym wdrożeniu we wszystkich państwach członkowskich.