IX kadencja

SEJM RZECZYPOSPOLITEJ POLSKIEJ

KANCELARIA SEJMU
Biuro Komisji Sejmowych

PEŁNY ZAPIS PRZEBIEGU POSIEDZENIA

■ **Komisji do Spraw Unii Europejskiej (nr 233)**

z dnia 7 lipca 2023 r.

Pełny zapis przebiegu posiedzenia

Komisji do Spraw Unii Europejskiej (nr 233)

7 lipca 2023 r.

Komisja do Spraw Unii Europejskiej, obradująca pod przewodnictwem posła **Kacpra Płażyńskiego (PiS)**, przewodniczącego Komisji, rozpatrzyła:

I. informację o dokumentach, w stosunku do których prezydium wnosi o niezgłaszanie uwag: COM(2022) 459, COM(2023) 229 (art. 7 ust. 4 ustawy z dnia 8 października 2010 r. o współpracy Rady Ministrów z Sejmem i Senatem w sprawach związanych z członkostwem Rzeczypospolitej Polskiej w Unii Europejskiej), COM(2023) 292, 316, 321, 322 (art. 8 ust. 2 ustawy z dnia 8 października 2010 r.), JOIN(2023) 17, COM(2023) 293, 294, 295, 298, 299, 301, 304, 308, 309, 311 (art. 151 ust. 1 regulaminu Sejmu z uwzględnieniem art. 3 ust. 2 ustawy z dnia 8 października 2010 r.),

II. w trybie art. 7 ust. 4 ustawy z dnia 8 października 2010 r. Wniosek dotyczący rozporządzenia Parlamentu Europejskiego i Rady zmieniającego rozporządzenie (UE) 2019/881 w odniesieniu do usług zarządzanych w zakresie bezpieczeństwa (COM(2023) 208 wersja ostateczna) i odnoszący się do niego projekt stanowiska RP,

III. w trybie art. 7 ust. 4 ustawy z dnia 8 października 2010 r. Wniosek dotyczący rozporządzenia Parlamentu Europejskiego i Rady w sprawie ustanowienia środków mających na celu zwiększenie solidarności i zdolności w Unii w zakresie wykrywania zagrożeń cyberbezpieczeństwa i incydentów w cyberbezpieczeństwie oraz przygotowywania się i reagowania na takie zagrożenia i incydenty (COM(2023) 209 wersja ostateczna) i odnoszący się do niego projekt stanowiska RP,

IV. w trybie art. 7 ust. 4 ustawy z dnia 8 października 2010 r. Wniosek dotyczący rozporządzenia Parlamentu Europejskiego i Rady zmieniające rozporządzenie (WE) nr 561/2006 w odniesieniu do minimalnych wymogów dotyczących minimalnych przerw oraz dziennego i tygodniowego okresu odpoczynku w sektorze okazjonalnego przewozu osób (COM(2023) 256 wersja ostateczna) i odnoszący się do niego projekt stanowiska RP.

W posiedzeniu udział wzięli: **Rafał Weber** sekretarz stanu w Ministerstwie Infrastruktury wraz ze współpracownikami, **Paweł Lewandowski** podsekretarz stanu w Ministerstwie Cyfryzacji wraz ze współpracownikami.

W posiedzeniu udział wzięli pracownicy Kancelarii Sejmu: **Agata Jackiewicz**, **Joanna Heger** – z sekretariatu Komisji w Biurze Spraw Międzynarodowych; **Marek Jaśkowski** – ekspert ds. legislacji z Biura Analiz Sejmowych, **Kamilla Kurczewska** – specjalista ds. systemu gospodarczego z BAS.

Przewodniczący poseł Kacper Płażyński (PiS):

Dzień dobry. Otwieram posiedzenie Komisji do Spraw Unii Europejskiej. Uwag do porządku dziennego nie słyszę. Zaczynamy od pkt I. Informacja o dokumentach, w stosunku do których prezydium wnosi o niezgłaszanie uwag. Są to następujące dokumenty: w trybie art. 7 ust. 4 ustawy z dnia 8 października 2010 r. o współpracy Rady Ministrów z Sejmem i Senatem w sprawach związanych z członkostwem Rzeczypospolitej Polskiej w Unii Europejskiej COM(2022) 459, COM(2023) 229, w trybie art. 8 ust. 2 ustawy z dnia 8 października 2010 r.COM(2023) 292, 316, 321, 322, w trybie art. 151 ust. 1 regulaminu Sejmu z uwzględnieniem art. 3 ust. 2 ustawy z dnia 8 października 2010 r. JOIN(2023) 17, COM(2023) 293, 294, 295, 298, 299, 301, 304, 308, 309, 311. Czy do wymienionych przeze mnie dokumentów państwo zgłaszają uwagi? Nie słyszę. W związku z tym stwierdzam, że **Komisja postanowiła nie zgłaszać uwag do tych dokumentów**.

Pkt II – rozpatrzenie w trybie art. 7 ust. 4 ustawy z dnia 8 października 2010 r. Wniosku dotyczącego rozporządzenia Parlamentu Europejskiego i Rady zmieniającego rozporządzenie (UE) 2019/881 w odniesieniu do usług zarządzanych w zakresie bezpieczeństwa (COM(2023) 208 wersja ostateczna) i odnoszącego się do niego projektu stanowiska RP. Rząd reprezentuje pan minister Paweł Lewandowski. Bardzo proszę.

Podsekretarz stanu w Ministerstwie Cyfryzacji Paweł Lewandowski:

Nie usłyszałem, że zostałem wywołany, przepraszam. Szanowni państwo, Wysoka Komisjo, panie przewodniczący, na początku chciałbym przedstawić podstawowe informacje na temat rozporządzenia PE i Rady, o którym mówimy, oraz certyfikat cyberbezpieczeństwa w zakresie technologii informacyjno-komunikacyjnych, oraz uchylenia rozporządzenia UE, zwanego dalej aktem o cyberbezpieczeństwie. Ten akt prawny powołał do życia ENISA – Agencję UE do spraw Cyberbezpieczeństwa oraz ustanowił ramy weryfikacji cyberbezpieczeństwa w Europie. Zgodnie z tymi przepisami przewidziane jest stworzenie programów certyfikacji cyberbepieczeństwa dotyczących produktów, usług lub procesów ICT. Certyfikacja ma być dobrowolna, ale w innych aktach prawa europejskiego. Na przykład w dyrektywie NIS 2 wskazano, że Komisja Europejska lub państwa członkowskie będą mogły wprowadzić obowiązek certyfikacji.

Obecna propozycja dąży do rozszerzenia zakresu europejskich ram certyfikacji o usługi zarządzania w zakresie bezpieczeństwa. Jej przyjęcie umożliwi Komisji przygotowanie europejskiego programu certyfikacji cybezpieczeństwa dla tych usług. W ocenie Komisji będzie to służyło rozwijaniu branży zaufanych usług w zakresie cyberbezpieczeństwa oraz pozwoli uniknąć rozdrobnienia rynku w tym zakresie. Regulacja ta jest powiązana z projektem aktu w sprawie cybersolidarności, który ustanawia cyberrezerwę, w ramach której zaufani dostawcy mają świadczyć usługi posiadające certyfikaty cyberbezpieczeństwa, o których mowa w akcie o cyberbezpieczeństwie.

Przedstawiona przez Komisję propozycja zmian przepisów budzi jednak bardzo duże wątpliwości, co sprawia, że trudno spodziewać się, by zostały osiągnięte cele wskazane przez Komisję. Zakres usług, które Komisja chce objąć europejskimi programami certyfikacji bezpieczeństwa, budzi wątpliwości. Zgodnie z definicją ma to być usługa polegająca na prowadzeniu lub wspomaganiu działań związanych z zarządzaniem ryzykiem w cyberprzestrzeni, takich jak reagowanie na incydenty, testy penetracyjne, audyty bezpieczeństwa i doradztwo.

Powyższe sformułowanie nie pozwala stwierdzić, czy w zakresie wyżej wymienionych usług znajdują się również zagadnienia związane z fizycznym bezpieczeństwem obiektów i urządzeń. Należy podkreślić, że bezpieczeństwo fizyczne i cyberbezpieczeństwo nie mogą być od siebie odseparowane. Zasady fizycznego dostępu do określonych pomieszczeń i urządzeń mają bezpośredni wpływ na bezpieczeństwo systemów teleinformatycznych i przetwarzanych w nich danych. Należy podkreślić, że takie podejście wynika między innymi z międzynarodowych norm, takich jak norma ISO 27001, która obejmuje między innymi kwestie związane z ochroną okablowania, przystosowanych fizycznych zabezpieczeń. Rozstrzygnięcie tej kwestii jest kluczowe dla zaproponowanych

zmian. W naszej ocenie nie można poprzeć regulacji, która budzi tak istotną wątpliwość w tej podstawowej sprawie.

Podsumowując, rozszerzenie zakresu europejskich ram cyberbezpieczeństwa, zanim zaczęły w ogóle funkcjonować w praktyce, jest przedwczesne. Działania Komisji Europejskiej powinny się skupić na zakończeniu prac nad obecnie procesowanymi programami certyfikacji. Wprowadzone zmiany, które mają oddziaływać na rynek, powinny być poprzedzone analizą tego rynku i wpływu na niego. Inne podejście prowadzi do utraty zaufania do UE i państw członkowskich i zniechęca do inwestycji w UE. Uważamy także, że zakres wprowadzonych zmian jest niejasny, przez co zmiany mogą nie wpływać pozytywnie na cyberbezpieczeństwo. W związku z powyższym w ocenie rządu nie można poprzeć w takim kształcie proponowanych zmian. Dziękuję bardzo.

Przewodniczący poseł Kacper Płażyński (PiS):

Panie ministrze, chciałbym się upewnić, który punkt pan referuje.

Podsekretarz stanu w MC Paweł Lewandowski:

Stanowisko rządu do projektu rozporządzenia Parlamentu Europejskiego i Rady zmieniającego rozporządzenie w odniesieniu do usług zarządzanych w zakresie bezpieczeństwa.

Przewodniczący poseł Kacper Płażyński (PiS):

Aha. Dobrze. Bo zakres pana wypowiedzi brzmi jak pkt III, ale w takim razie wszystko się zgadza. Posłem sprawozdawcą jest pan poseł Grzegorz Woźniak.

Poseł Grzegorz Woźniak (PiS):

Dziękuję, panie przewodniczący. Wysoka Komisjo, panie ministrze, tu pan przewodniczący dobrze zauważył, ponieważ ja też, analizując oba dokumenty, stwierdziłem, że są bardzo zbieżne. Ale po kolei. Najpierw przedstawię opinię do tego punktu, który teraz omawiamy, czyli wniosku dotyczącego rozporządzenia Parlamentu Europejskiego i Rady zmieniającego rozporządzenie UE z 2019/881 w odniesieniu do usług zarządzanych w zakresie bezpieczeństwa. To jest dokument COM 208. Przedmiotem tego projektu przedstawionego jest wprowadzenie ograniczonej i ukierunkowanej zmiany służącej rozszerzeniu zakresu europejskich ram certyfikacji bezpieczeństwa o usługi zarządzane w zakresie bezpieczeństwa. Usługami zarządzanymi w zakresie bezpieczeństwa są między innymi usługi polegające na prowadzeniu i wspomaganiu działań związanych z zarządzaniem ryzykiem w cyberprzestrzeni, takie jak reagowanie na incydenty, różnego rodzaju testy penetracyjne, audyty bezpieczeństwa i doradztwo.

Projektowana zmiana ma na celu poprawę jakości usług zarządzanych w zakresie bezpieczeństwa, zwiększenie ich porównywalności oraz ułatwienie dochowania szczególnej staranności przy wyborze dostawcy usług w zakresie bezpieczeństwa i zgodnie z wymogami dyrektywy z 2022 nr 2555.

Dnia 27 czerwca 2019 r. weszło w życie rozporządzenie nr 2019/881 obowiązujące wszystkie państwa członkowskie, w tym Polskę. Jednym z priorytetów tej regulacji było wprowadzenie jednolitych programów certyfikacji na obszarze całej UE oraz zapewnienie wsparcia państwom członkowskim w tym zakresie.

Projektowana zmiana według projektodawców w tym dokumencie 208 ma za zadanie umożliwienie zniesienia barier na rynku cyfrowym w kolejnym obszarze usług cyfrowych. Dzięki ujednoliceniu i podziałowi certyfikatów na trzy poziomy: wysoki, istotny i podstawowy, uważa się, że przedsiębiorcy będą mogli dobrać certyfikat do swoich indywidualnych potrzeb, możliwości szybkiego wyboru właściwego poziomu, zapewni im oszczędność czasu i środków przeznaczonych na certyfikację.

Ujednolicone ramy certyfikacji i poziomy certyfikatu zwiększą zaufanie konsumentów, którzy będą mogli wybierać rozwiązania spełniające odpowiednie normy bezpieczeństwa oraz przyniosą korzyści dla przedsiębiorców, ograniczając koszty i czas związany z uzyskaniem certyfikatów w każdym kraju osobno i dając pewność, że uzyskane przez nich certyfikaty będą uznane w każdym państwie należącym do UE. Tak zakłada ten projekt.

Z kolei przedsiębiorcy, którzy będą chcieli oferować usługi certyfikacji w zakresie bezpieczeństwa lub usługi zarządzane w zakresie bezpieczeństwa, będą mogli kierować swoją ofertę do klientów z innych państw z gwarancją uznania wystawionych przez nich dokumentów. Przedmiotem tego projektu jest wprowadzenie ograniczonej i ukierunkowanej zmiany służącej rozszerzeniu zakresu europejskich ram certyfikacji bezpieczeństwa, usługi zarządzane w zakresie bezpieczeństwa. Może tyle na temat projektu.

Stanowisko rządu było parę minut przed Komisją, więc już nie będę go odczytywał. Dostałem od pań z sekretariatu, bo dosyć późno przyszło, ale pan minister przedstawił, więc może już nie będę się powtarzał w tej materii. Dziękuję bardzo.

Przewodniczący poseł Kacper Płażyński (PiS):

Dziękuję. Otwieram dyskusję. Czy ktoś z państwa chciałby zabrać głos? Nie słyszę głosów w dyskusji, w związku z czym proponuję przyjąć konkluzję. Stwierdzam, że **Komisja przyjęła w trybie art. 7 ust. 4 ustawy z dnia 8 października 2010 r. dokument o sygnaturze COM(2023) 208 wersja ostateczna i odnoszący się do niego projekt stanowiska rządu. Komisja podzieliła stanowisko rządu.** Sprzeciwu nie słyszę.

Przechodzimy do pkt III, czyli rozpatrzenia w trybie art. 7 ust. 4 ustawy z dnia 8 października 2010 r. Wniosku dotyczącego rozporządzenia Parlamentu Europejskiego i Rady w sprawie ustanowienia środków mających na celu zwiększenie solidarności i zdolności w Unii w zakresie wykrywania zagrożeń cyberbezpieczeństwa i incydentów w cyberbezpieczeństwie oraz przygotowywania się i reagowania na takie zagrożenia i incydenty (COM(2023) 209 wersja ostateczna) i odnoszącego się do niego projektu stanowiska RP. Tutaj również pan minister Paweł Lewandowski przedstawi stanowisko.

Podsekretarz stanu w MC Paweł Lewandowski:

Dziękuję bardzo. Chciałem się tylko upewnić, że to stanowisko wpłynęło do Komisji? Pewnie też w ostatniej chwili. Ono jest dosyć szczegółowe. Pozwolę sobie ogólnie je omówić. Jeśli będą szczegółowe pytania do poszczególnych kwestii, to oczywiście jestem otwarty.

Przewodniczący poseł Kacper Płażyński (PiS):

O co chodzi z tą solidarnością? Bo to ostatnio takie modne pojęcie.

Podsekretarz stanu w MC Paweł Lewandowski:

Nie o to samo, co jest w narracji prowadzonej obecnie w mediach w innych kwestiach, którymi, jak rozumiem, Komisja jest zainteresowana. Przejdę do naszego cyberbezpieczeństwa. Tutaj akurat wydaje się, że stanowisko większości państw co do strategicznych aspektów w zakresie cyberbezpieczeństwa jest podobne. Nie stwierdzamy istotnych problemów.

Przechodząc wprost do stanowiska, celem omawianego projektu rozporządzenia jest zwiększenie solidarności i zdolności w zakresie wykrywania zagrożeń cyberbezpieczeństwa i incydentów w cyberbezpieczeństwie oraz przygotowania się i reagowania na takie zagrożenia i incydenty. Celem jest wzmocnienie bezpieczeństwa technologii cyfrowych, które są narażone na incydenty oraz przeciwdziałanie ich potencjalnym skutkom. Ważnym aspektem rozporządzenia jest transgraniczność. Państwa członkowskie są narażone na coraz większe ryzyko, w szczególności szybko rozprzestrzeniających się cyberataków transgranicznych, mogących wpłynąć na kilka państw członkowskich lub nawet całą UE. Osiągnięcie tych celów ma być zrealizowane w ramach rozporządzenia przez wprowadzenie ogólnoeuropejskiej infrastruktury, czyli Europejskiej Tarczy Cyberbezpieczeństwa w celu zbudowania i wzmocnienia wspólnych zdolności w zakresie wykrywania i orientacji sytuacyjnej.

Kolejnym celem jest stworzenie mechanizmu cyberkryzysowego, aby wesprzeć państwa członkowskie w przygotowaniu się na poważne incydenty w cyberbezpieczeństwie, incydenty również na dużą skalę w reagowaniu na nie i natychmiastowym usuwaniu ich skutków. Wsparcie w reagowaniu na incydenty udostępnia się również europejskim instytucjom, organom, urzędom i agencjom UE. Kolejnym celem jest ustanowienie euro-

pejskiego mechanizmu przeglądu incydentów w cyberbezpieczeństwie na potrzeby przeglądu i oceny konkretnych poważnych incydentów lub incydentów na dużą skalę.

Tu jest cały szereg bardzo szczegółowych kwestii. Przejdę tylko do ogólnej oceny. Rząd polski widzi potrzebę wzmacniania solidarności między państwami członkowskimi, jednak w tym celu nie jest konieczne przyjęcie kolejnej regulacji, która w większości duplikuje już funkcjonujące rozwiązania prawne. Kluczowe jest, aby nie doprowadzić do fragmentacji ram cyberbezpieczeństwa na poziomie UE oraz duplikowania zadań. Ważne jest ustalenie spójnej wizji działań w obszarze cyberbezpieczeństwa i konsekwentna ich realizacja. Temu służyć ma przygotowana przez prezydencję czeską mapa drogowa, która powinna być w pełni uwzględniona przez Komisję Europejską, co nie wydaje się mieć obecnie miejsca. Brak oceny wpływu przeprowadzonej przez Komisję Europejską regulacji zasadniczo ogranicza możliwość oceny jej na poziomie krajowym w kontekście współpracy w zakresie cyberbezpieczeństwa oraz realizacji projektów z programu „Cyfrowa Europa".

Mając na względzie powyższe, rząd polski będzie dążył do uzyskania wszelkich możliwych wyjaśnień, a także do zmiany kształtu proponowanej regulacji w taki sposób, by była ona komplementarna z już przyjętymi regulacjami w zakresie cyberbezpieczeństwa, w szczególności z dyrektywą NIS 2. Czyli, mówiąc w skrócie, to jest kolejny objaw tsunami legislacyjnego UE. Zanim dobrze wdrożymy jedne dyrektywy, zanim pozwolimy im zasadniczo działać, to są tworzone kolejne rozwiązania, mam wrażenie, bez oglądania się tak naprawdę na to, co obecnie funkcjonuje. Zresztą poprzednia dyrektywa, poprzedni akt prawny, który omawialiśmy w poprzednim punkcie, to jest dokładnie taki sam przykład duplikowania, nakładania się, wprowadzenia chaosu w regulacjach unijnych w tym zakresie, czego my nie potrzebujemy, bo w gruncie rzeczy tak naprawdę wszyscy mniej więcej wiedzą, co mają robić, bo standardy są znane. Dziękuję bardzo.

Przewodniczący poseł Kacper Płażyński (PiS):

Dziękuję, panie ministrze. Posłem sprawozdawcą jest tu również pan poseł Woźniak.

Poseł Grzegorz Woźniak (PiS):

Dziękuję bardzo, panie przewodniczący. Panie ministrze, znowu wracamy do cyberbezpieczeństwa i te tematy przy tym i przy 208 COM-ie są podobne. Może nie to, że się nakładają, ale dotyczą podobnych kwestii. Teraz przedstawię opinię na temat wniosku dotyczącego rozporządzenia PE i Rady w sprawie środków mających na celu zwiększenie solidarności i zdolności w Unii w zakresie wykrywania zagrożeń cyberbezpieczeństwa i incydentów w cyberbezpieczeństwie oraz przygotowywania się i reagowania na takie zagrożenia i incydenty COM(2023) 209. Celem projektu jest zwiększenie solidarności na szczeblu unijnym, o czym przed chwilą pan minister mówił, przez wzmocnienie możliwości wspólnego wykrywania cyberzagrożeń i cyberincydentów oraz poprawę orientacji sytuacji w tej dziedzinie, jak również zwiększenie gotowości podmiotów działających w sektorach krytycznych związanych z cyberbezpieczeństwem w UE, oraz zwiększenie odporności i ustalenie adekwatnych wzorców reakcji na tego typu zagrożenia, jeżeli one by się pojawiły. Czyli powinny być podobne.

Projektowane rozporządzenie ustanawia środki mające na celu zwiększenie zdolności w UE w zakresie wykrywania i reagowania na zagrożenia cyberbezpieczeństwa poprzez organizowanie europejskiej infrastruktury centrów monitorowania bezpieczeństwa, stworzenie mechanizmu cyberkryzysowego, aby pomóc państwom członkowskim w przygotowaniu się na tego typu incydenty związane z atakami hakerskimi, w tym incydenty w cyberbezpieczeństwie na dużą skalę. Również ustalenie europejskiego mechanizmu przeglądu incydentów w cyberbezpieczeństwie na potrzeby oceny poważnych incydentów lub incydentów na duża skalę.

Projektowany akt wprowadza regulacje organizacyjne pozwalające wykorzystać wspólny potencjał wszystkich państw członkowskich. Tak jak było przy COM 208, podobnie i tutaj – tak żeby były podobne standardy. Projektowane rozporządzenie wdraża przyjętą w grudniu 2020 r. unijną strategię cyberbezpieczeństwa, w której zapowiedziano utworzenie europejskiej tarczy cyberbezpieczeństwa wzmacniającej zdolności w zakresie wykrywania cyberzagrożeń i wymiany informacji w całej UE.

W polskim systemie prawnym podstawowe regulacje dotyczące zapewnienia bezpieczeństwa w cyberprzestrzeni zostały zawarte w ustawie o krajowym systemie cyberbezpieczeństwa oraz w rozporządzeniach wykonawczych do tej ustawy.

Projektowane rozwiązania organizacyjne w COM 209 przyczynią się według projektodawców do zwiększenia zdolności na poziomie UE, do wymiany informacji, gromadzenia analizy danych dotyczących zagrożeń cyberbezpieczeństwa, incydentów w cyberbepieczeństwie oraz pozwolą uniknąć powielania działań w UE i państwach członkowskich. Rozporządzenie ustanawia środki mające na celu zwiększenie zdolności w UE w zakresie wykrywania i reagowania na zagrożenia i incydenty w cyberbezpieczeństwie.

Co do stanowiska rządu, to również otrzymaliśmy je przed Komisją. Pan minister mówił o tym, o powielaniu i o kwestiach, które należy wyjaśnić, zanim miałoby się taki dokument rozpatrywać. Dziękuję bardzo.

Przewodniczący poseł Kacper Płażyński (PiS):

Dziękuję. Otwieram dyskusję. Czy ktoś chciałby zabrać głos w dyskusji? Nie słyszę. Proponuje konkluzję. Stwierdzam, że **Komisja rozpatrzyła w trybie art. 7 ust. 4 ustawy z dnia 8 października 2010 r. dokument o sygnaturze COM(2023) 209 wersja ostateczna i odnoszący się do niego projekt stanowiska rządu. Komisja podzieliła stanowisko rządu.** Dziękuję. Dziękuję, panie ministrze.

Przechodzimy do pkt IV, czyli rozpatrzenia w trybie art. 7 ust. 4 ustawy z dnia 8 października 2010 r. Wniosku dotyczącego rozporządzenia Parlamentu Europejskiego i Rady zmieniające rozporządzenie (WE) nr 561/2006 w odniesieniu do minimalnych wymogów dotyczących minimalnych przerw oraz dziennego i tygodniowego okresu odpoczynku w sektorze okazjonalnego przewozu osób (COM(2023) 256 wersja ostateczna) i odnoszącego się do niego projektu stanowiska RP. Rząd reprezentuje pan minister Rafał Weber. Bardzo proszę, panie ministrze.

Sekretarz stanu w Ministerstwie Infrastruktury Rafał Weber:

Dziękuję bardzo, panie przewodniczący. Wysoka Komisjo, szanowni państwo, przedmiotowy wniosek Komisji dotyczy rewizji rozporządzenia (WE) o numerze 561/2006. W rozporządzeniu tym określono minimalny dzienny i tygodniowy czas prowadzenia pojazdu, minimalne długości przerw oraz minimalny dzienny i tygodniowy okres odpoczynku kierowców w sektorze transportu drogowego.

Regulacja ta obejmuje dwie grupy kierowców. Pierwsza grupa – wykonujących przewóz drogowy rzeczy pojazdami, których dopuszczalna masa całkowita przekracza 3,5 tony, i druga grupa – wykonujących przewozy drogowe osób pojazdami skonstruowanymi lub trwale przystosowanymi i przeznaczonymi do przewozu więcej niż 9 osób łącznie z kierowcą.

Rozporządzenie to ma generalne zastosowanie do przewoźników drogowych i ich kierowców niezależnie od tego, czy wykonują oni przewóz drogowy osób czy rzeczy lub niezależnie od tego, czy w przypadku przewozu osób wykonują oni przewozy regularne czy okazjonalne.

Trzeba wspomnieć i mocno zaznaczyć, że sektor okazjonalnego przewozu osób charakteryzuje się jednak innymi cechami w porównaniu do przewozu rzeczy lub regularnego przewozu osób. Z tego względu, mając na uwadze, że charakterystyka pracy kierowcy wykonującego okazjonalne przewozy osób ma istotny wpływ na warunki jego pracy, niezbędne jest zatem odpowiednie dostosowanie tej specyfiki przepisów dotyczących czasu ich pracy, a w szczególności norm dotyczących obowiązkowych przerw i okresów odpoczynku.

Po przeprowadzeniu szczegółowej analizy Komisja Europejska podjęła inicjatywę legislacyjną mającą na celu: zapewnienie bardziej elastycznego rozłożenia przerw i okresów odpoczynku kierowców wykonujących okazjonalne przewozy osób oraz ustanowienie równego traktowania międzynarodowych i krajowych okazjonalnych przewozów osób. We wniosku Komisji nie wprowadzono żadnych zmian minimalnych długości przerw lub okresów odpoczynku ani maksymalnego czasu prowadzenia pojazdu.

Celem wniosku jest zatem zagwarantowanie skutecznych i wysokiej jakości okazjonalnych przewozów osób oraz poprawa warunków pracy kierowców i prowadzenie pojaz-

dów, w szczególności w celu zminimalizowania ich stresu i zmęczenia. Mając powyższe na uwadze, rząd polski pozytywnie odnosi się do proponowanych przez Komisję zmian. Podobnie jak Komisja, dostrzegamy potrzebę dostosowania przepisów rozporządzenia w odniesieniu do minimalnych wymogów dotyczących minimalnych przerw oraz dziennego i tygodniowego okresu odpoczynku w sektorze okazjonalnego przewozu osób i wyjścia naprzeciw postulatom i oczekiwaniom artykułowanym w tym zakresie również przez polskie środowisko transportowe.

W toku dalszych negocjacji i prac nad przedmiotowym wnioskiem rząd polski będzie podejmował starania mające na celu zapewnienie przewoźnikom drogowym, wykonującym okazjonalne przewozy drogowe osób, większej elastyczności i swobody w organizacji i planowaniu czasu pracy zatrudnionym kierowcom wykonującym przedmiotowe przewozy drogowe. Proszę Wysoką Komisję o przyjęcie przedmiotowej informacji. Dziękuję bardzo.

Przewodniczący poseł Kacper Płażyński (PiS):

Dziękuję, panie ministrze. Posłem sprawozdawcą jest pan poseł Krzysztof Truskolaski. Proszę bardzo.

Poseł Krzysztof Truskolaski (KO):

Dziękuję, panie przewodniczący. Panie ministrze, Wysoka Komisjo, rozporządzenie PE i Rady zmieniające rozporządzenie (WE) nr 561/2006 w odniesieniu do minimalnych wymogów dotyczących minimalnych przerw oraz dziennego i tygodniowego okresu odpoczynku w sektorze okazjonalnego przewozu osób COM(2023) 256. Rozporządzenie to nie budzi większych wątpliwości. Jeżeli chodzi o państwa członkowskie, to też nie zgłaszały większych uwag. Ten dokument będzie dalej negocjowany. Pan minister przedstawił szczegóły, więc nie będę się już powtarzał. Powiem tylko, że zgodnie z opinią BAS omawiany wniosek jest ważnym dokumentem wpisującym się w dążenia do poprawy bezpieczeństwa i zdrowia pracowników. W tym wymiarze skutki przedstawionej propozycji należy ocenić pozytywnie. Jeżeli chodzi o wymiar finansowy i gospodarczy, to w długim okresie skutki wprowadzenia proponowanych rozwiązań również będą pozytywne. Dziękuję bardzo.

Przewodniczący poseł Kacper Płażyński (PiS):

Dziękuję. Otwieram dyskusję. Czy ktoś z państwa chce zabrać głos w tej sprawie? Nie słyszę. W związku z tym proponuję, żeby przyjąć konkluzję. Stwierdzam, że **Komisja przyjęła w trybie art. 7 ust. 4 ustawy z dnia 8 października 2020 r. dokument o sygnaturze COM(2023) 256 wersja ostateczna i odnoszący się do niego projekt stanowiska rządu. Komisja podzieliła stanowisko rządu.** Sprzeciwu nie słyszę. Dziękuję bardzo.

Sekretarz stanu w MI Rafał Weber:

Dziękuję bardzo. Dziękuję państwu.

Przewodniczący poseł Kacper Płażyński (PiS):

To koniec. Chyba że mają państwo jeszcze jakieś uwagi? Nie. To kończymy. Zamykam posiedzenie. Dziękuję bardzo.