Parlament Europejski
2019-2024

Komisja Przemysłu, Badań Naukowych i Energii

2023/0108(COD)

7.9.2023

***I
PROJEKT SPRAWOZDANIA

w sprawie wniosku dotyczącego rozporządzenia Parlamentu Europejskiego i Rady zmieniającego rozporządzenie (UE) 2019/881 w odniesieniu do usług zarządzanych w zakresie bezpieczeństwa
(COM(2023)0208 – C9-0137/2023 – 2023/0108(COD))

Komisja Przemysłu, Badań Naukowych i Energii

Sprawozdawczyni: Josianne Cutajar

Objaśnienie używanych znaków

*	Procedura konsultacji
***	Procedura zgody
***I	Zwykła procedura ustawodawcza (pierwsze czytanie)
***II	Zwykła procedura ustawodawcza (drugie czytanie)
***III	Zwykła procedura ustawodawcza (trzecie czytanie)

(Wskazana procedura opiera się na podstawie prawnej zaproponowanej w projekcie aktu.)

Poprawki do projektu aktu

Poprawki Parlamentu w postaci dwóch kolumn

Skreślenia zaznacza się ***wytłuszczonym drukiem i kursywą*** w lewej kolumnie. Zmianę brzmienia zaznacza się ***wytłuszczonym drukiem i kursywą*** w obu kolumnach. Nowy tekst zaznacza się ***wytłuszczonym drukiem i kursywą*** w prawej kolumnie.

Pierwszy i drugi wiersz nagłówka każdej poprawki wskazuje element rozpatrywanego projektu aktu, którego dotyczy poprawka. Jeżeli poprawka odnosi się do obowiązującego aktu, do którego zmiany zmierza projekt aktu, nagłówek zawiera dodatkowo trzeci wiersz, w którym wskazuje się odpowiednio obowiązujący akt i przepis, którego dotyczy poprawka.

Poprawki Parlamentu w postaci tekstu skonsolidowanego

Nowe fragmenty tekstu zaznacza się ***wytłuszczonym drukiem i kursywą.*** Fragmenty tekstu, które zostały skreślone, zaznacza się za pomocą symbolu ▌ lub przekreśla. Zmianę brzmienia zaznacza się przez wyróżnienie nowego tekstu ***wytłuszczonym drukiem i kursywą*** i usunięcie lub przekreślenie zastąpionego tekstu.
Tytułem wyjątku nie zaznacza się zmian o charakterze ściśle technicznym wprowadzonych przez służby w celu opracowania końcowej wersji tekstu.

SPIS TREŚCI

Strona

PROJEKT REZOLUCJI USTAWODAWCZEJ PARLAMENTU EUROPEJSKIEGO 5

UZASADNIENIE 16

ZAŁĄCZNIK: WYKAZ PODMIOTÓW LUB OSÓB, OD KTÓRYCH SPRAWOZDAWCZYNI OTRZYMAŁA INFORMACJE 18

PROJEKT REZOLUCJI USTAWODAWCZEJ PARLAMENTU EUROPEJSKIEGO

w sprawie wniosku dotyczącego rozporządzenia Parlamentu Europejskiego i Rady zmieniającego rozporządzenie (UE) 2019/881 w odniesieniu do usług zarządzanych w zakresie bezpieczeństwa
(COM(2023)0208 – C9-0137/2023 – 2023/0108(COD))

(Zwykła procedura ustawodawcza: pierwsze czytanie)

Parlament Europejski,

– uwzględniając wniosek Komisji przedstawiony Parlamentowi Europejskiemu i Radzie (COM(2023)0208),

– uwzględniając art. 294 ust. 2 i art. 114 Traktatu o funkcjonowaniu Unii Europejskiej, zgodnie z którymi wniosek został przedstawiony Parlamentowi przez Komisję (C9/2023),

– uwzględniając art. 294 ust. 3 Traktatu o funkcjonowaniu Unii Europejskiej,

– uwzględniając opinię Europejskiego Komitetu Ekonomiczno-Społecznego z 13 lipca 2023 r.[1],

– uwzględniając art. 59 Regulaminu,

– uwzględniając pismo przedstawione przez Komisję Rynku Wewnętrznego i Ochrony Konsumentów,

– uwzględniając sprawozdanie Komisji Przemysłu, Badań Naukowych i Energii (A9-0000/2023),

1. przyjmuje poniższe stanowisko w pierwszym czytaniu;

2. zwraca się do Komisji o ponowne przekazanie mu sprawy, jeśli zastąpi ona pierwotny wniosek, wprowadzi w nim istotne zmiany lub planuje ich wprowadzenie;

3. zobowiązuje swoją przewodniczącą do przekazania stanowiska Parlamentu Radzie i Komisji oraz parlamentom narodowym.

[1] Dz.U. C 0 z 0.0.0000, s. 0. Dotychczas nieopublikowana w Dzienniku Urzędowym.

Poprawka 1

Wniosek dotyczący rozporządzenia
Motyw 1 a (nowy)

Tekst proponowany przez Komisję	*Poprawka*
	(1a) Aby zapewnić odporność Unii na cyberataki i zapobiec wszelkim lukom na rynku unijnym, niniejsze rozporządzenie uzupełni horyzontalne ramy regulacyjne ustanawiające kompleksowe wymogi cyberbezpieczeństwa dla wszystkich produktów z elementami cyfrowymi zgodnie z rozporządzeniem Parlamentu Europejskiego i Rady (UE) .../...*+, określając zasadnicze wymogi dotyczące usług zarządzanych w zakresie cyberbezpieczeństwa, ich stosowania i wiarygodności.

Rozporządzenie Parlamentu Europejskiego i Rady (UE) .../... z dnia … w sprawie ...

(Dz.U. ...).

+ Dz.U.: proszę wstawić w tekście numer rozporządzenia zawarty w dokumencie 2022/0272(COD) oraz wstawić w przypisie numer, datę, tytuł tego rozporządzenia i odniesienie do Dz.U.

Or. en

Poprawka 2

Wniosek dotyczący rozporządzenia
Motyw 2

Tekst proponowany przez Komisję	*Poprawka*
(2) Coraz większą rolę w zapobieganiu cyberincydentom i ograniczaniu ich skutków odgrywają usługi zarządzane w zakresie bezpieczeństwa, czyli usługi polegające na prowadzeniu lub wspomaganiu działań związanych z zarządzaniem ryzykiem w cyberprzestrzeni, na jakie narażeni są	(2) Coraz większą rolę w zapobieganiu cyberincydentom i ograniczaniu ich skutków odgrywają usługi zarządzane w zakresie bezpieczeństwa, czyli usługi polegające na prowadzeniu lub wspomaganiu działań związanych z zarządzaniem ryzykiem w cyberprzestrzeni, na jakie narażeni są

klienci dostawców tych usług. W związku z tym dostawców takich usług uznaje się za podmioty kluczowe lub ważne należące do sektora kluczowego na podstawie dyrektywy Parlamentu Europejskiego i Rady (UE) 2022/2555[8]. Zgodnie z motywem 86 tej dyrektywy szczególnie ważną rolę w pomaganiu podmiotom w działaniach mających na celu zapobieganie incydentom, wykrywanie ich, reagowanie na nie lub przywracanie normalnego działania po ich wystąpieniu odgrywają dostawcy usług zarządzanych w zakresie bezpieczeństwa zajmujący się obszarami takimi jak reagowanie na incydenty, testy penetracyjne, audyty bezpieczeństwa i doradztwo. Dostawcy usług zarządzanych w zakresie bezpieczeństwa również sami padają jednak ofiarą cyberataków, a ponieważ ich działalność jest ściśle zintegrowana z operacjami ich klientów, stanowią oni szczególne ryzyko. W związku z tym przy wyborze dostawcy usług zarządzanych w zakresie bezpieczeństwa podmioty kluczowe i ważne w rozumieniu przepisów dyrektywy (UE) 2022/2555 powinny dochować szczególnej staranności.

klienci dostawców tych usług***, m.in. w zakresie zapobiegania incydentom, wykrywania ich, reagowania na nie i usuwania ich skutków. Działalność dostawców usług zarządzanych w zakresie bezpieczeństwa obejmuje usługi związane z identyfikacją, ochroną, wykrywaniem, reagowaniem i przywracaniem gotowości do pracy, w tym m.in. analizę cyberzagrożeń, monitorowanie zagrożeń w czasie rzeczywistym za pomocą proaktywnych technik, w tym uwzględnianie bezpieczeństwa już w fazie projektowania, ocenę ryzyka, rozszerzone wykrywanie, remediację i reagowanie***. W związku z tym dostawców takich usług uznaje się za podmioty kluczowe lub ważne należące do sektora kluczowego na podstawie dyrektywy Parlamentu Europejskiego i Rady (UE) 2022/2555[8]. Zgodnie z motywem 86 tej dyrektywy szczególnie ważną rolę w pomaganiu podmiotom w działaniach mających na celu zapobieganie incydentom, wykrywanie ich, reagowanie na nie lub przywracanie normalnego działania po ich wystąpieniu odgrywają dostawcy usług zarządzanych w zakresie bezpieczeństwa zajmujący się obszarami takimi jak reagowanie na incydenty, testy penetracyjne, audyty bezpieczeństwa i doradztwo. Dostawcy usług zarządzanych w zakresie bezpieczeństwa również sami padają jednak ofiarą cyberataków, a ponieważ ich działalność jest ściśle zintegrowana z operacjami ich klientów, stanowią oni szczególne ryzyko. W związku z tym przy wyborze dostawcy usług zarządzanych w zakresie bezpieczeństwa podmioty kluczowe i ważne w rozumieniu przepisów dyrektywy (UE) 2022/2555 powinny dochować szczególnej staranności.

[8] Dyrektywa Parlamentu Europejskiego i Rady (UE) 2022/2555 z dnia 14 grudnia 2022 r. w sprawie środków na rzecz wysokiego wspólnego poziomu

[8] Dyrektywa Parlamentu Europejskiego i Rady (UE) 2022/2555 z dnia 14 grudnia 2022 r. w sprawie środków na rzecz wysokiego wspólnego poziomu

cyberbezpieczeństwa na terytorium Unii, zmieniająca rozporządzenie (UE) nr 910/2014 i dyrektywę (UE) 2018/1972 oraz uchylająca dyrektywę (UE) 2016/1148 (dyrektywa NIS 2) (Dz.U. L 333 z 27.12.2022, s. 80).	cyberbezpieczeństwa na terytorium Unii, zmieniająca rozporządzenie (UE) nr 910/2014 i dyrektywę (UE) 2018/1972 oraz uchylająca dyrektywę (UE) 2016/1148 (dyrektywa NIS 2) (Dz.U. L 333 z 27.12.2022, s. 80).
	Or. en

Poprawka 3

Wniosek dotyczący rozporządzenia
Motyw 4 a (nowy)

Tekst proponowany przez Komisję	*Poprawka*
	(4a) Europejskie systemy certyfikacji usług zarządzanych w zakresie bezpieczeństwa powinny przyczyniać się do dostępności i przystępności cenowej tych usług, zwłaszcza dla mniejszych podmiotów, takich jak mikroprzedsiębiorstwa oraz małe i średnie przedsiębiorstwa, które często są bardziej narażone na naruszenia cyberbezpieczeństwa mające skutki finansowe, prawne, reputacyjne i operacyjne.
	Or. en

Poprawka 4

Wniosek dotyczący rozporządzenia
Motyw 5 a (nowy)

Tekst proponowany przez Komisję	*Poprawka*
	(5a) Aby ułatwić rozwój wiarygodnego rynku unijnego, a zarazem tworzenie partnerstw z państwami trzecimi o podobnych poglądach, w tym w świetle przepisów rozporządzenia Parlamentu Europejskiego i Rady (UE).../... [*] [++] w odniesieniu do dostępu do unijnej rezerwy cyberbezpieczeństwa, należy usprawnić proces certyfikacji ustanowiony na mocy przepisów niniejszego rozporządzenia, tak by zapewnić międzynarodowe uznawanie i

dostosowanie do norm międzynarodowych.

---

[*] Rozporządzenie Parlamentu Europejskiego i Rady (UE) .../... z dnia … w sprawie ...

(Dz.U. ...).

[++] Dz.U.: proszę wstawić w tekście numer rozporządzenia zawarty w dokumencie 2023/0109(COD) oraz wstawić w przypisie numer, datę, tytuł tego rozporządzenia i odniesienie do Dz.U.

Or. en

Poprawka 5

Wniosek dotyczący rozporządzenia
Motyw 5 b (nowy)

Tekst proponowany przez Komisję	*Poprawka*
	(5b) Aby zapewnić rozwój wiarygodnego unijnego rynku usług zarządzanych w zakresie bezpieczeństwa, dostawcy tych usług i państwa członkowskie powinny współpracować i przyczyniać się do gromadzenia na dużą skalę danych na temat stanu i rozwoju rynku pracy w dziedzinie cyberbezpieczeństwa.

Or. en

Poprawka 6

Wniosek dotyczący rozporządzenia
Motyw 5 c (nowy)

Tekst proponowany przez Komisję	*Poprawka*
	(5c) Ogólnounijne skoordynowane podejście do wzmacniania odporności infrastruktury krytycznej opiera się na budowaniu zdolności państw członkowskich. Jak stwierdzono w niedawnym komunikacie Komisji z 8 kwietnia 2023 r. w sprawie

wyeliminowania niedoboru talentów w dziedzinie cyberbezpieczeństwa w celu zwiększenia konkurencyjności, wzrostu gospodarczego i odporności UE, nie można zagwarantować bezpieczeństwa Unii bez udziału najcenniejszego zasobu UE: jej obywateli. W związku z tym każdy europejski system certyfikacji powinien uwzględniać pomoc dla państw członkowskich, w tym w odniesieniu do niedoboru umiejętności w zakresie cyberbezpieczeństwa.

Or. en

Poprawka 7

Wniosek dotyczący rozporządzenia
Motyw 5 d (nowy)

Tekst proponowany przez Komisję	*Poprawka*
	(5d) W świetle opracowania i wdrożenia europejskiego systemu certyfikacji usług zarządzanych w zakresie bezpieczeństwa Komisja powinna zintensyfikować kontakty z ENISA i ułatwić dialog z państwami członkowskimi, sektorem prywatnym i środowiskiem akademickim, aby lepiej zrozumieć, jakiego typu pracownicy zajmują się cyberbezpieczeństwem i jakie umiejętności posiadają.

Or. en

Poprawka 8

Wniosek dotyczący rozporządzenia
Motyw 5 e (nowy)

Tekst proponowany przez Komisję	*Poprawka*
	(5e) Aby umożliwić europejskim programom cyberbezpieczeństwa poświadczanie, że usługi zarządzane w zakresie bezpieczeństwa, które oceniono zgodnie z takimi programami, są zgodne z określonymi wymogami bezpieczeństwa, w

tym w odniesieniu do bieżącego świadczenia tych usług przez pracowników o bardzo wysokim poziomie odpowiedniej wiedzy technicznej i uczciwości zawodowej, posiadających wymagane kompetencje, wiedzę fachową i doświadczenie, zgodnie z niniejszym rozporządzeniem, programy te powinny angażować środowiska akademickie, instytucje badawcze i inne zainteresowane strony posiadające doświadczenie w zakresie szkoleń specjalistów w dziedzinie cyberbezpieczeństwa oraz przyciągania, rekrutacji i rozwijania talentów, a także zachęcać do partnerstw publiczno-prywatnych. Powinno to stanowić czynnik umożliwiający gromadzenie pomysłów i dzielenie się wiedzą fachową w zakresie szkoleń oraz lepszą ocenę niezbędnych umiejętności, zwłaszcza w trakcie procesu rekrutacji. Poza wnoszeniem wkładu do programu sektor prywatny powinien również zapewniać szkolenia w miejscu pracy w zakresie najbardziej potrzebnych umiejętności, przy udziale administracji publicznej i przedsiębiorstw typu start-up, a także mikroprzedsiębiorstw oraz małych i średnich przedsiębiorstw.

Or. en

Poprawka 9

Wniosek dotyczący rozporządzenia
Motyw 5 f (nowy)

Tekst proponowany przez Komisję	*Poprawka*
	(5f) Aby ułatwić powstawanie wysokiej jakości podstawowych usług zarządzanych w zakresie bezpieczeństwa, państwa członkowskie powinny aktywnie działać na rzecz szkolenia i zatrzymywania talentów, m.in. poprzez włączenie cyberbezpieczeństwa do programów kształcenia i szkolenia, przy jednoczesnym zapewnieniu dostępu do praktyk i staży dla młodych ludzi, zwłaszcza osób mieszkających w regionach

	defaworyzowanych, takich jak wyspy, obszary słabo zaludnione, obszary wiejskie i obszary oddalone. Działania te powinny również mieć na celu przyciągnięcie większej liczby kobiet i dziewcząt do tej dziedziny oraz przyczynienie się do rozwiązania problemu różnic w traktowaniu kobiet i mężczyzn w dziedzinie nauk przyrodniczych, technologii, inżynierii i matematyki.

Or. en

Poprawka 10

Wniosek dotyczący rozporządzenia
Artykuł 1 – akapit 1 – punkt 2 – litera b
Rozporządzenie (UE) 2019/881
Artykuł 2 – punkt 14 a

Tekst proponowany przez Komisję	*Poprawka*
14a) „usługa zarządzana w zakresie bezpieczeństwa” oznacza usługę polegającą na prowadzeniu lub wspomaganiu działań związanych z zarządzaniem ryzykiem w cyberprzestrzeni, takich jak reagowanie na ***incydenty***, testy penetracyjne, audyty bezpieczeństwa i doradztwo;	14a) „usługa zarządzana w zakresie bezpieczeństwa” oznacza usługę ***zlecaną usługodawcy zewnętrznemu,*** polegającą na prowadzeniu lub wspomaganiu działań związanych z zarządzaniem ryzykiem w cyberprzestrzeni, takich jak ***zapobieganie incydentom, wykrywanie ich,*** reagowanie na ***nie i usuwanie ich skutków***, testy penetracyjne, audyty bezpieczeństwa i doradztwo;

Or. en

Poprawka 11

Wniosek dotyczący rozporządzenia
Artykuł 1 – akapit 1 – punkt 6
Rozporządzenie (UE) 2019/881
Artykuł 47 – ustęp 3 – litera e a (nowa)

Tekst proponowany przez Komisję	*Poprawka*
	ea) uprzednie dostosowanie do obowiązujących norm międzynarodowych;

Or. en

Poprawka 12

Wniosek dotyczący rozporządzenia
Artykuł 1 – akapit 1 – punkt 6
Rozporządzenie (UE) 2019/881
Artykuł 47 – ustęp 3 – litera e b (nowa)

Tekst proponowany przez Komisję	*Poprawka*
	eb) wkład dostawcy usług zarządzanych w zakresie bezpieczeństwa w oferowanie pracownikom możliwości szkolenia i podnoszenia kwalifikacji w celu osiągnięcia bardzo wysokiego poziomu odpowiedniej wiedzy technicznej i uczciwości zawodowej.

Or. en

Poprawka 13

Wniosek dotyczący rozporządzenia
Artykuł 1 – akapit 1 – punkt 6
Rozporządzenie (UE) 2019/881
Artykuł 47 – akapit 3 a (nowy)

Tekst proponowany przez Komisję	*Poprawka*
	3a. Ponadto włączenie konkretnych usług zarządzanych w zakresie bezpieczeństwa do unijnego kroczącego programu prac uwzględnia, w stosownych przypadkach, wkład dostawców usług zarządzanych w zakresie bezpieczeństwa w szkolenie i przyciąganie talentów, zwłaszcza poprzez partnerstwa z uniwersytetami i innymi instytucjami edukacyjnymi.

Or. en

Poprawka 14

Wniosek dotyczący rozporządzenia
Artykuł 1 – akapit 1 – punkt 7
Rozporządzenie (UE) 2019/881
Artykuł 49 – akapit 7 a (nowy)

Tekst proponowany przez Komisję	*Poprawka*
	7a. Propozycję programu opracowuje się z uwzględnieniem wszelkich informacji pochodzących z europejskiego systemu normalizacji technicznej lub z unijnych agencji sektorowych.

Or. en

Poprawka 15

Wniosek dotyczący rozporządzenia
Artykuł 1 – akapit 1 – punkt 9
Rozporządzenie (UE) 2019/881
Artykuł 51a – akapit 1 – litera b

Tekst proponowany przez Komisję	*Poprawka*
b) zapewniać, aby dostawca stosował odpowiednie procedury wewnętrzne w celu zagwarantowania, że usługi zarządzane w zakresie bezpieczeństwa są zawsze świadczone przy zachowaniu bardzo wysokiego poziomu jakości;	b) zapewniać, aby dostawca stosował odpowiednie procedury wewnętrzne w celu zagwarantowania, że usługi zarządzane w zakresie bezpieczeństwa są zawsze świadczone przy zachowaniu bardzo wysokiego poziomu jakości ***i niezawodności***;

Or. en

Poprawka 16

Wniosek dotyczący rozporządzenia
Artykuł 1 – akapit 1 – punkt 13 – litera b – podpunkt ii – litera bb
Rozporządzenie (UE) 2019/881
Artykuł 56 – ustęp 3 – litera d

Tekst proponowany przez Komisję	*Poprawka*
d) bierze pod uwagę terminy wdrożenia, środki i okresy przejściowe, w szczególności pod względem ewentualnego wpływu danego środka na wytwórców lub dostawców produktów ICT, usług ICT, procesów ICT lub usług zarządzanych w zakresie bezpieczeństwa, w tym ***na MŚP;***	d) bierze pod uwagę terminy wdrożenia, środki i okresy przejściowe, w szczególności pod względem ewentualnego wpływu danego środka na wytwórców lub dostawców produktów ICT, usług ICT, procesów ICT lub usług zarządzanych w zakresie bezpieczeństwa, w tym ***szczególne interesy i potrzeby mikroprzedsiębiorstw oraz małych i średnich przedsiębiorstw. Komisja***

zapewnia odpowiednie wsparcie finansowe w ramach istniejących programów Unii, w szczególności w celu zmniejszenia obciążeń finansowych dla mikroprzedsiębiorstw oraz małych i średnich przedsiębiorstw.

Or. en

UZASADNIENIE

Sprawozdawczyni popiera wniosek dotyczący rozporządzenia Parlamentu Europejskiego i Rady zmieniającego rozporządzenie (UE) 2019/8811 w odniesieniu do usług zarządzanych w zakresie bezpieczeństwa, rozumiejąc konieczność aktualizacji i wzmocnienia europejskiego programu certyfikacji cyberbezpieczeństwa, tak aby obejmował on ważne i rozwijające się usługi w tym sektorze. Biorąc pod uwagę, w jaki sposób poszczególne państwa członkowskie rozpoczęły już przyjmowanie programów certyfikacji dla usług zarządzanych w zakresie bezpieczeństwa, sprawozdawczyni jest zdania, że zmiany w akcie o cyberbezpieczeństwie mają kluczowe znaczenie dla zapobieżenia poważnym rozbieżnościom między programami krajowymi, które doprowadziłyby do fragmentacji rynku, co stoi w sprzeczności nie tylko z interesami gospodarczymi Unii, ale także z jej interesami strategicznymi.

W związku z tym sprawozdawczyni docenia sposób, w jaki omawiany wniosek ma uzupełniać akt w sprawie cybersolidarności, w szczególności rozszerzenie o europejski program certyfikacji cyberbezpieczeństwa, co umożliwi usługom zarządzanym w zakresie bezpieczeństwa – analogicznie do „zaufanych dostawców", o których mowa w akcie w sprawie cybersolidarności – odegrać ważną rolę w przyszłej unijnej rezerwie cyberbezpieczeństwa. Dlatego omawiany wniosek ma również ogromne znaczenie dla wspierania szerszych zdolności Unii w zakresie cyberbezpieczeństwa, które są kluczowe dla przeciwdziałania potencjalnym zagrożeniom w stale zmieniających się realiach geopolitycznych.

W granicach określonych we wniosku Komisji celem sprawozdawczyni jest skonsolidowanie tej ukierunkowanej zmiany aktu o cyberbezpieczeństwie i dalsze zwiększenie jasności przepisów. Ilustrują to zmiany wprowadzone przez sprawozdawczynię w definicji usług zarządzanych w zakresie bezpieczeństwa, wyjaśniające, że są one „zlecane usługodawcy zewnętrznemu", i doprecyzowujące zakres definicji. Zgłoszone poprawki dotyczące uznawania międzynarodowych norm cyberbezpieczeństwa mają na celu zwiększenie zaufania, a zarazem opracowanie kompleksowych przepisów UE.

W niniejszym projekcie sprawozdania położono większy nacisk na rozwiązanie problemu niedoboru kwalifikacji oraz na wspieranie mikroprzedsiębiorstw oraz małych i średnich przedsiębiorstw. W pierwszym przypadku poprawki opierają się na już istniejącym założeniu konieczności posiadania umiejętności w programie certyfikacji cyberbezpieczeństwa w odniesieniu do „pracowników o bardzo wysokim poziomie odpowiedniej wiedzy technicznej i uczciwości zawodowej, posiadających wymagane kompetencje, wiedzę fachową i doświadczenie". Zdaniem sprawozdawczyni europejski system certyfikacji, przy wsparciu współpracy między wszystkimi zaangażowanymi podmiotami, a także między państwami członkowskimi, sektorem prywatnym, środowiskiem akademickim i instytucjami badawczymi, musi stanowić czynnik umożliwiający opracowanie nowego planu działania na rzecz szkolenia i wzmocnienia pozycji pracowników, gromadząc więcej danych na temat potrzebnych umiejętności i przyczyniając się do rozwiązania problemu różnic w traktowaniu kobiet i mężczyzn w dziedzinie nauk ścisłych, technologii, inżynierii i matematyki.

Jednocześnie mikroprzedsiębiorstwa oraz małe i średnie przedsiębiorstwa, które stanowią trzon gospodarki europejskiej i z pewnością mogą odegrać pozytywną rolę w sektorze

cyberbezpieczeństwa, powinny korzystać z odpowiedniego wsparcia finansowego w ramach istniejących programów unijnych, aby zmniejszyć wszelkie ciążące na nich nieproporcjonalne obciążenia finansowe.

ZAŁĄCZNIK: WYKAZ PODMIOTÓW LUB OSÓB, OD KTÓRYCH SPRAWOZDAWCZYNI OTRZYMAŁA INFORMACJE

Poniższy wykaz opracowano na zasadzie zupełnej dobrowolności, na wyłączną odpowiedzialność sprawozdawczyni komisji opiniodawczej. Podczas przygotowywania projektu sprawozdania w sprawie wniosku dotyczącego rozporządzenia Parlamentu Europejskiego i Rady zmieniającego rozporządzenie (UE) 2019/881 w odniesieniu do usług zarządzanych w zakresie bezpieczeństwa (2023/0108 (COD)) sprawozdawczyni otrzymała informacje od następujących podmiotów lub osób:

Podmiot i/lub osoba
Europejski Komitet Ekonomiczno-Społeczny;
Komisja Europejska
ENISA
Leonardo Cyber and Security Solutions
Red Alert Labs IoT Security
ESET Slovak
Board of Cyber
IBM
Tecnalia
FERMA - Federation of European Risk Management Associations