



Warszawa, 27 czerwca 2026 roku

**Szanowny Pan Krzysztof Gawkowski
Wiceprezes Rady Ministrów, Minister Cyfryzacji
Pełnomocnik Rządu ds. Cyberbezpieczeństwa**

**Ministerstwo Cyfryzacji
ul. Królewska 27, 00-060 Warszawa**

Szanowny Panie Premierze,

Izba Gospodarki Elektronicznej zwraca się z apelem o rozważenie przez Ministerstwo Cyfryzacji doprecyzowania, złagodzenia lub odpowiedniego znuansowania stanowisk wyrażonych w dokumencie „Ustawa z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa po nowelizacji / PYTANIA I ODPOWIEDZI” (dalej: „Q&A”), a także przedstawienia wyjaśnień dotyczących obowiązków wynikających z ustawy o krajowym systemie cyberbezpieczeństwa (dalej: „UKSC”), z uwzględnieniem okoliczności przedstawionych poniżej.

Niniejsze pismo odnosi się do zagadnień praktycznych, które członkowie Izby identyfikują jako problematyczne na podstawie doświadczeń z wdrażania przepisów znowelizowanej UKSC. Biorąc pod uwagę deklarowany w trakcie prac komisji senackiej m.in. przez Ministra Pawła Olszewskiego zamiar doprecyzowania poszczególnych elementów ustawy, w tym wątpliwości interpretacyjnych, jakie wynikną w okresie jej stosowania, liczymy na przychylenie się do skierowanej przez Izbę prośby i przedstawienie wyjaśnień dotyczących poruszonych w piśmie zagadnień.

1. ŚWIADCZENIE USŁUG Z ZAKRESU CYBERBEZPIECZEŃSTWA WYŁĄCZNIE W RAMACH WŁASNEJ GRUPY KAPITAŁOWEJ

[Podstawa zagadnienia]

Na stronie 26 zaktualizowanych Q&A znalazło się następujące pytanie i odpowiedź:

1.21. Czy spółka IT realizująca zadania z zakresu cyberbezpieczeństwa tylko dla własnej grupy kapitałowej podlega znowelizowanej KSC?

Tak, jeżeli jest co najmniej małym przedsiębiorstwem. Skoro tego typu podmioty świadczą usługi np. obsługi incydentów, przetwarzając przy tym wrażliwe dane swoich klientów, to powinny spełniać wymogi z zakresu cyberbezpieczeństwa.

Ponadto na stronie 74 Q&A (w wersji po aktualizacji w początku czerwca) znalazło się następujące pytanie i odpowiedź:



3.34. Czy jeżeli spółka świadczy usługi zarządzane z zakresu cyberbezpieczeństwa tylko dla innych spółek w ramach grupy kapitałowej to czy podlega pod ustawę o KSC? [NOWE – aktualizacja czerwiec 2026 r.]

Tak, ponieważ jako odrębny podmiot świadczy usługi innemu podmiotowi.

[Zidentyfikowany problem]

Wątpliwości budzi samo sformułowanie użyte w Q&A, tj. „spółka IT realizująca zadania z zakresu cyberbezpieczeństwa”. Sformułowanie to nie jest tożsame z ustawowymi kategoriami odnoszącymi się np. do świadczenia usług zarządzanych lub usług zarządzanych w zakresie cyberbezpieczeństwa. Zasadne byłoby zatem doprecyzowanie i wyjaśnienie, czy w pytaniu 1.21 chodzi w istocie o świadczenie usług zarządzanych w zakresie cyberbezpieczeństwa, czy też o inne, szersze ujęcie – a jeśli tak, to jakie.

Zacytowane powyżej pytania i odpowiedzi 1.21 i 3.34 wiążą się z problemem prawnym, z którym mierzą się przedstawiciele rynku. Chodzi o wątpliwości dotyczące objęcia nowymi regulacjami (NIS2, znowelizowana UKSC) podmiotów (spółek) świadczących usługi zarządzane, w tym usługi zarządzane w zakresie cyberbezpieczeństwa, wyłącznie na rzecz spółki lub spółek z własnej grupy kapitałowej (np. spółka zależna świadczy usługi na rzecz spółki dominującej). Sprawa ta nie jest – na gruncie normatywnym – jednoznaczna.

Literalne brzmienie przepisów może prowadzić do wniosku, że takie podmioty są objęte, bez żadnych wyjątków, pełnym reżimem dyrektywy NIS2 i znowelizowanej UKSC (o ile spełniają kryteria wielkościowe). Za taką literalną interpretacją przepisów opowiada się jednoznacznie zaktualizowane Q&A. W ocenie Izby zaproponowane w Q&A podejście literalne jest nieproporcjonalne i nadmierne. Przemawiają za tym następujące argumenty:

- Zasada proporcjonalności regulacji. Wykładnia literalna, przedstawiona w Q&A, prowadzi do tego, że wewnętrzne, organizacyjne uporządkowanie funkcji ICT i cyberbezpieczeństwa w grupie kapitałowej jest traktowane na równi z profesjonalnym, rynkowym świadczeniem usług na rzecz niepowiązanych klientów, mimo że poziom ryzyka regulacyjnego i gospodarczego w obu przypadkach nie jest tożsamy.
- Ratio legis analizowanych regulacji. NIS2 oraz jej krajowa implementacja mają służyć podniesieniu poziomu cyberbezpieczeństwa podmiotów istotnych z perspektywy funkcjonowania państwa i gospodarki, w szczególności przez adresowanie ryzyk związanych z łańcuchem dostaw, zależnościami od podmiotów trzecich oraz outsourcingiem funkcji ICT i bezpieczeństwa. Tymczasem w przypadku świadczeń realizowanych wyłącznie wewnątrz grupy kapitałowej nie mamy do czynienia z typowym ryzykiem zewnętrznego rynku usług, lecz z wewnętrznym modelem organizacji tych samych funkcji w ramach – de facto – jednego organizmu gospodarczego. Innymi słowy, modelowi, w którym spółka z grupy kapitałowej realizuje usługi zarządzane, w tym usługi zarządzane z zakresu cyberbezpieczeństwa, bliżej jest do gospodarki wewnętrznej (wewnątrzgrupowej, wewnątrzzakładowej) niż do oferowania usług klientom.
- W powyższym ujęciu spółka usługowa z grupy kapitałowej pełni funkcję wewnętrznego centrum kompetencyjnego lub operacyjnego, a nie niezależnego dostawcy działającego na otwartym rynku.



Taki sposób patrzenia znajduje zresztą pewne analogie w innych dziedzinach prawa, w szczególności w prawie konkurencji, gdzie dla określonych celów grupa kapitałowa bywa traktowana jako jedno przedsiębiorstwo. Choć e-Izba rozumie, że analogii tej nie należy przenosić automatycznie na grunt NIS2 i znowelizowanej UKSC, to ilustruje ona, że świadczenia realizowane wyłącznie wewnątrz grupy powinny być oceniane z większym uwzględnieniem ich rzeczywistej funkcji gospodarczej, a nie wyłącznie przez pryzmat formalnego modelu świadczenia usług.

- Z perspektywy gospodarczej szerokie, literalne podejście tworzy ponadto niepożądany bodziec regulacyjny: zamiast wspierać budowanie kompetencji cyberbezpieczeństwa wewnątrz grup kapitałowych, może skłaniać przedsiębiorców do outsourcingu usług zarządzanych lub usług zarządzanych w zakresie cyberbezpieczeństwa, wyłącznie po to, aby zoptymalizować koszty związane z wdrożeniem rozbudowanych wymogów regulacyjnych. Co istotne, koszty prawidłowego wdrożenia wymogów regulacyjnych dla podmiotów świadczących usługi zarządzane lub usługi zarządzane w zakresie cyberbezpieczeństwa mogą pozostawać rażąco nieadekwatne do kosztów outsourcingu, czyniąc ten drugi rozwiązaniem opłacalnym. Taki efekt jest trudny do pogodzenia z celami NIS2, ponieważ osłabia motywację do rozwijania stabilnych, wyspecjalizowanych i dobrze kontrolowanych funkcji bezpieczeństwa wewnątrz organizacji.

[Kwestia wymagająca wyjaśnienia]

Stanowisko przedstawione w Q&A wprost opowiada się za objęciem takich podmiotów zakresem regulacji NIS2 i znowelizowanej UKSC. W przekonaniu Izby potrzebne jest odpowiednie złagodzenie lub zniuansowanie tego stanowiska - tak aby rozróżnić świadczenie usług na rynku od świadczeń realizowanych wyłącznie wewnątrz jednej grupy kapitałowej. Brak takiego rozróżnienia prowadzi do objęcia identycznym ciężarem *compliance* sytuacji jakościowo odmiennych. Zasadne jest w szczególności uwzględnienie, że podmioty świadczące usługi zarządzane wyłącznie na potrzeby własnej grupy kapitałowej, jeżeli nie oferują tych usług na rynku, nie generują ryzyk właściwych dla zewnętrznego łańcucha dostaw.

Z powyższych powodów Izba zwraca się z apelem o rozważenie przez Ministerstwo modyfikacji (złagodzenia lub zniuansowania) stanowiska przedstawionego w Q&A.

2. WYJAŚNIENIA DOTYCZĄCE POJĘCIA DOSTAWCY USŁUG CHMUROWYCH

[Podstawa zagadnienia]

Na stronie 26 zaktualizowanych Q&A znalazło się następujące pytanie i odpowiedź:

1.22. Kim jest dostawca usług chmurowych?

Dostawca usług chmurowych jest to podmiot świadczący usługi przetwarzania danych w modelu chmury obliczeniowej, zapewniając użytkownikowi na żądanie zdalny dostęp do skalowalnych oraz elastycznych zasobów IT - m.in. mocy obliczeniowej, pamięci, oprogramowania lub platform. Obejmuje to

w szczególności usługi w modelu infrastruktura jako usługa (IaaS), platforma jako usługa (PaaS) oraz oprogramowanie jako usługa (SaaS). Usługi te mogą być świadczone w różnych modelach wdrożeniowych, np. chmurze prywatnej, publicznej, hybrydowej, czy wspólnotowej. Przy identyfikacji,



czy dany dostawca jest dostawcą usług chmurowych należy przede wszystkim zwrócić uwagę na cel i funkcjonalność usługi, tj. czy usługa zapewnia użytkownikowi bezpośredni dostęp do skalowalnej i elastycznej puli zasobów obliczeniowych. W niektórych sytuacjach, w modelu SaaS, dostawca może być jedynie dostawcą oprogramowania, a nie dostawcą chmury obliczeniowej. Może to mieć miejsce w sytuacji, w której dostawca oprogramowania korzysta jedynie z chmury obliczeniowej, ale nie jest jej dostawcą, a dane oprogramowanie uruchamiane jest u odbiorcy na zasadzie on premise.

[Zidentyfikowany problem]

Brzmienie definicji dostawcy usług chmurowych oraz zaproponowane w Q&A wyjaśnienia budzą wątpliwości w części dotyczącej usług SaaS, które mogą prowadzić do nadmiernej kwalifikacji usług hostowanych (tj. różnego rodzaju oprogramowania udostępnianego jako działająca usługa).

[Kwestia wymagająca wyjaśnienia]

Zawarte w Q&A sformułowanie „zapewnienie użytkownikowi bezpośredniego dostępu do skalowalnej i elastycznej puli zasobów obliczeniowych” jest trudne do praktycznego zastosowania. **Zasadne jest więc doprecyzowanie, że chodzi o rozwiązania, których celem i funkcjonalnością jest przede wszystkim umożliwienie przetwarzania danych przez odbiorcę, za pomocą tej usługi, w skali**

i ilości, dla której w normalnym toku czynności istotne znaczenie ma dostępność i elastyczność zasobów obliczeniowych. Chodzi więc o oprogramowanie, które (i) jest hostowane przez dostawcę w chmurze (własnej lub dostarczanej przez podwykonawcę/-ów), (ii) które jest udostępniane jako działająca usługa, (iii) którego funkcjonalność głównie polega na przetwarzaniu danych dla odbiorcy, a nie pomocniczo w ramach innych celów, (iv) w którym dostęp do skalowalnych i elastycznych zasobów wystarczająco manifestuje się, np. przez cel użycia (oprogramowanie bazodanowe) lub sposób mierzenia usługi uwzględniający zużycie zasobów obliczeniowych. W obecnej sytuacji skrajnie dosłowna interpretacja definicji ustawowej może prowadzić do tego, że pod usługę chmurową w formule SaaS kwalifikuje się wiele usług hostowanych, nawet jeśli aspekt dostępu do zasobów jest w ich przypadku irrelevantny lub oferują one ograniczone funkcjonalności w zakresie przetwarzania danych (niewielkie aplikacje z ograniczoną liczbą funkcjonalności biznesowych). To dowodzi więc, że w tym przypadku również potrzebne są funkcjonalne kryteria pomocnicze dla definicji ustawowej.

Wątpliwości Izby budzi również sformułowanie z Q&A „w niektórych sytuacjach, w modelu SaaS, dostawca może być jedynie dostawcą oprogramowania, a nie dostawcą chmury obliczeniowej. Może to mieć miejsce w sytuacji, w której dostawca oprogramowania korzysta jedynie z chmury obliczeniowej, ale nie jest jej dostawcą, a dane oprogramowanie uruchamiane jest u odbiorcy na zasadzie on premise”.

W ocenie Izby wymagałoby dalszego doprecyzowania, że immanentną cechą modelu SaaS jest dostarczenie oprogramowania jako usługi, tj. dostępu do oprogramowania działającego w infrastrukturze chmurowej, zewnętrznej względem odbiorcy usługi SaaS. Może to być infrastruktura producenta aplikacji lub jego podwykonawcy, gdyż oba modele są w praktyce spotykane. Model, w którym dostawca SaaS „jedynie korzysta z chmury” budzi wątpliwości prawne chociażby na gruncie RODO, gdzie wtedy niejasne jest, kto jest procesorem danych, jeśli dostawca SaaS formalnie nie odpowiada za infrastrukturę chmurową, w której działa oprogramowanie, a którą to infrastrukturę dostarcza inny podmiot. W ocenie Izby uruchomienie aplikacji w infrastrukturze chmurowej klienta jest bliższe w swej istocie do licencji i usługi utrzymania oprogramowania, względnie usług



zarządzanych, niż do usługi SaaS. Wobec klasycznego modelu *on-premise* zmienia się bowiem jedynie typ infrastruktury IT – zamiast własnościowej infrastruktury klienta, zazwyczaj wystawia on wykupioną przez siebie przestrzeń w chmurze obliczeniowej. Zasadne jest zatem doprecyzowanie, że model SaaS obejmuje usługi, w których dostawca (i) zapewnia dostęp do działającego oprogramowania, (ii) odpowiedzialność za hosting oprogramowania modelowo jest po stronie dostawcy SaaS, zarówno jeśli kontroluje on infrastrukturę chmurową lub korzysta w tym zakresie z podwykonawcy, (iii) spełnione są kryteria definicji ustawowej, tj. usługa zapewnia (odpowiedni do charakteru usługi SaaS) dostęp do skalowalnego i elastycznego zbioru zasobów obliczeniowych do wspólnego wykorzystywania przez wielu użytkowników. Poprzez „odpowiedni” dostęp w tym przypadku należy rozumieć charakterystykę SaaS opisaną przy poprzednim zagadnieniu.

3. OBLICZANIE WIELKOŚCI PRZEDSIĘBIORSTWA NA POTRZEBY KWALIFIKACJI JAKO PODMIOT KLUCZOWY LUB WAŻNY

[Podstawa zagadnienia]

Sposób ustalania liczby pracowników oraz danych finansowych dla celów samoidentyfikacji na gruncie ustawy o krajowym systemie cyberbezpieczeństwa.

Na stronie 16 zaktualizowanych Q&A znalazło się następujące pytanie i odpowiedź:

1.1. Co musi zrobić przedsiębiorca, który nie wie czy podlega pod krajowy system cyberbezpieczeństwa?

Przed wszystkim taki przedsiębiorca musi zorientować się jaka jest jego wielkość oraz jakie działalności prowadzi. Dane finansowe przedsiębiorstwa są wskazane w sprawozdaniu finansowym (przesłanki uznania za podmiot kluczowy lub podmiot ważny bada się według stanu na dzień sporządzenia sprawozdania finansowego). Konieczne będzie również ustalenie liczby zatrudnionego personelu. Działalność należy określić w oparciu o prawidłowo zadeklarowane kody Polskiej Klasyfikacji Działalności (PKD) oraz dokumenty urzędowe takie jak koncesje, zezwolenia, wpisy z rejestrów działalności regulowanej. Następnie należy przeanalizować art. 5 ustawy - gdzie wskazano jakie podmioty są podmiotami kluczowymi albo podmiotami ważnymi oraz przeanalizować rodzaje działalności wskazane w załączniku nr 1 i nr 2 do ustawy o KSC.

[Zidentyfikowany problem]

W przywołanej odpowiedzi na pytanie „Co musi zrobić przedsiębiorca, który nie wie, czy podlega pod krajowy system cyberbezpieczeństwa?” wskazano, że przedsiębiorca powinien ustalić m.in. swoją wielkość oraz zakres prowadzonej działalności, a przesłanki uznania za podmiot kluczowy lub podmiot ważny należy badać **według stanu na dzień sporządzenia sprawozdania finansowego**. Taki kierunek jest spójny z art. 5 ust. 5 ustawy o krajowym systemie cyberbezpieczeństwa, który stanowi analogicznie, że jeżeli status podmiotu kluczowego lub podmiotu ważnego zależy od wielkości podmiotu, przesłanki uznania bada się właśnie według stanu na dzień sporządzenia sprawozdania finansowego.

Na tym tle może powstać jednak istotna wątpliwość interpretacyjna: **przepis ten określa moment, na który należy badać spełnienie przesłanek, ale nie przesądza jednoznacznie metodyki**



obliczania liczby personelu. Innymi słowy, z literalnego brzmienia ustawy wynika „kiedy” należy badać status podmiotu, natomiast nie wynika z niej jednoznacznie „jak” należy liczyć zatrudnienie i dane finansowe dla potrzeb tej oceny.

Ustawa o KSC odwołuje się bowiem wyraźnie do art. 2 ust. 1 załącznika I do rozporządzenia Komisji (UE) nr 651/2014 jako podstawy kwalifikowania przedsiębiorstwa według jego wielkości. Równocześnie konstrukcja ustawy zakłada - co do zasady - uwzględnianie danych przedsiębiorstw partnerskich i powiązanych według zasad przewidzianych w art. 6 ust. 2-4 ww. załącznika I.

Jednocześnie **ustawa nie zawiera wyraźnego odesłania do art. 4 i 5 załącznika I do rozporządzenia 651/2014**, które mają kluczowe znaczenie z perspektywy praktycznej metodyki ustalania wielkości przedsiębiorstwa. Tymczasem art. 4 załącznika I stanowi, że dane służące do określania liczby personelu i kwot finansowych powinny odnosić się do ostatniego zatwierdzonego okresu obrachunkowego i być obliczane w skali rocznej, a ponadto przewiduje regułę dwuletniej stabilizacji statusu przedsiębiorstwa. Z kolei art. 5 załącznika I wprost wskazuje, że liczba personelu odpowiada liczbie rocznych jednostek pracy (RJP), a więc średniorocznemu zatrudnieniu, a nie prostemu stanowi zatrudnienia na określony dzień.

W konsekwencji można bronić tezy, że **samo wskazanie w ustawie dnia sporządzenia sprawozdania finansowego jako momentu badania przesłanek nie rozstrzyga jeszcze, czy liczba pracowników ma być ustalana jako stan na ten dzień, czy też zgodnie z unijną metodologią RJP odnoszoną**

do całego okresu obrachunkowego. W praktyce są to dwa różne podejścia, które mogą prowadzić do odmiennych wyników klasyfikacyjnych, zwłaszcza w przypadku podmiotów o zmiennym zatrudnieniu, grup kapitałowych albo przedsiębiorstw korzystających z różnych modeli zatrudnienia.

Źródłem dodatkowej niepewności jest to, że w materiałach towarzyszących procesowi legislacyjnemu można odnaleźć założenie pełniejszego odwołania do metodologii unijnej, obejmującej zarówno roczne dane finansowe, jak i średnioroczne zatrudnienie liczone w RJP oraz regułę stabilizacji statusu w okresie dwóch kolejnych lat. Jeżeli jednak takie założenie nie zostało dostatecznie wprost odzwierciedlone

w samym tekście normatywnym lub w oficjalnych wyjaśnieniach interpretacyjnych, w związku z czym w naszej ocenie istnieje ryzyko, że praktyka samoidentyfikacji może nie być jednolita.

To z kolei może prowadzić do sytuacji, w której część przedsiębiorców będzie stosowała pełną metodologię wynikającą z załącznika I do rozporządzenia 651/2014, w tym średnioroczne zatrudnienie w RJP i dane roczne, podczas gdy inni przyjmą inne podejście, np. oparte wyłącznie na stanie zatrudnienia na dzień sporządzenia sprawozdania finansowego. Z perspektywy pewności prawa i jednolitości stosowania przepisów taki stan należy ocenić krytycznie, ponieważ zwiększa on ryzyko błędnej samoidentyfikacji podmiotów jako kluczowych, ważnych albo pozostających poza zakresem ustawy.

[Kwestia wymagająca wyjaśnienia]

Wydaje się zatem zasadne, aby w oficjalnych pytaniach i odpowiedziach ministerstwo jednoznacznie doprecyzowało, czy przy ustalaniu wielkości przedsiębiorstwa na potrzeby art. 5 ustawy należy stosować pełną metodologię wynikającą z załącznika I do rozporządzenia 651/2014, w szczególności:



sposób liczenia personelu w rocznych jednostkach pracy (RJP), a także regułę dwuletniej stabilizacji statusu przedsiębiorstwa.

Bez takiego doprecyzowania obecne brzmienie przepisów i wyjaśnień może prowadzić do rozbieżności interpretacyjnych oraz niejednolitej praktyki rynkowej, co w obszarze obowiązkowej samoidentyfikacji podmiotów objętych reżimem cyberbezpieczeństwa należy uznać za szczególnie niepożądane.

Z wyrazami szacunku

Patrycja Sass-Staniszevska

Prezes Izby Gospodarki Elektronicznej

poświadczenie złożenia podpisów i pieczęci elektronicznych

Certyfikat dla dokumentu o Autenti ID: 956779c3-9b7d-4c62-b44b-688e259d117f
utworzonego: 2026-06-29 11:43 (GMT+02:00)

Dokument przekazany do podpisu przez Izba Gospodarki Elektronicznej biuro@eizba.pl, został zabezpieczony pieczęcią elektroniczną Autenti przed wprowadzeniem nieautoryzowanych zmian.



2026-06-29 11:43 (GMT+02:00)

Patrycja Staniszevska

patrycja.staniszevska@eizba.pl

Izba Gospodarki Elektronicznej

NIP: 7010391922 | Prezes Zarządu



**Podpis elektroniczny
zabezpieczony pieczęcią Autenti**

Uwierzytelnienie: e-mail

Powód: Podpisanie dokumentu

Adres IP: 2a00:f41:14d3:15ff:0:11:fab:f201

2026-06-29 11:52 (GMT+02:00)

Autentyczność oraz integralność podpisanego dokumentu przed wprowadzeniem nieautoryzowanych zmian została zabezpieczona pieczęcią elektroniczną Autenti.



2026-06-29 11:52 (GMT+02:00)

Niniejszy dokument stanowi poświadczenie wykonania usługi zaufania, w tym złożenia podpisów elektronicznych, zgodnie z zasadami opisanymi w Polityce.

Osoby podpisujące dokument złożyły podpisy elektroniczne zgodnie z zasadami opisanymi w Polityce Usług Zaufania Autenti dla podpisów elektronicznych Autenti oraz obsługi podpisywania dokumentów (dostępnej na: <https://autenti.com/pl/regulaminy>) oraz oświadczyły, że znają i akceptują treść podpisywanego dokumentu a także potwierdziły poprawność i prawdziwość danych służących do złożenia podpisu elektronicznego.

W ramach składania podpisów elektronicznych przeprowadzono uwierzytelnienie podpisujących.

Usługa została wykonana zgodnie z Rozporządzeniem Parlamentu Europejskiego i Rady (UE) nr 910/2014 z dnia 23 lipca 2014 r. w sprawie identyfikacji elektronicznej i usług zaufania w odniesieniu do transakcji elektronicznych na rynku wewnętrznym oraz uchylające dyrektywę 1999/93/WE (Rozporządzenie eIDAS).

Karta podpisów stanowi poświadczenie Autenti w zakresie realizacji poszczególnych usług zaufania, zgodnie z zasadami ich świadczenia oraz definicjami zawartymi w Polityce.