Uwagi Polskiej Izby Informatyki i Telekomunikacji (PIIT) do projektu ustawy o zmianie ustawy o usługach zaufania oraz identyfikacji elektronicznej (UD352). Projekt z dnia 1 czerwca 2026 r.

Rekomendacja główna

PIIT rekomenduje całościową rezygnację z projektowanego mechanizmu wstrzymania świadczenia kwalifikowanej usługi zaufania i oparcie działań nadzorczych na mechanizmach ustawy o krajowym systemie cyberbezpieczeństwa oraz istniejących mechanizmach eIDAS. Jeżeli projektodawca uzna, że dodatkowy środek powinien zostać utrzymany, powinien on zostać ograniczony zgodnie z warunkami wskazanymi w tabeli uwag.

Uwagi ogólne

W ocenie PIIT projekt ustawy oraz OSR nie uwzględniają w wystarczającym stopniu relacji projektowanych środków nadzorczych do obowiązującego reżimu ustawy o krajowym systemie cyberbezpieczeństwa. Szczegółowe uwagi do poszczególnych przepisów zostały przedstawione w tabeli uwag. Na poziomie ogólnym konieczne jest jednak wskazanie, że kwalifikowani dostawcy usług zaufania są już objęci szczególnym nadzorem w zakresie cyberbezpieczeństwa jako podmioty kluczowe.

Zgodnie z art. 5 ust. 1 pkt 4 lit. b ustawy o krajowym systemie cyberbezpieczeństwa kwalifikowany dostawca usług zaufania w rozumieniu art. 3 pkt 20 rozporządzenia 910/2014 stanowi, że podmiotem kluczowym jest podmiot niezależnie od wielkości podmiotu. Ponadto załącznik nr 1 do ustawy KSC wskazuje dostawców usług zaufania w sektorze infrastruktury cyfrowej. W konsekwencji kwalifikowani dostawcy usług zaufania podlegają obowiązkom przewidzianym dla podmiotów kluczowych, w tym obowiązkom zarządzania ryzykiem, obsługi incydentów, audytu, utrzymywania dokumentacji oraz zapewnienia ciągłości działania.

Zgodnie z art. 41 pkt 8 ustawy KSC organem właściwym do spraw cyberbezpieczeństwa dla sektora infrastruktury cyfrowej, z wyłączeniem komunikacji elektronicznej, jest minister właściwy do spraw informatyzacji. Oznacza to, że ten sam organ już obecnie posiada kompetencje nadzorcze wobec kwalifikowanych dostawców usług zaufania jako podmiotów kluczowych. Projekt ustawy o usługach zaufania powinien zatem jednoznacznie wyjaśniać, dlaczego istniejące

instrumenty nadzorcze wynikające z KSC są niewystarczające oraz jak projektowane środki mają być stosowane bez naruszenia spójności systemu nadzoru nad cyberbezpieczeństwem.

Istniejące mechanizmy KSC

Art. 53 ust. 5 ustawy KSC przyznaje organowi właściwemu szeroki zestaw środków nadzorczych wobec podmiotów kluczowych. Organ może m.in. nakazać podjęcie określonych czynności dotyczących obsługi incydentu, nakazać zaniechanie naruszeń, nakazać zapewnienie zgodności systemu zarządzania bezpieczeństwem informacji, nakazać poinformowanie odbiorców usług, nakazać wdrożenie zaleceń z audytu, wyznaczyć urzędnika monitorującego oraz nakazać podanie informacji do wiadomości publicznej. Są to narzędzia ukształtowane specjalnie dla nadzoru nad podmiotami kluczowymi i uwzględniające charakter cyberbezpieczeństwa, proporcjonalność działań oraz potrzebę utrzymania ciągłości usług.

Wprowadzenie dodatkowego, równoległego mechanizmu wstrzymania kwalifikowanej usługi zaufania, bez jasnego powiązania z mechanizmami KSC, może prowadzić do niespójności regulacyjnej i błędnych decyzji nadzorczych. Ryzyko to jest szczególnie istotne, ponieważ ustawa KSC nie traktuje podmiotów kluczowych wyłącznie jako podmiotów, które mają zapewniać jakość usług, ale także jako podmiotów, których usługi powinny być utrzymywane w sposób ciągły.

Art. 8 ust. 1 pkt 2 lit. f KSC wymaga wdrażania, dokumentowania, testowania i utrzymywania planów ciągłości działania umożliwiających ciągłe i niezakłócone świadczenie usługi, a także planów awaryjnych i planów odtworzenia działalności. Z kolei art. 8 ust. 1 pkt 5 lit. d KSC, nawet przy działaniach ograniczających skutki podatności lub cyberzagrożeń, nakazuje uwzględniać minimalizację skutków ograniczenia dostępności usług.

Ryzyko dla administracji i bezpieczeństwa obrotu

Kwalifikowane usługi zaufania są powszechnie wykorzystywane przez rynek i administrację publiczną. Kwalifikowani dostawcy usług zaufania świadczą usługi na rzecz organów administracji, ministerstw, systemów publicznych i procesów gospodarczych. Ich usługi są wykorzystywane m.in. przy kwalifikowanych pieczęciach elektronicznych, zabezpieczaniu doręczeń elektronicznych, wydawaniu i odbieraniu dokumentów przez urzędy, zapewnianiu bezpieczeństwa procesów wewnętrznych administracji publicznej oraz obsłudze wielu procesów sektora prywatnego.

Czasowe wyłączenie kwalifikowanej usługi zaufania może więc nie tylko ograniczyć działalność konkretnego dostawcy, ale także spowodować poważne zakłócenia w przepływie informacji, obsłudze dokumentów i funkcjonowaniu usług publicznych. Tego rodzaju decyzja powinna być poprzedzona planem działania, oceną skutków, analizą ciągłości działania oraz oceną wpływu na użytkowników i strony ufające.

Kierunek postulowanej zmiany

W związku z powyższym projekt powinien zostać zmieniony w kierunku całościowej rezygnacji z mechanizmu administracyjnego wstrzymania świadczenia kwalifikowanej usługi zaufania. W sytuacjach, w których źródłem ryzyka jest incydent, podatność, naruszenie bezpieczeństwa lub zagrożenie ciągłości działania, właściwą podstawą działania powinny być mechanizmy ustawy KSC, w szczególności art. 53 ust. 5, stosowane z uwzględnieniem obowiązku zapewnienia ciągłości działania wynikającego z art. 8 KSC.

Jeżeli projektodawca uzna, że dodatkowy mechanizm powinien zostać utrzymany w ustawie o usługach zaufania oraz identyfikacji elektronicznej, powinien on mieć charakter absolutnie wyjątkowy. W takim wariancie przepis powinien zawierać co najmniej następujące ograniczenia:

- jednoznaczne ograniczenie przesłanek do bezpośredniego, wykazanego i aktualnego zagrożenia bezpieczeństwa, którego nie można usunąć środkami mniej dolegliwymi;
- obowiązek wykazania w uzasadnieniu decyzji, że środki KSC oraz środki nadzoru eIDAS są niewystarczające;
- maksymalny łączny czas stosowania środka, bez możliwości faktycznie bezterminowego ponawiania decyzji;
- obowiązek przygotowania planu wykonania decyzji, obejmującego ciągłość działania, skutki dla klientów, stron ufających, administracji publicznej i rynku;
- doprecyzowanie, które czynności dostawcy mają zostać wstrzymane, a które muszą być kontynuowane, np. publikacja CRL, obsługa statusu certyfikatów, walidacja, archiwizacja dowodów i obowiązki informacyjne;
- realną, pilną kontrolę decyzji oraz możliwość wstrzymania jej wykonania w razie uprawdopodobnienia nieproporcjonalności lub ryzyka szkody nieodwracalnej.

Ryzyko konfliktu interesów

Projekt budzi również wątpliwości z perspektywy konfliktu interesów. Projektowany mechanizm pozwala ministrowi właściwemu do spraw informatyzacji wstrzymać kwalifikowaną usługę zaufania m.in. wtedy, gdy miałoby to służyć ochronie interesów innych dostawców usług zaufania. Jednocześnie minister właściwy do spraw informatyzacji, bezpośrednio lub przez podległe albo nadzorowane jednostki, realizuje zadania związane z usługami zaufania lub usługami opartymi o mechanizmy zaufania. W takim modelu dostawcy działający na rynku mogą pozostawać w relacji konkurencyjnej lub funkcjonalnie kolizyjnej wobec rozwiązań publicznych.

Przepis przyznający organowi możliwość wstrzymania usługi ze względu na interes innych dostawców powinien być skonstruowany wyjątkowo ostrożnie i zawierać silne gwarancje proceduralne, w tym wyłączenie arbitralności, wymóg wykazania bezpośredniego zagrożenia oraz mechanizmy kontroli decyzji. Niniejsza uwaga nie stanowi oceny sposobu działania obecnego rządu ani obecnego ministra właściwego do spraw informatyzacji. Chodzi o zasadę poprawnej legislacji: przepisy powinny być projektowane tak, aby działały prawidłowo niezależnie od tego, kto w danym czasie wykonuje władzę wykonawczą.

Uzupełnienie OSR

OSR powinien zostać uzupełniony o analizę relacji projektowanych przepisów do ustawy KSC, w szczególności do art. 5 ust. 1 pkt 4 lit. b, art. 8, art. 41 pkt 8 oraz art. 53 KSC. OSR powinien także wykazać, dlaczego istniejące środki nadzoru nad podmiotami kluczowymi są niewystarczające oraz jakie gwarancje zapewnią, że projektowany środek wstrzymania kwalifikowanej usługi zaufania nie doprowadzi do naruszenia ciągłości działania usług krytycznych dla administracji publicznej, rynku i bezpieczeństwa obrotu gospodarczego.

Tabela szczegółowych uwag

Poniższa tabela konsoliduje uwagi dotyczące tych samych przepisów. W przypadku mechanizmu wstrzymania usługi wskazano rekomendację podstawową, tj. rezygnację z mechanizmu i oparcie działań na KSC, oraz wariant alternatywny polegający na istotnym ograniczeniu środka.

Lp.	Podmiot zgłaszający	Artykuł, punkt, litera, akapit...	Opis uwagi	Uzasadnienie	Propozycja zmiany
1	PIIT	Uwagi ogólne do art. 30, art. 30b oraz OSR - relacja do KSC	Projekt i OSR nie wykazują, dlaczego istniejące środki nadzorcze wynikające z ustawy o krajowym systemie cyberbezpieczeństwa są niewystarczające wobec kwalifikowanych dostawców usług zaufania jako podmiotów kluczowych.	Kwalifikowany dostawca usług zaufania jest podmiotem kluczowym na podstawie art. 5 ust. 1 pkt 4 lit. b KSC, a organem właściwym dla sektora infrastruktury cyfrowej jest minister właściwy do spraw informatyzacji na podstawie art. 41 pkt 8 KSC. Art. 53 ust. 5 KSC daje szerokie narzędzia nadzorcze, w tym nakazy dotyczące obsługi incydentu, zgodności SZBI, wdrożenia zaleceń z audytu, informowania odbiorców usług oraz wyznaczenia urzędnika monitorującego.	Preferowane jest usunięcie projektowanego mechanizmu wstrzymania kwalifikowanej usługi zaufania i oparcie działań nadzorczych na mechanizmach KSC oraz eIDAS. Alternatywnie, jeżeli mechanizm zostanie utrzymany, musi zostać ograniczony przez gwarancje wskazane w dalszych uwagach: ścisłe przesłanki, maksymalny łączny czas, obowiązek oceny skutków i ciągłości działania, plan wykonania decyzji oraz realną kontrolę decyzji.
2	PIIT	OSR, pkt 7 / odwołanie do art. 46 pkt 13	OSR zawiera odwołanie do dodania art. 46 pkt 13, podczas gdy w projekcie ustawy ani w obowiązującym brzmieniu ustawy nie widać takiego przepisu. Jednocześnie OSR posługuje się nieprecyzyjnymi pojęciami „naruszeń" i „podatności".	Takie odwołanie utrudnia ocenę rzeczywistego zakresu projektowanej zmiany i może sugerować zamiar wprowadzenia dodatkowej sankcji lub obowiązku, którego nie ma w tekście projektu. W konsultacjach powinno być jasne, czy chodzi wyłącznie o uzasadnienie dla istniejących zmian, czy o odrębny projektowany przepis.	Doprecyzować OSR przez wskazanie właściwego przepisu projektu albo uzupełnić projekt o pełne brzmienie planowanego art. 46 pkt 13. Jeżeli intencją jest reakcja na podatności i naruszenia niebędące incydentami KSC, należy jednoznacznie zdefiniować zakres tych zdarzeń oraz ich konsekwencje prawne.
3	PIIT	Art. 1 pkt 3 projektu - art. 30 ust. 1 pkt 3 oraz ust. 2 ustawy	Uprawnienie organu nadzoru do wstrzymania świadczenia kwalifikowanej usługi zaufania jest ujęte zbyt szeroko. Przesłanki zastosowania środka są nieostre, a pojęcie „wstrzymania świadczenia kwalifikowanej usługi zaufania" nie określa, jakie czynności	Wstrzymanie usługi może mieć różne skutki w zależności od rodzaju usługi zaufania. Nie jest jasne, czy obejmuje ono np. publikację CRL, obsługę statusu certyfikatów, utrzymanie procesów walidacyjnych, obsługę wydanych pieczęci lub procesy działające po stronie klientów. Przepis dopuszcza ponawianie decyzji na kolejne okresy 14-dniowe bez maksymalnego łącznego limitu, co może	Sugerowana jest rezygnacja z tego mechanizmu na rzecz środków KSC. Alternatywnie należy doprecyzować zakres „wstrzymania" dla poszczególnych typów usług, wprowadzić maksymalny łączny okres stosowania środka, ograniczyć zastosowanie do bezpośredniego i wykazanego zagrożenia bezpieczeństwa oraz zobowiązać organ do wykazania, że środki mniej dolegliwe były niewystarczające.

Lp.	Podmiot zgłaszający	Artykuł, punkt, litera, akapit...	Opis uwagi	Uzasadnienie	Propozycja zmiany
			dostawca ma faktycznie zatrzymać i jakie obowiązki utrzymaniowe nadal wykonuje.	prowadzić do długotrwałego albo faktycznie bezterminowego wstrzymania usługi.	
4	PIIT	Art. 1 pkt 4 projektu - art. 30b ust. 1 i 2 ustawy	Projekt nadmiernie ogranicza prawo do skutecznej ochrony prawnej przez połączenie natychmiastowej wykonalności decyzji z wyłączeniem wniosku o ponowne rozpatrzenie sprawy oraz z wyłączeniem możliwości wstrzymania wykonania decyzji w trybie art. 61 § 2 pkt 1 p.p.s.a.	Dostawca może zostać pozbawiony realnej ochrony przed decyzją, która natychmiast wpływa na działalność operacyjną i relacje z klientami. Skarga do WSA, nawet w terminie 14 dni, nie zapewnia ochrony ex-ante. Problem pogłębia możliwość ponawiania decyzji o wstrzymaniu usługi.	Pozostawić możliwość złożenia wniosku o ponowne rozpatrzenie sprawy albo wprowadzić szczególny pilny tryb sądowej kontroli decyzji. Umożliwić wstrzymanie wykonania decyzji co najmniej wtedy, gdy dostawca uprawdopodobni rażącą nieproporcjonalność środka lub ryzyko szkody nieodwracalnej. Doprecyzować skutki zaskarżenia kolejnych decyzji przedłużających wstrzymanie.
5	PIIT	Art. 1 pkt 5 projektu - art. 32 ust. 3-7 ustawy	Projekt rozszerza możliwość wyznaczenia audytora organu nadzoru lub obserwatora organu nadzoru spośród określonych pracowników administracji. Istniejący art. 32 ust. 2 zawiera podstawowe reguły konfliktu interesów, ale nie przewiduje procedury ich praktycznej weryfikacji przez podmiot audytowany.	Osoba uczestnicząca w audycie może uzyskać dostęp do informacji technicznych, organizacyjnych i biznesowych dostawcy. Brak mechanizmu zgłaszania uzasadnionego sprzeciwu albo weryfikacji konfliktu interesów może rodzić ryzyko naruszenia interesu audytowanego podmiotu.	Dodać obowiązek złożenia przez audytora lub obserwatora oświadczenia o bezstronności, poufności i braku konfliktu interesów. Wprowadzić możliwość zgłoszenia przez podmiot audytowany uzasadnionego sprzeciwu wobec konkretnej osoby oraz obowiązek rozpatrzenia takiego sprzeciwu przed dopuszczeniem tej osoby do czynności.
6	PIIT	Art. 1 pkt 7 projektu - art. 39j ust. 3-7 ustawy	Regulacja dotycząca osób upoważnianych do kontroli w ramach krajowego schematu identyfikacji elektronicznej jest zbyt ogólna. Kryterium „wiedzy specjalistycznej i doświadczenia zawodowego” nie daje jasnych wymagań kompetencyjnych, a projekt nie przewiduje mechanizmu badania konfliktu interesów kontrolujących.	Kontrole w obszarze identyfikacji elektronicznej wymagają kompetencji technicznych, organizacyjnych i prawnych. Brak mierzalnych kryteriów może prowadzić do niejednolitej praktyki oraz kwestionowania ustaleń kontroli. Osoby kontrolujące mogą mieć dostęp do informacji wrażliwych, technicznych i biznesowych.	Wskazać minimalne kryteria kompetencyjne, np. akredytację, certyfikację, udokumentowane doświadczenie lub określony staż w obszarze usług zaufania, identyfikacji elektronicznej, cyberbezpieczeństwa albo audytu zgodności. Dodać obowiązek oświadczenia o poufności, bezstronności i braku konfliktu interesów oraz procedurę zgłaszania przez podmiot kontrolowany uzasadnionych zastrzeżeń.
7	PIIT	Art. 1 pkt 8 projektu - art. 39ja ustawy	Przepisy o wystąpieniu pokontrolnym i zaleceniach są zbyt ogólne. Projekt nie rozdziela jasno planu kontroli od projektu wystąpienia pokontrolnego, nie wymaga przypisania zaleceń do konkretnych wymagań oraz wyłącza środki odwoławcze od końcowego wystąpienia pokontrolnego.	Zalecenia pokontrolne powinny wynikać z konkretnych, możliwych do zweryfikowania wymagań prawnych lub normatywnych. Brak odwołania od końcowego wystąpienia jest szczególnie problematyczny, jeżeli dokument ten nakłada na podmiot kontrolowany konkretne obowiązki wykonania zaleceń.	Rozdzielić dokumenty: plan kontroli doręczany przed kontrolą oraz projekt wystąpienia pokontrolnego doręczany po kontroli. Każde stwierdzone naruszenie i każde zalecenie powinno zawierać referencję do konkretnego wymagania oraz odniesienie do stanowiska organu i stanowiska podmiotu kontrolowanego. Wprowadzić odwołanie albo szczególny tryb ponownej weryfikacji końcowego wystąpienia pokontrolnego.

Lp.	Podmiot zgłaszający	Artykuł, punkt, litera, akapit...	Opis uwagi	Uzasadnienie	Propozycja zmiany
8	PIIT	Art. 1 pkt 10 projektu - art. 39l ustawy	Wyłączenie stosowania art. 55 ust. 1 Prawa przedsiębiorców może spowodować, że kontrola w ramach krajowego schematu identyfikacji elektronicznej będzie mogła trwać bez realnego ustawowego limitu czasowego.	Brak limitu czasu kontroli zwiększa obciążenie organizacyjne podmiotu kontrolowanego i może prowadzić do nieproporcjonalnej ingerencji w działalność przedsiębiorcy.	Pozostawić stosowanie art. 55 ust. 1 Prawa przedsiębiorców albo wprowadzić sektorowy, jednoznaczny limit czasu kontroli wraz z warunkami jego przedłużenia i maksymalnym łącznym czasem kontroli.
10	PIIT	Uwagi ogólne do art. 30, art. 30b oraz OSR - relacja do KSC	Projekt i OSR nie wykazują, dlaczego istniejące środki nadzorcze wynikające z ustawy o krajowym systemie cyberbezpieczeństwa są niewystarczające wobec kwalifikowanych dostawców usług zaufania jako podmiotów kluczowych.	Kwalifikowany dostawca usług zaufania jest podmiotem kluczowym na podstawie art. 5 ust. 1 pkt 4 lit. b KSC, a organem właściwym dla sektora infrastruktury cyfrowej jest minister właściwy do spraw informatyzacji na podstawie art. 41 pkt 8 KSC. Art. 53 ust. 5 KSC daje szerokie narzędzia nadzorcze, w tym nakazy dotyczące obsługi incydentu, zgodności SZBI, wdrożenia zaleceń z audytu, informowania odbiorców usług oraz wyznaczenia urzędnika monitorującego.	Preferowane jest usunięcie projektowanego mechanizmu wstrzymania kwalifikowanej usługi zaufania i oparcie działań nadzorczych na mechanizmach KSC oraz eIDAS. Alternatywnie, jeżeli mechanizm zostanie utrzymany, musi zostać ograniczony przez gwarancje wskazane w dalszych uwagach: ścisłe przesłanki, maksymalny łączny czas, obowiązek oceny skutków i ciągłości działania, plan wykonania decyzji oraz realną kontrolę decyzji.