Minister
Finansów i Gospodarki

Warszawa, 3 listopada 2026 roku

Sprawa: Interpelacja nr 20374 P. Posła Janusza Kowalskiego w sprawie zagrożeń dla bezpieczeństwa i poufności danych gospodarczych przetwarzanych w Krajowym Systemie e- Faktur KSeF wynikających z mechanizmu anonimowego dostępu do faktur oraz wykorzystania infrastruktury zagranicznych dostawców usług informatycznych
Znak sprawy: DAK1.054.67.2026
Kontakt: Kancelaria MF
tel.: +48 22 694 55 55
e-mail: kancelaria@mf.gov.pl

**Sz. P. Włodzimierz Czarzasty**
Marszałek Sejmu
Kancelaria Sejmu
ul. Wiejska 4/6/8
00-902 Warszawa

# Odpowiedź na interpelację nr 20374 Pana Posła Janusza Kowalskiego

Szanowny Panie Marszałku,

W odpowiedzi na interpelację nr 20374 Pana Posła Janusza Kowalskiego w sprawie zagrożeń dla bezpieczeństwa i poufności danych gospodarczych przetwarzanych w Krajowym Systemie e-Faktur (KSeF) wynikających z mechanizmu anonimowego dostępu do faktur oraz wykorzystania infrastruktury zagranicznych dostawców usług informatycznych, Ministerstwo Finansów udziela następujących odpowiedzi.

tel.: +48 22 694 55 55
fax: +48 22 694 36 84
gov.pl/finanse
e-mail: kancelaria@mf.gov.pl

ul. Świętokrzyska 12
00-916 Warszawa

*Ad. 1-10*

***Jakimi przesłankami kierowało się Ministerstwo Finansów, wprowadzając mechanizm umożliwiający pobranie pełnej treści faktury bez uwierzytelnienia użytkownika, wyłącznie na podstawie pięciu danych identyfikujących dokument? Czy przed przyjęciem tego rozwiązania przeprowadzono analizę ryzyka nieuprawnionego dostępu do informacji gospodarczych i jakie były jej wyniki?***

***Czy Ministerstwo Finansów potwierdza, że dane wymagane do anonimowego pobrania faktury na podstawie § 8 wskazanego rozporządzenia odpowiadają informacjom udostępnianym w odpowiedziach na zapytania o metadane faktur za pośrednictwem API KSeF 2.0? Czy przeanalizowano ryzyko wykorzystania takich metadanych do uzyskania pełnej treści dokumentów z pominięciem standardowego mechanizmu uwierzytelniania?***

***Czy Ministerstwo Finansów przeprowadziło testy bezpieczeństwa sprawdzające możliwość pozyskania metadanych faktury przez podmiot trzeci, a następnie wykorzystania ich do anonimowego pobrania pełnego dokumentu? Jeżeli tak, kiedy przeprowadzono takie testy, kto był za nie odpowiedzialny i jakie stwierdzono zagrożenia?***

***Jakie mechanizmy zabezpieczające zastosowano w anonimowym dostępie do faktur, aby przeciwdziałać automatyzacji pobierania dokumentów, próbom masowego pozyskiwania danych oraz wielokrotnemu wykorzystywaniu tych samych informacji identyfikacyjnych? Czy system pozwala wykrywać i blokować nietypowe lub podejrzane próby pobierania faktur?***

***Czy każda operacja anonimowego wyszukania i pobrania faktury jest rejestrowana w systemie KSeF w sposób umożliwiający późniejszą identyfikację źródła żądania? Czy podatnik ma możliwość sprawdzenia, że jego faktura została pobrana w trybie anonimowym, a jeżeli nie, z jakich względów nie przewidziano takiej funkcjonalności?***

***Ile razy od uruchomienia KSeF 2.0 skorzystano z mechanizmu anonimowego pobierania faktur, o którym mowa w § 8 rozporządzenia? Ile odnotowano nieudanych prób wyszukania dokumentów, przypadków przekroczenia limitów zapytań oraz zdarzeń zakwalifikowanych jako podejrzane lub potencjalnie nieuprawnione próby dostępu?***

***Czy Ministerstwo Finansów konsultowało z właściwymi instytucjami odpowiedzialnymi za cyberbezpieczeństwo i bezpieczeństwo państwa ryzyko wykorzystania KSeF do pozyskiwania informacji o kontrahentach, cenach, strukturze dostaw oraz transakcjach przedsiębiorstw działających w sektorach strategicznych, w szczególności w przemyśle obronnym, energetycznym i telekomunikacyjnym? Jakie wnioski sformułowano w wyniku tych konsultacji?***

***Czy Ministerstwo Finansów rozważa zastąpienie obecnego mechanizmu anonimowego dostępu rozwiązaniem wykorzystującym dodatkowe, niezależne i możliwe do unieważnienia poświadczenie, którego nie można odtworzyć na podstawie metadanych faktury? Jeżeli nie, jakie argumenty przemawiają za utrzymaniem obecnego rozwiązania?***

***Czy Ministerstwo Finansów zamierza przeprowadzić ponowną, kompleksową ocenę bezpieczeństwa KSeF 2.0, uwzględniającą możliwość wykorzystania metadanych do nieuprawnionego pobierania faktur przez podmioty trzecie, w tym operatorów infrastruktury pośredniczącej? Jeżeli tak, w jakim terminie zostanie przeprowadzona taka ocena, czy jej wyniki zostaną przedstawione opinii publicznej oraz jakie działania naprawcze przewidziano w przypadku potwierdzenia wskazanych zagrożeń?***

***Czy Ministerstwo Finansów potwierdza, że infrastruktura pośrednicząca wykorzystywana w KSeF 2.0, w tym rozwiązania firmy Imperva, uczestniczy w terminacji połączeń TLS obsługujących API KSeF i może na poziomie technicznym przetwarzać niezabezpieczone dodatkowym szyfrowaniem aplikacyjnym treści żądań i odpowiedzi HTTP? Czy przeprowadzono ocenę możliwości uzyskania przez operatora tej infrastruktury dostępu do metadanych faktur, pełnej treści pojedynczych faktur oraz danych uwierzytelniających? Jeżeli tak, jakie kategorie zabezpieczeń technicznych, organizacyjnych i kontraktowych zastosowano w celu ograniczenia tych zagrożeń, bez konieczności ujawniania szczegółów konfiguracji bezpieczeństwa systemu?***

Ministerstwo Finansów informuje, że na etapie prac nad systemem została przeprowadzona kompleksowa analiza ryzyka odnosząca się do bezpieczeństwa KSeF. W oparciu o tę analizę, wdrożono odpowiednie mechanizmy uwierzytelnienia w systemie oraz modele nadawania uprawnień do korzystania z KSeF, które zabezpieczają dane znajdujące się w KSeF przed nieuprawnionym dostępem.

Dostęp do faktur znajdujących się w KSeF możliwy jest na dwa sposoby. Pierwsza metoda polega na uwierzytelnieniu się w systemie przez podatnika lub osoby przez niego uprawnionej do dostępu do faktur np. certyfikatem kwalifikowanym, certyfikatem KSeF lub Węzłem krajowym.

Druga metoda polega na dostępie do faktur w sposób niewymagający uwierzytelnienia w systemie. Rozporządzenie przewiduje w tym zakresie dwie opcje – z wykorzystaniem kodu QR lub bez niego.

Pierwsza opcja - określona w § 7 rozporządzenia Ministra Finansów i Gospodarki z 12 grudnia w sprawie korzystania z Krajowego systemu e-Faktur[1] polega na tym, że nabywca po zeskanowaniu QR kodu, uzyska informację czy dana faktura została wystawiona w KSeF (etap 1 dostępu). W kolejnym kroku nabywca może pobrać fakturę z KSeF (etap 2 dostępu). Konieczne jest podanie w tym celu, danych z faktury tj.:

- numeru faktury,
- identyfikatora podatkowego nabywcy lub informacji o jego braku,

[1] Dz. U. z 2025 r. poz. 1815 ze zm.

- kwoty należności ogółem.

Druga opcja – określona w § 8 ww. rozporządzenia umożliwia dostęp do faktury lub w KSeF po podaniu poniższego zestawu danych:

- numeru KSeF faktury,
- numeru faktury nadanego przez podatnika,
- numeru NIP lub innego identyfikatora nabywcy towarów lub usług, albo informacji o jego braku,
- imienia i nazwiska lub nazwy nabywcy towarów lub usług albo informacji o braku tych danych,
- kwoty należności ogółem.

Wprowadzenie mechanizmu umożliwiającego pobranie faktury bez konieczności uwierzytelnienia się użytkownika było podyktowane potrzebą zapewnienia dostępu do faktury w KSeF dla osób i podmiotów, które nie posługują się numerem identyfikacji podatkowej, a tym samym nie mają możliwości zalogowania się do systemu tj. np. dla osób fizycznych nieprowadzących działalności gospodarczej lub podmiotów zagranicznych. Mowa tu jest generalnie o nabywcach, którym faktura jest wydawana w sposób uzgodniony (zgodnie z art. 106gb ust. 4 ustawy o VAT).

Zdefiniowanie katalogu danych wymaganych do uzyskania dostępu do faktury było poprzedzone analizą odnoszącą się do ryzyk i kwestii bezpieczeństwa tego rozwiązania.

W ocenie Ministerstwa Finansów przewidziana w rozporządzeniu możliwość pobrania faktury w sposób anonimowy spełnia więc swoją rolę. Kwestie związane z zapewnieniem odpowiedniego poziomu bezpieczeństwa tej usługi są monitorowane. W związku z powyższym w ocenie Ministerstwa Finansów wprowadzenie wskazanych w treści interpelacji działań naprawczych nie jest zasadne.

Ministerstwo Finansów informuje, że KSeF 2.0 został zbudowany w najwyższym standardzie technicznym i organizacyjnym, z uwzględnieniem najlepszych praktyk rynkowych oraz uznanych norm bezpieczeństwa. Architektura systemu została zaprojektowana w sposób zapewniający wysoką dostępność, w szczególności poprzez zastosowanie mechanizmów redundancji, eliminację pojedynczych punktów awarii oraz ciągłe monitorowanie kluczowych komponentów infrastruktury. KSeF był regularnie poddawany licznym i cyklicznym testom, w tym testom wydajnościowym, bezpieczeństwa oraz odporności na awarie. Został także przetestowany w zakresie cyberbezpieczeństwa. System gwarantuje integralność danych dzięki zastosowaniu mechanizmów kontroli, walidacji danych, szyfrowania oraz rejestrowania zdarzeń (audytów). Dostęp do danych jest realizowany zgodnie z zasadą najmniejszych uprawnień, a wszystkie operacje są wykonywane w kontrolowanym i zabezpieczonym środowisku.

Mechanizmy związane z zapewnieniem bezpieczeństwa dotyczą całego systemu oraz wszystkich jego użytkowników, a nie tylko konkretnych branż lub sektorów.

Informacje dotyczące architektury technicznej oraz bezpieczeństwa systemów stanowiących kluczowe elementy infrastruktury IT administracji publicznej nie są publicznie ujawniane. Publicznie komunikowane są wyłącznie ogólne zasady

funkcjonowania takich systemów, natomiast detale operacyjne pozostają objęte ograniczeniami informacyjnymi ze względów bezpieczeństwa. Komunikowanie informacji technicznych mogłoby osłabić poziom ochrony systemów IT administracji publicznej.

Z wyrazami szacunku

Z upoważnienia Ministra Finansów i Gospodarki

**Zbigniew Stawicki**
Podsekretarz Stanu Zastępca Szefa Krajowej Administracji Skarbowej

w Ministerstwie Finansów