Minister
Finansów i Gospodarki

Warszawa, 4 marca 2026 roku

Sprawa: Sprawa: Interpelacja nr 15213 w sprawie ujawnienia ryzyk związanych z Krajowym Systemem e-Faktur oraz podjęcia pilnych działań korygujących i naprawczych
Znak sprawy: DAK1.054.25.2026
Kontakt: Kancelaria MF
tel.: +48 22 694 55 55
e-mail: kancelaria@mf.gov.pl

Pan
Włodzimierz Czarzasty
Marszałek Sejmu
Rzeczpospolitej Polskiej

Odpowiedź na Interpelację nr 15213 Posła Krzysztof Tuduj w sprawie ujawnienia ryzyk związanych z Krajowym Systemem e-Faktur oraz podjęcia pilnych działań korygujących i naprawczych

Szanowny Panie Marszałku,

Ministerstwo Finansów w odpowiedzi na pytania zawarte w interpelacji nr 15213 przedstawia wyjaśnienia:

Czy przeprowadzono niezależne audyty bezpieczeństwa oraz testy penetracyjne KSeF obejmujące scenariusze ataków na dużą skalę, w tym próby przejęcia lub wycieku danych o znaczeniu strategicznym dla Państwa Polskiego, np. w sektorze obronnym lub infrastruktury krytycznej, a jeżeli tak, to kiedy i jakie audyty zostały zweryfikowane i jakimi procedurami zostały udokumentowane?

W trakcie projektowania i tworzenia KSeF był regularnie poddawany licznym testom, w tym testom wydajnościowym, bezpieczeństwa i testom funkcjonalnym. Szczególny nacisk położono na testy cyberbezpieczeństwa.
W celu zachowania odpowiedniego poziomu bezpieczeństwa systemów informatycznych resortu finansów oraz danych w nich przetwarzanych, szczegółowe informacje w tym zakresie nie są upubliczniane.

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

Czy istnieje lub powstanie w najbliższym czasie, a jeżeli tak, to kiedy, plan awaryjny na wypadek wycieku danych krytycznych z perspektywy bezpieczeństwa państwowego lub plan wyłączenia z KSeF podmiotów o znaczeniu strategicznym?

KSeF stanowi kluczowy element infrastruktury informatycznej administracji publicznej, wspierający realizację istotnych zadań państwa. W celu zachowania odpowiedniego poziomu bezpieczeństwa systemów informatycznych resortu finansów oraz danych w nich przetwarzanych nie udzielamy szczegółowych informacji w tym zakresie.

Jakie mechanizmy bezpieczeństwa, kontroli dostępu oraz pełnego rejestrowania operacji (audit trail) zostały wdrożone w KSeF, aby uniemożliwić nieuprawnionym osobom trzecim przeglądanie lub pobieranie faktur na podstawie znanych parametrów (takich jak numer KSeF, NIP nabywcy czy wartość faktury) i kodu QR? Jakie konkretne rozwiązania techniczne, organizacyjne i prawne zostały wdrożone w KSeF w celu zabezpieczenia danych przedsiębiorców przed nieuprawnionym dostępem, w szczególności przed atakami hakerskimi oraz nadużyciami ze strony nieuczciwych kontrahentów? Czy przedsiębiorca będzie każdorazowo informowany o próbach dostępu do danych dotyczących jego działalności?

KSeF jest oparty na modelu poświadczeń, tzn. że wymagane jest uwierzytelnienie i autoryzacja danej osoby lub podmiotu w systemie. Po uwierzytelnieniu się w systemie dana osoba lub podmiot korzysta z KSeF w zakresie posiadanych przez siebie uprawnień. Oznacza to, że tylko osoba posiadająca właściwe uprawnienie po dokonanym wcześniej prawidłowo uwierzytelnieniu może korzystać z KSeF. Zatem jedynie uprawnione osoby posiadające właściwe narzędzia w zakresie posiadanych uprawnień będą miały dostęp do KSeF.

W przypadku dostępu anonimowego aby posiadać dostęp do faktury w KSeF należy być w posiadaniu faktury z kodem QR lub samego kodu QR (analogicznie linku weryfikacyjnego), a na etapie dodatkowego uwierzytelnienia należy podać dodatkowe dane odnoszące się do treści weryfikowanej faktury. Zatem nie posiadając danych o tej fakturze nie ma możliwości anonimowego dostępu do tego dokumentu. System KSeF nie generuje powiadomień informujących o uwierzytelnieniu się danej osoby do KSeF.

KSeF stanowi kluczowy element infrastruktury informatycznej administracji publicznej, wspierający realizację istotnych zadań państwa. Z uwagi na jego rolę, system został zaprojektowany zgodnie z ustawą o krajowym systemie cyberbezpieczeństwa i podlega najwyższym standardom bezpieczeństwa.

W celu zachowania odpowiedniego poziomu bezpieczeństwa systemów informatycznych resortu finansów oraz danych w nich przetwarzanych nie udzielamy szczegółowych informacji w tym zakresie.

Jakie konkretne procedury prawne i techniczne przewidziano w sytuacji wystawienia w KSeF faktury dokumentującej transakcję, która w rzeczywistości nie miała miejsca lub została anulowana, w szczególności gdy odbiorca faktury nie ma możliwości jej odrzucenia ani zakwestionowania w systemie, a faktura posiada status autentycznej i integralnej - zgodnie z art. 106m ust. 5 pkt 3 ustawy o podatku od towarów i usług (Dz. U. 2004 Nr 54 poz. 535)?

W jaki sposób Ministerstwo Finansów zamierza chronić podatników przed wykorzystaniem KSeF jako narzędzia do prób wyłudzeń zapłaty, w sytuacji gdy faktura wystawiona w systemie może zostać użyta jako autentyczny dowód istnienia rzekomego zobowiązania, mimo braku rzeczywistej transakcji gospodarczej - zgodnie z art. 106m ust. 5 pkt 3 ustawy o podatku od towarów i usług (Dz. U. 2004 Nr 54 poz. 535)?

W przypadku faktur dokumentujących transakcję, która w rzeczywistości nie miała miejsca, co do której istnieje uzasadnione przypuszczenie, że jest ona np. wynikiem oszustwa, odbiorca ma obecnie możliwość skorzystania z mechanizmu zgłaszania nadużycia (tzw. faktury scamowej), która jest dostępna z poziomu formularza kontaktowego a w późniejszym czasie będzie dostępna w ramach dedykowanej funkcjonalności systemu KSeF 2.0 z poziomu poszczególnej faktury.

W jaki sposób system KSeF oraz przepisy wykonawcze przewidują audyt działań poszczególnych użytkowników i przypisywanie odpowiedzialności do konkretnej osoby w przypadku posługiwania się certyfikatem firmowym?

Właściwe zarządzanie kwalifikowaną pieczęcią elektroniczną jest wyłączną kompetencją przedsiębiorcy (właściciela tej pieczęci). Ministerstwo Finansów ani KSeF nie ma możliwości weryfikacji procesu udostępniania pieczęci kwalifikowanej pracownikom czy innym osobom. Kluczowe w tym przypadku jest maksymalne zabezpieczenie pieczęci, a także wygenerowanych na jej podstawie tokenów czy Certyfikatów KSeF.

Czy i kiedy planowane jest wprowadzenie mechanizmów śledzenia i rejestracji operacji w sposób pozwalający na identyfikację faktycznego użytkownika wykorzystującego certyfikat firmy w danym momencie?

Nie jest planowane wdrożenie narzędzi śledzących procesy i mechanizmy identyfikujących faktycznego użytkownika działającego na podstawie pieczęci kwalifikowanej.

Faktura wystawiona po uwierzytelnieniu się użytkownika za pomocą pieczęci kwalifikowanej jest widoczna w systemie jako wystawiana przez ten podmiot. Jak już wyżej wskazano, to po stronie użytkowników jest zabezpieczenie procesu udostępniania pieczęci, a także wygenerowanych na jej podstawie tokenów oraz Certyfikatów KSeF osobom trzecim.

Czy i jakie analizy wpływu na mikroprzedsiębiorców, osoby prowadzące działalność nierejestrowaną oraz małe firmy zostały przeprowadzone w związku z obowiązkiem korzystania z KSeF oraz jakie konkretne działania osłonowe lub uproszczenia planuje wprowadzić rząd, aby zapobiec wzrostowi tzw. szarej strefy i rezygnacji z legalnego prowadzenia działalności gospodarczej?

Zgodnie z przepisami epizodycznymi do końca 2026 r. podatnicy obowiązani do wystawiania faktur ustrukturyzowanych będą mogli wystawiać faktury elektroniczne lub faktury w postaci papierowej, jeżeli łączna wartość sprzedaży (wraz z podatkiem) udokumentowana tymi fakturami wystawionymi w danym miesiącu będzie mniejsza lub równa 10 000 zł. Należy wskazać również, że do końca 2026 r. podatnicy obowiązani do wystawiania faktur ustrukturyzowanych będą mogli wystawiać faktury elektroniczne lub faktury w postaci papierowej przy zastosowaniu kas rejestrujących i paragony fiskalne uznane za faktury (do 450 zł). Należy podkreślić, że do końca 2026 roku nie będą wyciągane konsekwencje w stosunku do przedsiębiorców za błędne stosowanie KSeF.

Etapowe wdrożenie KSeF stanowiło odpowiedź na potrzebę elastycznego wdrożenia tego systemu. Wypracowane, finalne rozwiązania prawne, techniczne i biznesowe są efektem szerokich konsultacji przeprowadzonych w 2024 i 2025 r. z udziałem rynku, w tym podatników, branży IT, księgowych, przedstawicieli JST, oraz organizacji zrzeszających przedsiębiorców. W konsultacjach wzięło udział 10 tysięcy podmiotów. Były to największe, przeprowadzone w historii resortu finansów konsultacje rozwiązań prawnych i biznesowych.

W przygotowanych rozwiązaniach uwzględniono większość postulatów zgłoszonych w toku konsultacji. Szczegółowe odniesienie do wszystkich zgłoszonych postulatów zostało przedstawione w raportach z konsultacji, które są publicznie dostępne pod adresem:
https://legislacja.rcl.gov.pl/projekt/12391205/katalog/13092624#13092624

Czy w ministerstwie wiodącym w tej kwestii przewidziano jak ogromne bazy danych będą konieczne dla systemu KSeF i czy jest w stanie zagwarantować ich bezawaryjne utrzymanie oraz bieżącą obsługę, bez częstych problemów technicznych, które będą paraliżowały obrót gospodarczy?

System KSeF jest zbudowany w najwyższym standardzie technicznym i organizacyjnym, z uwzględnieniem najlepszych praktyk rynkowych, spełniając normy 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 infrastruktur.

Informacje dotyczące architektury technicznej 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.

Czy Pan Minister rozważa odroczenie obowiązków wynikających z systemu KSeF po stronie podatników do czasu wyjaśnienia zagadnień bezpieczeństwa technicznego i proceduralnego obejmującego także finansowanie terroryzmu oraz pranie brudnych pieniędzy, jak również ustanowienia mechanizmów bezpieczeństwa prawnego dla stron obrotu gospodarczego i bezpieczeństwa danych wrażliwych Państwa Polskiego?

W ocenie Ministerstwa Finansów obecne mechanizmy weryfikacji spełniają swoją rolę (zostały one opisane w odpowiedzi na pytanie nr 3).

Dostęp do danych znajdujących się w KSeF został umocowany w obowiązujących przepisach prawa. W oparciu o art. 297h ustawy Ordynacji podatkowa posiadają uprawnione do tego organy. Dostęp do danych znajdujących się w KSeF dla pracowników administracji skarbowej jest możliwy w ściśle określonych, uzasadnionych sytuacjach.

Każdorazowy wgląd do danej faktury przez uprawnionego pracownika jest na bieżąco monitorowany w systemie, opatrzony wyraźnymi zgodami przełożonych – po uprzednim uzasadnieniu w celu poboru danych oraz jest cyklicznie audytowany.

Ministerstwo Finansów podkreśla, że zapewnia bezpieczeństwo informacji, w tym informacji przetwarzanych we wszystkich systemach teleinformatycznych w Resorcie Finansów, które odbywa się na podstawie przepisów prawa, w szczególności Ordynacji podatkowej, ustawy o ochronie danych osobowych i RODO oraz regulacji wewnętrznych. W Resorcie Finansów wdrożono system zarządzania bezpieczeństwem informacji. Należy również zwrócić uwagę, że dane w systemie KSeF stanowią tajemnicę skarbową i każdy pracownik w KAS jest zobowiązany do jej przestrzegania zgodnie z obowiązującymi przepisami prawa.

Wypracowane przez KAS procedury związane z uzyskaniem dostępu do faktur ustrukturyzowanych, poparte regulacjami dotyczącymi zachowania tajemnicy skarbowej oraz wdrożonymi politykami zapewniają ochronę danych zgromadzonych w KSeF. System został wdrożony z zastosowaniem adekwatnych środków technicznych i organizacyjnych zapewniających poufność, integralność i dostępność przetwarzanych danych.

Z wyrazami szacunku

Z upoważnienia Ministra Finansów i Gospodarki

Zbigniew Stawicki
Podsekretarz Stanu Zastępca Szefa Krajowej Administracji Skarbowej

w Ministerstwie Finansów