Warszawa, 20 listopada 2025 r.

KSeF a RODO – nowe wyzwania w ochronie danych osobowych

Wraz z obowiązkowym wdrożeniem Krajowego Systemu e-Faktur (KSeF) od 2026 roku przedsiębiorcy staną przed nie tylko podatkową, ale przede wszystkim organizacyjną i prawną zmianą w obszarze ochrony danych osobowych.
KSeF, jako centralny system zarządzany przez Ministerstwo Finansów, stanie się nowym i istotnym procesem przetwarzania danych – obejmującym dane setek tysięcy osób fizycznych prowadzących działalność gospodarczą.

Dane osobowe w KSeF – co naprawdę trafia do systemu

Choć faktura jest dokumentem księgowym, w wielu przypadkach zawiera dane pozwalające na identyfikację osoby fizycznej. Dotyczy to w szczególności jednoosobowych działalności gospodarczych, gdzie dane przedsiębiorcy są jednocześnie danymi osobowymi w rozumieniu art. 4 pkt 1 RODO.
W KSeF przekazywane będą m.in.:

- imię i nazwisko przedsiębiorcy,
- adres prowadzenia działalności,
- numer NIP,
- dane kontaktowe (jeśli widnieją na fakturze).

Te dane – po przesłaniu faktury – trafiają do centralnej bazy Ministerstwa Finansów, gdzie będą przechowywane przez okres 10 lat.

KSeF w rejestrze czynności przetwarzania (RCP)

Z punktu widzenia ochrony danych osobowych, wprowadzenie KSeF wymaga aktualizacji wewnętrznej dokumentacji RODO.
Każdy przedsiębiorca powinien w swoim Rejestrze Czynności Przetwarzania (RCP) ująć nową pozycję: „Przetwarzanie danych osobowych w związku z wystawianiem i przesyłaniem faktur ustrukturyzowanych w systemie KSeF".
W tym dokumencie należy określić m.in.:

- cel przetwarzania (wypełnienie obowiązków podatkowych),
- kategorie osób, których dane dotyczą (kontrahenci, osoby reprezentujące kontrahentów),
- zakres danych,
- podstawę prawną (art. 6 ust. 1 lit. c RODO – obowiązek prawny),
- okres przechowywania (zgodnie z przepisami podatkowymi – 10 lat),
- odbiorców danych (Ministerstwo Finansów, ewentualnie biuro rachunkowe).

Dualizm administratorów danych – kto za co odpowiada?

W systemie KSeF występuje dwupoziomowa odpowiedzialność za dane:

- Przedsiębiorca (wystawca faktury) – pełni rolę administratora danych swoich kontrahentów, odpowiadając za zgodność procesu fakturowania z RODO w obrębie własnej organizacji (np. kto ma dostęp do faktur, jak są one przesyłane, czy dane są poprawne).
- Ministerstwo Finansów – pełni rolę odrębnego administratora danych, przetwarzając dane w systemie centralnym w oparciu o ustawowy obowiązek.

Ten model oznacza, że nie ma tu klasycznego powierzenia danych, lecz dwóch niezależnych administratorów, z których każdy odpowiada za własną sferę przetwarzania.

Ryzyka z perspektywy RODO

Centralizacja danych w KSeF generuje szereg potencjalnych zagrożeń dla prywatności i bezpieczeństwa informacji. Do najczęściej wskazywanych należą:

- ryzyko nadmiernego dostępu – zbyt szeroki krąg pracowników uprawnionych do podglądu lub pobierania faktur,
- brak kontroli nad uprawnieniami po stronie przedsiębiorcy (np. byłych pracowników, biur rachunkowych),
- niewystarczające procedury reagowania na incydenty,
- błędy ludzkie podczas wprowadzania lub pobierania danych,
- możliwość nieuprawnionego ujawnienia danych osobom trzecim.

Z punktu widzenia RODO kluczowe jest, aby przedsiębiorca mógł wykazać, że podjął odpowiednie środki techniczne i organizacyjne, zgodnie z zasadą rozliczalności (art. 5 ust. 2 RODO).

Jak przygotować firmę do KSeF w świetle RODO?

Przygotowanie do obowiązkowego korzystania z KSeF powinno obejmować nie tylko wdrożenie rozwiązań informatycznych, ale również aktualizację procedur ochrony danych.
Rekomendowane działania to:

- aktualizacja dokumentacji – wprowadzenie nowego procesu do RCP i polityki ochrony danych,
- nadanie uprawnień dostępu według zasady minimalizacji – dostęp do faktur tylko dla osób, którym jest on niezbędny,
- wprowadzenie rejestru uprawnień do KSeF – ewidencjonowanie, kto ma dostęp do systemu i w jakim zakresie,
- przeszkolenie personelu – zwłaszcza działów księgowych, administracyjnych i współpracujących biur rachunkowych,
- wdrożenie procedury reagowania na incydenty – obejmującej sposób postępowania w przypadku naruszenia ochrony danych,
- zawarcie umów powierzenia przetwarzania danych z podmiotami, które pomagają w obsłudze faktur (np. biura rachunkowe, operatorzy IT),
- okresowy przegląd bezpieczeństwa – weryfikacja konfiguracji kont, certyfikatów i systemów komunikacji z KSeF.

Podstawa prawna przetwarzania danych w KSeF

Wystawianie i przekazywanie faktur ustrukturyzowanych odbywa się na podstawie przepisów prawa podatkowego. Dlatego podstawą prawną przetwarzania danych osobowych w tym procesie jest art. 6 ust. 1 lit. c RODO – przetwarzanie jest niezbędne do wypełnienia obowiązku prawnego ciążącego na administratorze. Nie ma więc potrzeby uzyskiwania zgody od osób, których dane widnieją na fakturze. Przedsiębiorca jednak ma obowiązek poinformować kontrahentów o przetwarzaniu danych – może go realizować np. poprzez klauzulę RODO w umowie lub na fakturze.

Wnioski

Wdrożenie KSeF to nie tylko zmiana technologiczna w fakturowaniu, ale nowy, długoterminowy proces przetwarzania danych osobowych, który musi być ujęty w systemie ochrony danych każdej firmy.

Warto potraktować KSeF jako okazję do uporządkowania polityk ochrony danych, weryfikacji dostępów i przeszkolenia personelu, zanim system stanie się obowiązkowy.
Dobrze przygotowana organizacja nie tylko uniknie ryzyka naruszeń RODO i potencjalnych kar, ale też zyska lepszą kontrolę nad przepływem danych – co w dobie cyfryzacji staje się jednym z filarów odpowiedzialnego zarządzania przedsiębiorstwem.

Maria Lothamer – ekspert ds. ochrony danych osobowych, Wiceprezes Zarządu w iSecure Sp. z o.o.