Warszawa, 10 marca 2026 r.

KSeF po 1 lutego 2026 r. – pierwsze błędy, nowe ryzyka i co to oznacza dla RODO

1 lutego 2026 r. najwięksi przedsiębiorcy zostali objęci obowiązkiem wystawiania faktur wyłącznie przez **Krajowy System e-Faktur (KSeF)**. Choć system był zapowiadany od wielu miesięcy, a firmy miały czas na przygotowanie, pierwsze tygodnie funkcjonowania przyniosły szereg problemów technicznych i organizacyjnych. Co istotne – część z nich ma bezpośrednie konsekwencje w obszarze ochrony danych osobowych i zgodności z **RODO**.
Poniżej przedstawiam podsumowanie najważniejszych zjawisk po starcie KSeF oraz ich realne znaczenie z perspektywy bezpieczeństwa danych osobowych.

Problemy z logowaniem i uwierzytelnianiem – ryzyko organizacyjne, nie systemowe

W pierwszych dniach obowiązywania systemu przedsiębiorcy zgłaszali trudności z logowaniem przy użyciu **profilu zaufanego**. Pojawiały się komunikaty o błędach uwierzytelnienia, chwilowej niedostępności czy przeciążeniu systemu.
Warto podkreślić: nie był to problem bezpieczeństwa samego KSeF, lecz przeciążenia infrastruktury uwierzytelniającej.
Dlaczego to ma znaczenie dla RODO?
W wielu firmach w reakcji na trudności:

- zaczęto korzystać z kont współdzielonych,
- nadawano uprawnienia „na wszelki wypadek”,
- pomijano formalną ewidencję dostępu.

Nie doszło tu do „wycieku” danych w sensie technicznym, ale powstało realne ryzyko nadmiernego dostępu do danych osobowych. A to już może stanowić naruszenie zasad minimalizacji i integralności danych.

Błędy integracji i walidacji faktur – zagrożenie poza KSeF

Pierwsze tygodnie pokazały, że największym wyzwaniem jest integracja systemów ERP z KSeF. Pojawiały się następujące problemy:

- odrzucenia faktur z powodu błędów w strukturze XML,
- niezgodność faktur z obowiązującym wzorem KSeF,
- rozbieżności między środowiskiem testowym a produkcyjnym.

Sam fakt odrzucenia faktury nie oznacza naruszenia danych. Problem pojawia się „po drodze”. Gdzie powstaje ryzyko RODO?

- w logach systemowych zawierających pełne dane osobowe,
- w przesyłaniu plików XML do dostawców oprogramowania,
- w środowiskach testowych, które nie są zabezpieczone jak produkcyjne.

To oznacza, że zagrożenie nie leży w centralnym systemie, lecz w wewnętrznych procesach przedsiębiorstw.

Zarządzanie uprawnieniami – największe ryzyko praktyczne

Najpoważniejszym problemem po starcie KSeF okazało się nadawanie uprawnień. W wielu firmach:

- generowano tokeny dostępu bez kontroli zakresu,
- nie cofano uprawnień byłym pracownikom,
- nie prowadzono rejestru osób mających dostęp do faktur.

A dostęp do faktur oznacza dostęp do danych osobowych kontrahentów, w tym jednoosobowych działalności gospodarczych (adresy, NIP, dane kontaktowe). Z perspektywy RODO to realne ryzyko nieuprawnionego ujawnienia danych – nawet jeśli dane nie opuściły systemu, ale dostęp miała osoba bez uzasadnionej potrzeby.

Co z bezpieczeństwem samego systemu?

Zgodnie z komunikatami **Ministerstwo Finansów**:

- dane są przetwarzane na serwerach w Polsce,
- system przeszedł testy bezpieczeństwa,
- zakres danych nie jest większy niż w dotychczasowych fakturach.

Nie ma obecnie informacji o naruszeniach bezpieczeństwa na poziomie centralnym. Jednak odpowiedzialność za politykę dostępu, konfigurację ERP i procedury wewnętrzne spoczywa wyłącznie na przedsiębiorcach.

Brak kar podatkowych nie jest tożsamy z brakiem odpowiedzialności

Ministerstwo zapowiedziało brak sankcji podatkowych do końca 2026 r. za niektóre błędy związane z wdrożeniem KSeF. To jednak nie dotyczy RODO. Jeśli dojdzie do naruszenia ochrony danych osobowych:

- administrator ma 72 godziny na zgłoszenie do UODO,
- w niektórych przypadkach musi poinformować osoby, których dane dotyczą,
- może ponieść administracyjną karę pieniężną.

Odpowiedzialność w tym zakresie jest regulowana na poziomie RODO oraz krajowych przepisów dotyczących ochrony danych osobowych.

Co przedsiębiorcy powinni zrobić teraz?

- przeprowadzić audyt uprawnień w KSeF,
- wprowadzić zasadę minimalnego dostępu,
- uporządkować procedury nadawania i cofania dostępów,
- zweryfikować sposób przechowywania logów i danych testowych,
- przeszkolić pracowników z zasad przetwarzania danych w KSeF.

Podsumowanie

Wprowadzenie obowiązkowego KSeF oznacza utworzenie kolejnego, scentralizowanego repozytorium danych gospodarczych i osobowych. Z perspektywy ochrony danych trudno uznać to za neutralne zdarzenie. Im więcej miejsc, w których dane są przetwarzane, tym większy obszar potencjalnego ryzyka – niezależnie od zapewnień o testach bezpieczeństwa czy zabezpieczeniach infrastruktury.

Ostateczne ryzyko zależy nie tylko od jakości zabezpieczeń systemowych, ale również od praktyki nadawania uprawnień, integracji systemów i kontroli dostępu w firmach. To właśnie kumulacja tych czynników zdecyduje, czy KSeF okaże się bezpiecznym narzędziem, czy kolejnym punktem podatnym na nadużycia.

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