**UCHWAŁA NR 43/2026**

**ZARZĄDU ZWIĄZKU ZACHODNIOPOMORSKIEJ STREFY CENTRALNEJ**

z dnia 19 stycznia 2026r.

**w sprawie wprowadzenia instrukcji zarządzania uprawnieniami w ramach Krajowego Systemu e-Faktur w Związku Zachodniopomorskiej Strefy Centralnej**

Na podstawie §21 Statutu Związku Zachodniopomorskiej Strefy Centralnej (tekst jednolity Dz. Urz. Woj. Zachodniopomorskiego z 2025r. poz. 3625) zarządza się, co następuje:

**§ 1.** Wprowadza się instrukcję zarządzania uprawnieniami w ramach Krajowego Systemu e-Faktur w Związku Zachodniopomorskiej Strefy Centralnej, określoną w załączniku nr 1 do niniejszej uchwały.

**§ 2.** Wykonanie uchwały powierza się Przewodniczącej Zarządu Związku Zachodniopomorskiej Strefy Centralnej.

**§ 3.** Uchwała wchodzi w życie z dniem 1 lutego 2026 roku.

Zarząd Związku Zachodniopomorskiej Strefy Centralnej:

1) Przewodnicząca Zarządu – Beata Gadzinowska ….....

2) Zastępca Przewodniczącego Zarządu – Edward Arys ….....

3) Członek Zarządu – Katarzyna Szlońska - Getka ….....

4) Członek Zarządu – Jacek Szadzewicz ……..

5) Członek Zarządu – Tomasz Waszczyk ……..

6) Członek Zarządu – Rafał Żukowski ……..

**Uzasadnienie**

**do Uchwały Nr 43/2026**

**Zarządu Związku Zachodniopomorskiej Strefy Centralnej**

**z dnia 19 stycznia 2026r.**

Na podstawie Ustawy z dnia 5 sierpnia 2025r. o zmianie ustawy o podatku od towarów i usług oraz ustawy o zmianie ustawy o podatku od towarów i usług oraz niektórych innych ustaw (Dz. U. z 2025r. poz. 1203) oraz zgodnie z Rozporządzeniem Ministra Finansów z dnia 27 grudnia 2021r. w sprawie korzystania z Krajowego Systemu e-Faktur (Dz. U. z 2021 r. poz. 2481, z 2022r. poz. 2667, z 2023r. poz. 1760) wprowadzono zapisy dotyczące zarządzania uprawnieniami w ramach Krajowego Systemu e-Faktur (KSeF), jako aplikacji obligatoryjnej do wystawiania i odbioru faktur ustrukturyzowanych.

**Załącznik Nr 1**
**do Uchwały Nr 43/2026 Zarządu Związku Zachodniopomorskiej Strefy Centralnej**
**z dnia 19 stycznia 2026r.**

# *INSTRUKCJA ZARZĄDZANIA UPRAWNIENIAMI W RAMACH KRAJOWEGO SYSTEMU E-FAKTUR W ZWIĄZKU ZACHODNIOPOMORSKIEJ STREFY CENTRALNEJ*

## Rozdział I
## Przepisy ogólne

### § 1

Ilekroć w niniejszym dokumencie jest mowa o:

1) Związku – należy przez to rozumieć Związek Zachodniopomorskiej Strefy Centralnej,
2) KSeF – Krajowy System e-Faktur,
3) administratorze systemu KSeF – należy przez to rozumieć Przewodniczącą Zarządu Związku Zachodniopomorskiej Strefy Centralnej, wyznaczoną na podstawie upoważnienia, którego wzór stanowi załącznik nr 1 do niniejszej instrukcji,
4) użytkowniku systemu – należy przez to rozumieć osobę upoważnioną do:

a) nadawania uprawnień,
b) nadawania uprawnień do zarządzania jednostkami podrzędnymi,
c) wystawiania faktur,
d) dostępu do faktur.

## Rozdział II
## Procedury nadawania i zmiany uprawnień w ramach

### § 2

1. Każdy użytkownik systemu przed uzyskaniem uprawnień do systemu KSeF ma obowiązek zapoznać się z:
   1) rozporządzeniem Ministra Finansów z dnia 27 grudnia 2021 r. w sprawie korzystania z Krajowego Systemu e-Faktur (Dz.U. z 2021 r. poz. 2481 z późn. zm.),
   2) niniejszą instrukcją.
2. Zapoznanie się z przepisami wymienionymi w ustępie 1 pracownik potwierdza własnoręcznym podpisem na oświadczeniu, którego wzór stanowi załącznik nr 2 do niniejszej instrukcji.
3. Administrator systemu KSeF przyznaje pracownikowi uprawnienia w zakresie dostępu do systemu.
4. Karta ewidencyjna powinna odzwierciedlać aktualny stan systemu w zakresie użytkowników i ich uprawnień oraz umożliwiać przeglądanie historii zmian uprawnień użytkowników.

5. Wzór karty ewidencyjnej powinien zawierać:
   1) imię i nazwisko użytkownika systemów informatycznych,
   2) rodzaj uprawnienia,
   3) datę nadania uprawnienia,
   4) datę odebrania uprawnienia,
   5) przyczynę odebrania uprawnienia,
   6) podpis administratora systemu KSeF.
6. Wzór karty ewidencyjnej uprawnień w zakresie dostępu i obsługi KSeF związanych z dostępem do KSeF stanowi załącznik nr 3 do niniejszej instrukcji.
7. Przyznanie uprawnień w zakresie dostępu do systemu KSeF polega na wprowadzeniu do systemu każdego użytkownika oraz wykazu dostępnych mu danych i operacji.
8. Pracownik ma prawo do wykonywania tylko tych czynności, do których został upoważniony.
9. Pracownik ponosi odpowiedzialność za wszystkie operacje wykonane przy użyciu jego identyfikatora i hasła dostępu.
10. Wszelkie przekroczenia lub próby przekroczenia przyznanych uprawnień traktowane będą jako naruszenie podstawowych obowiązków pracowniczych.
11. Pracownik zatrudniony przy pracy w systemie KSeF zobowiązany jest do zachowania tajemnicy. Tajemnica obowiązuje go również po ustaniu zatrudnienia.
12. W systemie KSeF stosuje się uwierzytelnianie dwustopniowe: na poziomie dostępu do komputera oraz na poziomie dostępu do aplikacji.
13. Odebranie uprawnień pracownikowi dokonywane jest przez administratora systemu z podaniem daty oraz przyczyny odebrania uprawnień. Odebranie uprawnień pracownikowi równoważne jest z usunięciem konta w systemie KSeF.
14. Kierownicy komórek organizacyjnych zobowiązani są pisemnie informować administratora systemu KSeF o każdej zmianie dotyczącej podległych pracowników, mającej wpływ na zakres posiadanych uprawnień w systemie informatycznym.
15. Identyfikator osoby, która utraciła uprawnienia dostępu do systemu KSeF, należy niezwłocznie zablokować w systemie informatycznym, w którym jest on przetwarzany, oraz unieważnić jej hasło.
16. Administrator systemu KSeF zobowiązany jest do prowadzenia i ochrony rejestru użytkowników i ich uprawnień w systemie informatycznym.

## Rozdział III
## Zasady posługiwania się hasłami

### § 3

1. Bezpośredni dostęp do systemu KSeF może mieć miejsce wyłącznie po podaniu identyfikatora i hasła.
2. Hasło powinno być zmieniane przez użytkownika co najmniej raz w miesiącu.

3. Identyfikator użytkownika nie powinien być zmieniany bez wyraźnej przyczyny, a po wyrejestrowaniu użytkownika z systemu KSeF nie powinien być przydzielany innej osobie.
4. Pracownicy są odpowiedzialni za zachowanie poufności swoich haseł.
5. Hasła użytkownika utrzymuje się w tajemnicy również po upływie ich ważności.
6. Hasło należy wprowadzać w sposób, który uniemożliwia innym osobom jego poznanie.
7. W sytuacji, kiedy zachodzi podejrzenie, że ktoś poznał hasło w sposób nieuprawniony, pracownik zobowiązany jest do natychmiastowej zmiany hasła.
8. Przy wyborze hasła obowiązują następujące zasady:
   1) minimalna długość hasła – 8 znaków;
   2) zakazuje się stosowania:
      a) haseł, które użytkownik stosował uprzednio w okresie minionego roku,
      b) swojej nazwy użytkownika w jakiejkolwiek formie (pisanej dużymi literami, w odwrotnym porządku, dublując każdą literę itp.),
      c) swojego imienia, drugiego imienia, nazwiska, przezwiska, pseudonimu w jakiejkolwiek formie,
      d) imion (w szczególności imion osób z najbliższej rodziny),
      e) ogólnie dostępnych informacji o użytkowniku, takich jak: numer telefonu, numer rejestracyjny samochodu, jego marka, numer dowodu osobistego, nazwa ulicy, na której mieszka lub pracuje, itp.,
      f) wyrazów słownikowych,
      g) przewidywalnych sekwencji znaków z klawiatury np.: „QWERTY”, „12345678” itp.,
      h) identyfikatora użytkownika;
   3) należy stosować:
      a) hasła zawierające kombinacje liter i cyfr,
      b) hasła zawierające znaki specjalne: znaki interpunkcyjne, nawiasy, symbole @, #, & itp., o ile system informatyczny na to pozwala,
      c) hasła, które można zapamiętać bez zapisywania,
      d) hasła łatwe i szybkie do wprowadzenia, po to, by trudniej było podejrzeć je osobom trzecim.
9. Zmiany hasła nie wolno zlecać innym osobom.
10. W systemach, które umożliwiają opcję zapamiętania nazw użytkownika lub jego hasła, nie należy korzystać z tej funkcji.
11. Hasło użytkownika o prawach administratora powinno znajdować się w zalakowanej kopercie w zamykanej na klucz szafie metalowej, do której dostęp mają:
   1) administrator KSeF,
   2) kierownik jednostki,
   3) pracownik odpowiedzialny za sprawy kadrowe.

## Rozdział IV
## Procedury rozpoczęcia, zawieszenia i zakończenia pracy w systemie

### § 4

1. Aby rozpocząć pracę w systemie KSeF, należy zalogować się do systemu przy użyciu indywidualnego identyfikatora oraz hasła.
2. Przy opuszczeniu stanowiska pracy na odległość uniemożliwiającą jego obserwację należy wylogować się z systemu (zablokować dostęp) lub – jeżeli taka możliwość nie istnieje – wyjść z programu.
3. Osoba udostępniająca stanowisko komputerowe innemu upoważnionemu pracownikowi zobowiązana jest wykonać operację wylogowania z systemu.
4. Przed wyłączeniem komputera należy bezwzględnie zakończyć pracę uruchomionych programów, wykonać zamknięcie systemu i – jeżeli jest to konieczne – wylogować się z sieci komputerowej.
5. Niedopuszczalne jest wyłączanie komputera przed zamknięciem oprogramowania oraz zakończeniem pracy w sieci.

## Rozdział V
## Środki ochrony systemu przed złośliwym oprogramowaniem, w tym wirusami komputerowymi

### § 5

1. Na każdym stanowisku komputerowym musi być zainstalowane oprogramowanie antywirusowe pracujące w trybie monitora.
2. Definicje wzorców wirusów aktualizowane są kilka razy w czasie dnia.
3. Zabrania się używania nośników niewiadomego pochodzenia bez wcześniejszego sprawdzenia ich programem antywirusowym. Sprawdzenia dokonuje użytkownik, który nośnika zamierza użyć.
4. Zabrania się pobierania z Internetu plików niewiadomego pochodzenia. Każdy plik pobrany z Internetu musi być sprawdzony programem antywirusowym. Sprawdzenia dokonuje użytkownik, który pobrał plik.
5. Zabrania się odczytywania załączników poczty elektronicznej bez wcześniejszego sprawdzenia ich programem antywirusowym. Sprawdzenia dokonuje pracownik, który pocztę otrzymał.
6. Kontrola antywirusowa przeprowadzana jest cyklinie przez osobę zajmującą się obsługą informatyczną Związku, jak również na wybranym komputerze w przypadku zgłoszenia nieprawidłowości w funkcjonowaniu sprzętu komputerowego lub oprogramowania.
7. W przypadku wykrycia wirusów komputerowych sprawdzane jest stanowisko komputerowe, na którym wirusa wykryto.

## Rozdział VI
## Postępowanie w sytuacji naruszenia dostępu do KSeF

### § 6

Postępowanie w sytuacji naruszenia dostępu do KSeF określa instrukcja regulująca postępowanie pracowników Związku zatrudnionych przy obsłudze KSeF w przypadku stwierdzenia naruszenia bezpieczeństwa danych osobowych, stanowiąca załącznik nr 4 do niniejszej instrukcji.

## Rozdział VII
## Procedury wykonywania przeglądów i konserwacji systemu

### § 7

1. Awaria systemu KSeF:
   1) w czasie niedostępności KSeF nie będzie możliwości korzystania z systemu;
   2) faktury będą mogły być wystawiane wyłącznie w czasie dostępności systemu; w przypadku, gdy data wystawienia zawarta w fakturze (pole P_1) będzie inna niż data przesłania do systemu, fakturę uznaje się za wystawioną w momencie jej przesłania zgodnie z art. 106na ust. 1 ustawy o VAT;
   3) komunikaty o niedostępności systemu monitoruje wyznaczony pracownik jednostki pod adresem: https://www.gov.pl/web/kas/komunikaty.
2. Rejestracja działań konserwacyjnych, awarii oraz napraw:
   1) administrator systemu KSeF prowadzi „Dziennik systemu informatycznego”; wzór i zakres informacji rejestrowanych w dzienniku określa załącznik nr 5 do niniejszej instrukcji;
   2) wpisów do dziennika może dokonywać administrator systemu KSeF, osoba zajmująca się obsługą informatyczną Związku lub osoby wyznaczone.

## Rozdział VIII
## Połączenie do sieci Internet

### § 8

Połączenie lokalnej sieci komputerowej z Internetem jest dopuszczalne wyłącznie po zainstalowaniu mechanizmów ochronnych oraz kompleksowego oprogramowania antywirusowego.

## Rozdział IX
## Postanowienia końcowe

### § 9

Na stanowisku pracy obowiązuje bezwzględny zakaz instalowania jakiegokolwiek oprogramowania. Pracownik, chcąc zainstalować aplikację lub program, musi uzyskać zgodę od osoby zajmującej się obsługą informatyczną Związku.

**Załącznik nr 1**
**do Instrukcji zarządzania uprawnieniami w ramach Krajowego Systemu e-Faktur**
**w Związku Zachodniopomorskiej Strefy Centralnej**

**Upoważnienie dla administratora systemu KSeF**

Na podstawie § 2 pkt 1 Instrukcji zarządzania systemem informatycznym z dniem ..... wyznaczam administratora systemu KSeF, powierzając tę funkcję Panu/ /Pani ....., posługującemu/ej się numerem PESEL .....

.....
(podpis administratora bezpieczeństwa
informacji lub administratora
danych osobowych)

Ja, niżej podpisany/a, zobowiązuję się do pełnienia obowiązków administratora systemu KSeF w oparciu o przepisy wewnętrzne obowiązujące w jednostce organizacyjnej.

.....
(podpis administratora systemu KSeF)

**Załącznik nr 2**
**do Instrukcji zarządzania uprawnieniami w ramach Krajowego Systemu e-Faktur**
**w Związku Zachodniopomorskiej Strefy Centralnej**

**Oświadczenie**

Oświadczam, że w związku z wykonywaniem obowiązków służbowych przetwarzam dane oraz mam dostęp do systemu KSeF, a także zapoznałem się z:

1) rozporządzeniem Ministra Finansów z dnia 27 grudnia 2021 r. w sprawie korzystania z Krajowego Systemu e-Faktur (Dz. U. z 2021 r. poz. 2481 z późn. zm.),
2) Instrukcją zarządzania uprawnieniami w ramach Krajowego Systemu e-Faltur w Związku Zachodniopomorskiej Strefy Centralnej.

.....
(podpis pracownika)

**Załącznik nr 2**
**do Instrukcji zarządzania uprawnieniami w ramach Krajowego Systemu e-Faktur**
**w Związku Zachodniopomorskiej Strefy Centralnej**

**Karta ewidencyjna uprawnień w zakresie dostępu i obsługi KSeF**
**w Związku Zachodniopomorskiej Strefy Centralnej**

| Lp. | Identyfikator użytkownika | Nazwisko i imię użytkownika | Rodzaj uprawnienia | Data nadania uprawnień | Podpis administratora systemu KSeF | Data i przyczyna odebrania uprawnień |
|---|---|---|---|---|---|---|
| 1. | | | | | | |
| 2. | | | | | | |
| 3. | | | | | | |
| 4. | | | | | | |
| 5. | | | | | | |
| 6. | | | | | | |

**Załącznik nr 4**
**do Instrukcji zarządzania uprawnieniami w ramach KSeF**

# Instrukcja regulująca postępowanie pracowników Związku Zachodniopomorskiej Strefy Centralnej zatrudnionych przy przetwarzaniu danych osobowych w przypadku stwierdzenia naruszenia bezpieczeństwa danych osobowych

**§ 1**

Niniejsza instrukcja reguluje postępowanie pracowników Związku Zachodniopomorskiej Strefy Centralnej zatrudnionych przy obsłudze systemu KSeF w przypadku stwierdzenia naruszenia bezpieczeństwa danych.

**§ 2**

Celem niniejszej instrukcji jest określenie zadań pracowników zatrudnionych przy obsłudze systemu KSeF w zakresie:

1) ochrony danych przed modyfikacją, zniszczeniem, nieuprawnionym dostępem i ujawnieniem lub pozyskaniem danych osobowych, a także ich utratą oraz
2) ochrony zasobów technicznych w przypadku stwierdzenia naruszenia ochrony danych lub zabezpieczeń systemu informatycznego.

**§ 3**

Naruszenie ochrony danych systemu KSeF może zostać stwierdzone na podstawie oceny:

1) stanu urządzeń technicznych,
2) zawartości zbiorów danych osobowych,
3) sposobu działania programu lub jakości komunikacji w sieci teleinformatycznej,
4) metod pracy (w tym obiegu dokumentów).

**§ 4**

W przypadku stwierdzenia naruszenia ochrony danych systemu KSeF należy bezzwłocznie:

1) powiadomić administratora systemu KSeF;
2) zablokować dostęp do systemu dla użytkowników oraz osób nieupoważnionych;
3) podjąć działania mające na celu zminimalizowanie lub całkowite wyeliminowanie powstałego zagrożenia – o ile czynności te nie spowodują przekroczenia uprawnień pracownika;
4) zabezpieczyć dowody umożliwiające ustalenie przyczyn oraz skutków naruszenia bezpieczeństwa systemu.

**§ 5**

1. Pracownik, który stwierdził naruszenie bezpieczeństwa danych systemu KSeF, jest zobowiązany niezwłocznie powiadomić administratora systemu KSeF.

2. Na stanowisku, na którym stwierdzono naruszenie zabezpieczenia danych, administrator systemu KSeF i osoba przełożona pracownika przejmują nadzór nad pracą w systemie, odsuwając jednocześnie od stanowiska pracownika, który dotychczas na nim pracował, aż do czasu wydania odmiennej decyzji.

**§ 6**

Administrator systemu KSeF lub osoba przez niego upoważniona podejmuje czynności wyjaśniające, mające na celu ustalenie:

1) przyczyn i okoliczności naruszenia bezpieczeństwa danych osobowych;
2) osób winnych naruszenia bezpieczeństwa danych osobowych;
3) skutków naruszenia.

**§ 7**

1. Administrator danych zobowiązany jest do powiadomienia o zaistniałej sytuacji kierownika Związku Zachodniopomorskiej Strefy Centralnej, który podejmuje decyzje o wykonaniu czynności zmierzających do przywrócenia poprawnej pracy systemu oraz o ponownym przystąpieniu do pracy w systemie.

2. Administrator systemu KSeF lub osoba przez niego upoważniona zobowiązana jest do sporządzenia pisemnego raportu na temat zaistniałej sytuacji, zawierającego co najmniej:

1) datę i miejsce wystąpienia naruszenia,
2) zakres ujawnionych danych,
3) przyczynę ujawnienia, osoby odpowiedzialne oraz stosowne dowody winy,
4) sposób rozwiązania problemu,
5) przyjęte rozwiązania mające na celu wyeliminowanie podobnych zdarzeń w przyszłości.

**Załącznik nr 5**
**do Instrukcji zarządzania uprawnieniami w ramach KSeF**

**Dziennik systemu informatycznego**
**Związku Zachodniopomorskiej Strefy Centralnej**

Dziennik zawiera opisy wszelkich zdarzeń istotnych dla działania systemu KSeF, a w szczególności:

1) w przypadku awarii – opis awarii, przyczyn awarii, szkód wynikłych na skutek awarii, sposobu usunięcia awarii, opis systemu po awarii, wnioski;
2) w przypadku konserwacji systemu – opis podjętych działań, wnioski.

| **Lp.** | **Data i godzina zdarzenia** | **Opis zdarzenia** | **Podjęte działania** | **Wnioski** | **Podpis** |
|---|---|---|---|---|---|
| 1. | | | | | |
| 2. | | | | | |
| 3. | | | | | |
| 4. | | | | | |