

## **SYSTEM ZARZĄDZANIA BEZPIECZEŃSTWEM INFORMACJI. WYMAGANIA I REGULACJE PRAWNE**

### **WAŻNE INFORMACJE:**

Mimo, iż przepisy krajowe wymagają od kierowników jednostek sektora finansów publicznych wdrożenia i zapewnienia ciągłości działania Systemu Zarządzania Bezpieczeństwem Informacji wiele podmiotów nie potrafi w sposób interpretować tych wymagań. W związku ze stosowaniem przepisów europejskich o ochronie danych osobowych większość podmiotów administracji publicznej skupiło się na ochronie danych osobowych zapominając zupełnie o wymaganiach m.in. rozporządzenia KRI czy ustawy KSC. Szkolenie ma pomóc uczestnikom połączyć wymagania wynikające z przepisów krajowych spełniając jednocześnie wymagania RODO. Udział w szkoleniu wymaga podstawowej wiedzy na temat Bezpieczeństwa Informacji oraz istniejących wymagań, na szkoleniu prelegent skupiać się będzie na wdrażaniu rozwiązań w celu wypełnienia wymagań oraz sposobu weryfikacji ich wypełnienia. Od uczestników nie jest wymagana znajomość normy ISO 27001.

### **CELE I KORZYŚCI:**

- Zapoznanie uczestników z wymaganiami prawnymi w zakresie funkcjonowania Systemu Zarządzania Bezpieczeństwem Informacji w Jednostkach Sektora Finansów Publicznych.
- Wyjaśnienie uczestnikom wymagań regulacyjnych oraz przedstawienie rozwiązań pomagających wypełnić te wymagania.
- Konsultacje z trenerem oraz innymi uczestnikami spotkania.

### **PROGRAM:**

- 1. Wprowadzenie do Systemu Zarządzania Bezpieczeństwem Informacji (ISMS):**
  - a. Co to jest System Zarządzania Bezpieczeństwem Informacji?
  - b. Wprowadzenie do standardu ISO 27001,
  - c. Korzyści wynikające z wdrożenia Systemu Zarządzania Bezpieczeństwem Informacji.
- 2. Przegląd wymagań regulacyjnych:**
  - a. Wymagania regulacyjne dotyczące Systemu Zarządzania Bezpieczeństwem Informacji,
  - b. Przegląd głównych aktów prawnych związanych z ochroną informacji, w tym RODO (Rozporządzenie o ochronie danych osobowych) ustawa o KSC, Rozporządzenie w sprawie KRI.
- 3. Etapy wdrożenia Systemu Zarządzania Bezpieczeństwem Informacji:**
  - a. Etapy wdrażania Systemu Zarządzania Bezpieczeństwem Informacji,
  - b. Planowanie wdrożenia Systemu Zarządzania Bezpieczeństwem Informacji,
  - c. Ocena ryzyka i zarządzanie ryzykiem.
- 4. Procesy biznesowe w Systemie Zarządzania Bezpieczeństwem Informacji:**
  - a. Zarządzanie dokumentacją,
  - b. Wdrażanie polityki bezpieczeństwa informacji,
  - c. Przegląd audytów i testów bezpieczeństwa informacji,
  - d. Reagowanie na incydenty bezpieczeństwa informacji.
- 5. Audytowanie Systemu Zarządzania Bezpieczeństwem Informacji:**
  - a. Przygotowanie do audytu Systemu Zarządzania Bezpieczeństwem Informacji,
  - b. Przeprowadzenie audytu Systemu Zarządzania Bezpieczeństwem Informacji,
  - c. Ocena wyników audytu Systemu Zarządzania Bezpieczeństwem Informacji.
- 6. Podsumowanie spotkania. Dyskusja.**

### **ADRESACI:**

Pracownicy Jednostek Sektora Finansów Publicznych odpowiadających za Bezpieczeństwo Informacji, Ochronę Danych Osobowych, ale również za sprawy organizacyjne, bezpieczeństwo prawne i zapewnienie funkcjonowania ciągłości funkcjonowania jednostki. Szkolenie głównie skierowane do takich stanowisk jak: Sekretarze, Informatycy, Inspektorzy Ochrony Danych, Pełnomocnicy Systemu Zarządzania Bezpieczeństwem Informacji, Prawnicy, firmy dostarczające oprogramowanie dla podmiotów publicznych.

## System zarządzania bezpieczeństwem informacji. Wymagania i regulacje prawne



Szkolenie będziemy realizowali **w formie webinarium on line.**



**3 lipca 2023 r.**

**Szkolenie w godzinach 09:30-14:00**



**Cena: 379 PLN netto/os.** Udział w szkoleniu zwolniony z VAT w przypadku finansowania szkolenia ze środków publicznych.

### CENA zawiera:

udział w profesjonalnym szkoleniu on-line z możliwością zadawania pytań,  
materiały szkoleniowe w wersji elektronicznej,  
certyfikat ukończenia szkolenia.

### DANE

### DO

### KONTAKTU:

**Ośrodek Kształcenia Samorządu Terytorialnego im. Waleriana Pańki**

ul. Piłsudskiego 43, 50-032 Wrocław

ul. Moniuszki 7, 40-005 Katowice

71 344 26 90, 32 206 98 43

[milena.dudek@okst.pl](mailto:milena.dudek@okst.pl); [szkolenia@okst.pl](mailto:szkolenia@okst.pl)

## DANE UCZESTNIKA ZGŁASZANEGO NA SZKOLENIE

Nazwa i adres nabywcy  
(dane do faktury)

Nazwa i adres odbiorcy

NIP

Telefon

1. Imię i nazwisko uczestnika, stanowisko,  
E-MAIL i TEL. DO KONTAKTU

2. Imię i nazwisko uczestnika, stanowisko,  
E-MAIL i TEL. DO KONTAKTU

Oświadczam, że szkolenie dla ww. pracowników jest kształceniem zawodowym finansowanym w całości lub  
co najmniej 70% ze środków publicznych (proszę zaznaczyć właściwe)

TAK

NIE

Proszę o przesłanie faktury na adres mailowy: .....

Proszę o przesłanie certyfikatu na adres mailowy: .....

Dokonanie zgłoszenia na szkolenie jest równoznaczne z zapoznaniem się i zaakceptowaniem regulaminu szkoleń Fundacji Rozwoju Demokracji Lokalnej zamieszczonym na stronie Organizatora [www.okst.pl](http://www.okst.pl) oraz zawartej w nim Polityce prywatności i ochrony danych osobowych.

**Wypełnioną kartę zgłoszenia należy przesłać poprzez formularz zgłoszenia na [www.okst.pl](http://www.okst.pl)  
do 28 czerwca 2023 r.**

**UWAGA!** Liczba miejsc ograniczona. O udziale w szkoleniu decyduje kolejność zgłoszeń. Zgłoszenie na szkolenie musi zostać potwierdzone przesłaniem do Ośrodka karty zgłoszenia. Brak pisemnej rezygnacji ze szkolenia najpóźniej na trzy dni robocze przed terminem jest równoznaczny z obciążeniem Państwa należnością za szkolenie niezależnie od przyczyny rezygnacji. Płatność należy uregulować przelewem na podstawie wystawionej i przesłanej FV.

Podpis osoby upoważnionej \_\_\_\_\_