Do: Działu Informatyki | DW: Kierownika Jednostki

Szanowni Państwo,

w imieniu **wydawcy miesięcznika "IT w Administracji"** oraz **mec. Sylwestra Szczepaniaka** zapraszam na:

SZKOLENIE ONLINE

„Krajowy System Cyberbezpieczeństwa - nowe obowiązki dla urzędów"

Prowadzenie: mec. Sylwester Szczepaniak*

10 lipca 2026 roku (piątek) na profesjonalnej platformie do SZKOLEŃ ONLINE

***mec. Sylwester Szczepaniak** - radca prawny, ekspert w obszarze paperless oraz EIDAS; wieloletni pracownik Ministerstwa Cyfryzacji, gdzie uczestniczył lub koordynował ok 30 dużych projektów legislacyjnych m.in. projekt e-płatności, mDokumenty, projekty związane informatyzacją i ochroną danych osobowych (w tym w zakresie prawa pracy) oraz identyfikacją elektroniczną; koordynator prac legislacyjnych w obszarze doręczeń elektronicznych; zasiadał w komitecie sterujących m.in. Projektu EZD RP; uczestniczył w pracach nad wdrożeniem eDowodu Osobistego; autor licznych publikacji z obszaru prawa samorządowego oraz rozwiązań paperless (podpisy elektroniczne, pieczęci elektroniczne, e-doręczenia) oraz prawa administracyjnego.*

Najnowsze zmiany w Krajowym Systemie Cyberbezpieczeństwa, proponowane przez rząd, mocno wpłyną na podmioty publiczne: urzędy gmin, szkoły, przedszkola, ośrodki pomocy społecznej, a także na spółki komunalne. Nowy zakres obowiązków będzie dodatkowo zróżnicowany i uzależniony od rodzaju podmiotu, jego głównych obszarów działalności oraz wielkości. **Nowy KSC istotnie zwiększa wymagania** prawne, regulacyjne oraz procesowe i techniczne. **Kładzie także duży nacisk na rolę i odpowiedzialność kierowników jednostek.**

Proponowane zmiany sprawiają, że cyberbezpieczeństwo przestaje być domeną IT - staje się sposobem działania całej organizacji. Pokazują one również konieczność podejścia kompleksowego w tym zakresie.

W trakcie szkolenia zostaną przedstawione praktyczne możliwości wdrożenia zmian, które wprowadza nowelizacja - wykraczające poza czysto techniczne aspekty.

Szkolenie jest skierowane do informatyków i osób odpowiedzialnych za obszar cyberbezpieczeństwa, a także do działów ochrony danych, pracowników wydziałów organizacyjnych i strategii.

Szkolenie odbędzie się 10 lipca 2026 roku (piątek) **na profesjonalnej platformie do SZKOLEŃ ONLINE**.

Co jest potrzebne od strony technicznej?

- **Komputer z przeglądarką internetową** (Google Chrome, Mozilla Firefox, Safari, Microsoft Edge, Opera) **lub tablet lub telefon z przeglądarką lub bezpłatną aplikacją** do pobrania z Apple App Store lub Google Play Store.
- Można, ale nie trzeba używać podczas szkolenia wbudowanej kamery lub kamery internetowej, mikrofonu, zestawu słuchawkowego lub głośników, ale nie powinny być one jednocześnie używane przez inną aplikację.

Warunkiem uczestnictwa jest dokonanie wpłaty na konto organizatora **oraz przesłanie zgłoszenia** na e-mail: szkolenia@itwadministracji.pl lub numer faksu: 71 798 48 48 albo wypełnienie formularza na stronie www: **szkolenia.itwadministracji.pl/t/KSC**

W razie wątpliwości pozostajemy do Państwa dyspozycji pod numerem telefonu: 71 798 48 40.

Z poważaniem,

Arkadiusz Karasek

- **Szkolenie w czasie rzeczywistym** - nie jest to uprzednio nagrany materiał
- **6 godzin wraz z przerwą** - rozpoczynamy o godz. 9.00
- **Możliwość zadawania pytań** i dyskusji z innymi uczestnikami
- **Grupa do 25 osób** - każdy będzie miał czas na zadawanie pytań
- **Niższa cena** - w porównaniu do szkolenia stacjonarnego
- **Wydrukowany certyfikat** - wyślemy pocztą
- **Dostępne na komputerze, tablecie i smartfonie** - z dowolnego miejsca

Pełny kalendarz naszych szkoleń i konferencji na stronie www: **szkolenia.itwadministracji.pl**

IT w administracji CENTRUM SZKOLENIOWE | online | szkolenia.itwadministracji.pl

HARMONOGRAM SZKOLENIA ONLINE

„Krajowy System Cyberbezpieczeństwa - nowe obowiązki dla urzędów”

Prowadzenie: mec. Sylwester Szczepaniak

***10 lipca 2026 roku (piątek)**, godz. 9.00-15.00 na profesjonalnej platformie do SZKOLEŃ ONLINE*

1. **Wprowadzenie do celu i zakresu szkolenia.**
2. **Obecne ramy prawne cyberbezpieczeństwa:**
   a. rozproszony system źródeł prawa zapewniania cyberbezpieczeństwa w pomiotach publicznych;
   b. rola podmiotów publicznych w obecnym Krajowym Systemie Cyberbezpieczeństwa;
   c. wymagania Krajowych Ram Interoperacyjności;
   d. wymagania ustawy o działaniach antyterrorystycznych;
   e. aspekty bezpieczeństwa informacji wynikające z RODO (ogólne rozporządzenie o ochronie danych osobowych).
3. **Doświadczenia z realizacji obecnych wymagań prawnych:**
   a. praktyka stosowania KRI w podmiotach publicznych;
   b. obecne doświadczania z działań w ramach alertów CRP;
   c. praktyka stosowania mechanizmów bezpieczeństwa informacji w kontekście RODO;
   d. doświadczenia jst w systemowym podejściu w samorządach do realizacji obecnych obowiązków.
4. **Ustawa o krajowym systemie certyfikacji cyberbezpieczeństwa:**
   a. cel i zakres ustawy;
   b. zasady certyfikacji;
   c. wykorzystanie certyfikacji w działalności jst.
5. **Nowe rozwiązania zawarte w Krajowym Systemie Cyberbezpieczeństwa:**
   a. założenia Dyrektywy NIS2 vs. NIS1 (i obecnej ustawy o KSC);
   b. podział podmiotów obowiązanych do stosowania dyrektywy NIS2 i nowego KSC;
   c. podmioty publiczne w nowym KSC w podziale na zakres obowiązków;
   d. podmioty kluczowe i podmioty ważne vs. podmioty ważne podmioty publiczne;
   e. przykłady analizy zaszeregowania podmiotów dla konkretnej grupy.
6. **Wymagania dla poszczególnych grup podmiotów:**
   a. kluczowe pojęcia niezbędne dla opisu wymagań;
   b. wymagania nowego KSC dla podmiotów kluczowych (sektorowych i publicznych);
   c. wymagania nowego KSC dla podmiotów ważnych;
   d. wymagania nowego KSC dla podmiotów ważnych - podmiotów publicznych.
7. **Odpowiedzialność kierowników podmiotów objętych nowym KSC:**
   a. zasady ponoszenia odpowiedzialności;
   b. odpowiedzialność za działania jednostki - kary dla jednostek;
   c. odpowiedzialności za działania jednostki - kary osobowe pieniężne na kierowników.
8. **Możliwości współpracy w realizacji obowiązków wynikających z nowego KSC:**
   a. współpraca w ramach struktur administracji publicznej;
   b. współpraca w ramach jednostki samorządu terytorialnego (CUWy, nieformalna współpraca wewnętrzna itp.);
   c. współpraca pomiędzy jednostkami samorządu terytorialnego (porozumienia itp.).
9. **Odpowiedzi na pytania uczestników szkolenia.**

Jak wygląda szkolenie online?

1. **Zgłoszenia dokonujesz** wysyłając wypełnioną kartę zgłoszeniową na adres: **szkolenia@itwadministracji.pl**, lub numer faksu: **71 798 48 48** lub poprzez formularz na stronie www: **szkolenia.itwadministracji.pl/t/KSC**
2. Na 2 dni przed szkoleniem na wskazane w zgłoszeniu adresy e-mail prześlemy unikatowe linki do platformy.
3. W dniu szkolenia logujesz się do platformy z dowolnego miejsca na dowolnym urządzeniu (komputer, tablet lub smartfon).
4. W trakcie szkolenia widać ekran prowadzącego oraz jego samego.
5. Możesz zadawać pytania trenerowi przez mikrofon lub wbudowany czat.
6. Materiały w formacie PDF będą do pobrania w trakcie szkolenia, a wydrukowany certyfikat otrzymasz pocztą.
7. Po zakończeniu szkolenia, nie ma możliwości jego ponownego odtworzenia.

IT w administracji CENTRUM SZKOLENIOWE | online | szkolenia.itwadministracji.pl

KARTA ZGŁOSZENIA NA SZKOLENIE ONLINE

„Krajowy System Cyberbezpieczeństwa - nowe obowiązki dla urzędów”

Prowadzenie: mec. Sylwester Szczepaniak

***10 lipca 2026 roku (piątek)**, godz. 9.00-15.00 na profesjonalnej platformie do SZKOLEŃ ONLINE*

Wypełnioną kartę prosimy przesyłać na numer faksu: **71 798 48 48** lub e-mail: **szkolenia@itwadministracji.pl** Zgłoszenia można także dokonać na stronie www: **szkolenia.itwadministracji.pl/KSC**			
1. Imię i nazwisko		Stanowisko	
Telefon	E-mail (na który wyślemy unikatowy kod dostępu do platformy)		**Kwota**
2. Imię i nazwisko		Stanowisko	
Telefon	E-mail (na który wyślemy unikatowy kod dostępu do platformy)		**Kwota**
RAZEM			**Suma kwot**

Koszt uczestnictwa 1 osoby w szkoleniu online wynosi 690 zł i obejmuje koszt materiałów w formie elektronicznej oraz wydrukowany certyfikat przesyłany pocztą po szkoleniu. Przy zgłoszeniach na szkolenie nadesłanych po dniu 7 lipca 2026 roku koszt uczestnictwa jednej osoby wynosi 790 zł. **Liczba miejsc ograniczona jest do 25.**

Do podanych cen nie doliczamy podatku VAT po podpisaniu poniższego oświadczenia o finansowaniu ze środków publicznych. W przeciwnym razie doliczamy podatek VAT w wysokości 23%.

❑ **Oświadczam, że szkolenie korzysta ze zwolnienia z VAT, ponieważ stanowi usługę kształcenia zawodowego lub przekwalifikowania zawodowego i jest finansowane w całości ze środków publicznych** zgodnie z art. 43 ust. 1 pkt 29c ustawy z dnia 11 marca 2004 r. o podatku od towarów i usług (z późn. zm.).

Data, pieczątka, podpis

DANE DO FAKTURY:	Płatności prosimy realizować: **PRESSCOM Sp. z o.o., ul. Krakowska 29, 50-424 Wrocław** **Erste Bank Polska: 96 1090 1522 0000 0001 0162 2418** z tytułem płatności: **20260710KSC**		
DANE ODBIORCY:	Nazwa		
Ulica		Kod	Miejscowość
NIP	IDWew / nr zamówienia	E-mail do księgowości	
DANE NABYWCY:	Nazwa		NIP
Ulica		Kod	Miejscowość

Przesłanie karty zgłoszenia stanowi prawnie wiążące zobowiązanie do uczestnictwa w szkoleniu na warunkach w niej określonych. Rezygnacji z udziału w szkoleniu można dokonać wyłącznie w formie pisemnej (e-mail, fax, poczta), najpóźniej 7 dni roboczych przed szkoleniem. W przypadku otrzymania rezygnacji przez organizatora później niż na 7 dni roboczych przed dniem szkolenia lub niezalogowania się uczestnika do platformy i tym samym niewzięcia udziału w szkoleniu, zgłaszający zostanie obciążony pełnymi kosztami uczestnictwa, wynikającymi z przesłanej karty zgłoszenia, na podstawie wystawionej faktury VAT. Niedokonanie wpłaty nie jest jednoznaczne z rezygnacją z udziału w szkoleniu.

Przesłanie zgłoszenia i podanie danych osobowych jest dobrowolne. Niepodanie wymaganych danych uniemożliwi realizację umowy/zamówienia. Informujemy, że Państwa dane osobowe będą przetwarzane w celach marketingu produktów i usług własnych Presscom Sp. z o.o. Administratorem danych osobowych będzie Presscom Sp. z o.o. z siedzibą we Wrocławiu, numer KRS 0000173413. Dane osobowe nie będą przekazywane podmiotom trzecim bez prawidłowej podstawy prawnej. W szczególności mają Państwo prawo do sprzeciwu wobec przetwarzania w celach marketingowych, a także żądania od Presscom Sp. z o.o. dostępu do swoich danych osobowych oraz ich sprostowania lub usunięcia. W sprawach z zakresu ochrony danych osobowych możliwy jest kontakt z do@presscom.pl. Pełna treść klauzuli informacyjnej dostępna jest na stronie internetowej: https://presscom.pl/do.

Data, pieczątka, podpis