Możliwość dofinansowania

SOVERANO

SOVERANO SPÓŁKA Z OGRANICZONĄ ODPOWIEDZIALNOŚCIĄ

4,6 / 5

82 oceny

# Ochrona danych osobowych i zarządzanie informacjami wrażliwymi w administracji samorządowej – szkolenie.

**Numer usługi** 2026/04/16/217200/3491512

800,00 PLN brutto
800,00 PLN netto
100,00 PLN brutto/h
100,00 PLN netto/h
131,67 PLN cena rynkowa

zdalna w czasie rzeczywistym
Usługa szkoleniowa
8 h
08.05.2026 do 08.05.2026

# Informacje podstawowe

| | |
|---|---|
| **Kategoria** | Prawo i administracja / Administracja publiczna |
| **Grupa docelowa usługi** | Szkolenie skierowane jest do osób pracujących w jednostkach samorządu terytorialnego, pracowników administracyjnych, osób zajmujących się obsługą interesantów oraz wszystkich osób chcących podnieść swoje kompetencje w zakresie bezpiecznego przetwarzania danych wrażliwych i informacji prawnie chronionych. |
| **Minimalna liczba uczestników** | 5 |
| **Maksymalna liczba uczestników** | 15 |
| **Data zakończenia rekrutacji** | 07-05-2026 |
| **Forma prowadzenia usługi** | zdalna w czasie rzeczywistym |
| **Liczba godzin usługi** | 8 |
| **Podstawa uzyskania wpisu do BUR** | Standard Usług Szkoleniowo– Rozwojowych PIFS SUS 3.0 |

# Cel

## Cel edukacyjny

Usługa prowadzi osobę uczestniczącą do samodzielnego identyfikowania zagrożeń dla bezpieczeństwa informacji oraz poprawnego stosowania procedur ochrony danych osobowych i informacji wrażliwych w codziennej pracy administracyjnej.

### Efekty uczenia się oraz kryteria weryfikacji ich osiągnięcia i Metody walidacji

| Efekty uczenia się | Kryteria weryfikacji | Metoda walidacji |
|---|---|---|
| Klasyfikuje dane osobowe oraz informacje wrażliwe zgodnie z obowiązującymi przepisami prawa. | Osoba uczestnicząca wymienia różnice między danymi zwykłymi a szczególnymi kategoriami danych. | Test teoretyczny z wynikiem generowanym automatycznie |
| | Osoba uczestnicząca poprawnie przypisuje zbiory danych do odpowiednich poziomów ochrony. | Test teoretyczny z wynikiem generowanym automatycznie |
| Stosuje techniczne i organizacyjne środki bezpieczeństwa w celu zapobiegania wyciekom informacji. | Osoba uczestnicząca projektuje bezpieczne stanowisko pracy zgodnie z zasadą czystego biurka i czystego ekranu. | Test teoretyczny z wynikiem generowanym automatycznie |
| | Osoba uczestnicząca wskazuje prawidłowe metody zabezpieczania nośników danych i przesyłek elektronicznych. | Test teoretyczny z wynikiem generowanym automatycznie |
| Reaguje na naruszenia ochrony danych osobowych zgodnie z procedurą zgłaszania incydentów. | Osoba uczestnicząca definiuje, co stanowi incydent bezpieczeństwa w środowisku pracy samorządowej. | Test teoretyczny z wynikiem generowanym automatycznie |
| | Osoba uczestnicząca opisuje ścieżkę raportowania naruszenia do Inspektora Ochrony Danych. | Test teoretyczny z wynikiem generowanym automatycznie |
| Analizuje ryzyko w procesach przetwarzania danych wewnątrz jednostki samorządu terytorialnego. | Osoba uczestnicząca wskazuje potencjalne punkty krytyczne w obiegu dokumentacji papierowej i elektronicznej. | Test teoretyczny z wynikiem generowanym automatycznie |
| | Osoba uczestnicząca dobiera odpowiednie metody przeciwdziałania zidentyfikowanym zagrożeniom cyfrowym. | Test teoretyczny z wynikiem generowanym automatycznie |

# Kwalifikacje

## Kompetencje

Usługa prowadzi do nabycia kompetencji.

**Warunki uznania kompetencji**

Pytanie 1. Czy dokument potwierdzający uzyskanie kompetencji lub wyraźnie z nim powiązane inne dokumenty związane ze wsparciem zawierają opis efektów uczenia się?

TAK

**Pytanie 2. Czy dokument lub wyraźnie z nim powiązane inne dokumenty związane ze wsparciem potwierdzają, że walidacja została przeprowadzona w oparciu o zdefiniowane w efektach uczenia się kryteria ich weryfikacji i zgodnie z zaplanowanymi metodami walidacji?**

TAK

**Pytanie 3. Czy dokument lub wyraźnie z nim powiązane inne dokumenty związane ze wsparciem potwierdzają zastosowanie rozwiązań zapewniających rozdzielenie procesów kształcenia i szkolenia od walidacji?**

TAK

# Program

## WARUNKI ORGANIZACYJNE

- **Czas trwania usługi:** 8 godzin zegarowych (60 min)
- **Przerwy:** wliczone w czas usługi rozwojowej i odbywają się zgodnie z harmonogramem.
- **Klauzula Dostępności:** W oparciu o zasadę racjonalnych usprawnień i dostępności (wynikającą z Ustawy o dostępności) oraz standardy równego traktowania, organizator zapewnia wsparcie dla osób ze szczególnymi potrzebami. W celu skorzystania z racjonalnych usprawnień, uczestnik proszony jest o wcześniejsze zgłoszenie swoich potrzeb organizatorowi szkolenia.
- **Platforma:** Google Meet lub Zoom (obsługa przez przeglądarkę). Wymagania:Komputer, stabilne łącze internetowe, mikrofon orazobowiązkowo włączona kamera(niezbędna do walidacji tożsamości i aktywności).
- **Dostęp:** Link znajduje się w sekcji karty kody dostępowe.
- **Walidacja:** Walidacja przeprowadzana jest w formie testu teoretycznego generowanego wynikiem automatycznym. W celu zapewnienia obiektywności oceny, proces walidacji jest prowadzony zgodnie z zasadą rozdzielności procesów kształcenia i walidacji.

Typy zajęć: [T] Teoretyczne: Wykłady, prezentacje, analiza koncepcji. [P] Praktyczne: Ćwiczenia, zadania, praca z narzędziami pod okiem trenera. [M] Mieszane: Łączą wprowadzenie teoretyczne z zadaniami praktycznymi.

*Program stanowi kompleksowe ujęcie problematyki bezpieczeństwa informacji w sektorze publicznym, łącząc teoretyczne aspekty Ogólnego Rozporządzenia o Ochronie Danych z praktycznymi warsztatami z zakresu cyberbezpieczeństwa. Podczas ośmiogodzinnego cyklu osoba uczestnicząca przeanalizuje pełną ścieżkę obiegu danych – od ich pozyskania od interesanta, przez bezpieczne przetwarzanie w systemach informatycznych, aż po procedury archiwizacji i reagowania na próby wyłudzenia informacji.*

**HARMONOGRAM SZCZEGÓŁOWY**

**Data: 08.05.2026 r.**

- **08:00 – 10:00** | Podstawy prawne i klasyfikacja danych w samorządzie [T] | Osoba prowadząca: Maciej Cieśla
- **10:00 – 10:15** | **Przerwa regeneracyjna**
- **10:15 – 12:15** | Obieg dokumentacji i zasady bezpiecznego stanowiska pracy [P] | Osoba prowadząca: Maciej Cieśla
- **12:15 – 12:45** | **Przerwa regeneracyjna**
- **12:45 – 14:30** | Cyberbezpieczeństwo i ochrona danych w chmurze oraz systemach IT [P] | Osoba prowadząca: Maciej Cieśla
- **14:30 – 14:45** | **Przerwa regeneracyjna**
- **14:45 – 15:45** | Procedury reagowania na incydenty i naruszenia ochrony danych [M] | Osoba prowadząca: Maciej Cieśla
- **15:45 – 16:00** | Walidacja efektów uczenia się – Test wiedzy | Walidator: Mateusz Świąder

# Harmonogram

Liczba przedmiotów/zajęć: 8

| Przedmiot / temat zajęć | Prowadzący | Data realizacji zajęć | Godzina rozpoczęcia | Godzina zakończenia | Liczba godzin |
|---|---|---|---|---|---|
| 1 z 8 Podstawy prawne i klasyfikacja danych w samorządzie | Maciej Cieśla | 08-05-2026 | 08:00 | 10:00 | 02:00 |
| 2 z 8 Przerwa | Maciej Cieśla | 08-05-2026 | 10:00 | 10:15 | 00:15 |
| 3 z 8 Obieg dokumentacji i zasady bezpiecznego stanowiska pracy | Maciej Cieśla | 08-05-2026 | 10:15 | 12:15 | 02:00 |
| 4 z 8 Przerwa | Maciej Cieśla | 08-05-2026 | 12:15 | 12:45 | 00:30 |
| 5 z 8 Cyberbezpieczeństwo i ochrona danych w chmurze oraz systemach. | Maciej Cieśla | 08-05-2026 | 12:45 | 14:30 | 01:45 |
| 6 z 8 Przerwa | Maciej Cieśla | 08-05-2026 | 14:30 | 14:45 | 00:15 |
| 7 z 8 Procedury reagowania na incydenty i naruszenia ochrony danych. | Maciej Cieśla | 08-05-2026 | 14:45 | 15:45 | 01:00 |
| 8 z 8 Walidacja | - | 08-05-2026 | 15:45 | 16:00 | 00:15 |

# Cennik

## Cennik

| Rodzaj ceny | Cena |
|---|---|
| **Koszt przypadający na 1 uczestnika brutto** | 800,00 PLN |
| Podmiot uprawniony do zwolnienia z VAT na podstawie art. 43 ust. 1 ustawy o VAT | |
| **Koszt przypadający na 1 uczestnika netto** | 800,00 PLN |
| **Koszt osobogodziny brutto** | 100,00 PLN |

| | |
|---|---|
| **Koszt osobogodziny netto** | 100,00 PLN |

# Prowadzący

Liczba prowadzących: 1

1 z 1

## Maciej Cieśla

Maciej Cieśla – ceniony ekspert, praktyk oraz doświadczona osoba prowadząca procesy edukacyjne, specjalizująca się w szeroko rozumianym bezpieczeństwie informacji, ochronie danych osobowych oraz przeciwdziałaniu nowoczesnym zagrożeniom cyfrowym. Posiada wieloletnie doświadczenie zawodowe, które zdobywał realizując zaawansowane projekty z zakresu audytu, wdrażania systemów zarządzania bezpieczeństwem oraz szkolenia kadr administracji publicznej i sektora prywatnego. Jego wiedza merytoryczna jest poparta licznymi certyfikatami o charakterze międzynarodowym, co gwarantuje najwyższy standard merytoryczny prowadzonych zajęć.
Maciej Cieśla Specjalizuje się w analizie ryzyka, projektowaniu bezpiecznych procedur obiegu dokumentacji oraz weryfikacji odporności systemów na próby nieuprawnionego uzyskania dostępu do informacji wrażliwych. Jego unikalne kompetencje pozwalają osobom uczestniczącym na głębokie zrozumienie mechanizmów działania oszustw internetowych oraz naukę skutecznych metod obrony przed nimi w codziennej pracy urzędnika.
W procesie kształcenia stawia na budowanie realnej sprawczości osób szkolonych, ucząc ich nie tylko przepisów Ogólnego Rozporządzenia o Ochronie Danych, ale przede wszystkim krytycznego myślenia w obliczu incydentów bezpieczeństwa.
Posiadane doświadczenie zawodowe i kompetencje spełniają wymagania Bazy Usług Rozwojowych

# Informacje dodatkowe

## Informacje o materiałach dla uczestników usługi

Osoba uczestnicząca otrzymuje komplet materiałów w formie cyfrowej: prezentację multimedialną, skrypt z wykazem najnowszych interpretacji prawnych, wzory protokołów zgłaszania naruszeń oraz listę kontrolną „Bezpieczne stanowisko pracy”.

## Warunki uczestnictwa

Aby wziąć udział w szkoleniu, osoba uczestnicząca powinna być zainteresowana tematem, otwarta na naukę, gotowa do pracy w grupie, posiadać podstawowe umiejętności komunikacyjne oraz mieć dostęp do narzędzi niezbędnych do udziału w szkoleniu. Warunkiem udziału w usłudze jest dokonanie zapisu co najmniej jeden dzień (**do godziny 14.00**) przed jej rozpoczęciem i uzyskanie akceptacji. Warunkiem uzyskania zaświadczenia jest uczestnictwo w co najmniej osiemdziesięciu procentach zajęć oraz uzyskanie pozytywnej oceny z walidacji.

## Informacje dodatkowe

Dodatkowo uczestnik zobowiązany jest do okazania się dokumentem potwierdzającym tożsamość ze zdjęciem, przed zespołem monitorującym usługę rozwojową.

Walidacja jest prowadzona w formie testu wiedzy z wynikiem generowanym automatycznie, co zapewnia obiektywną i natychmiastową weryfikację nabytych kompetencji. Proces ten odbywa się w ostatnim bloku szkolenia (godz. 15:45–16:00) pod nadzorem niezależnego walidatora, zgodnie z zasadą rozdzielności funkcji dydaktycznej od oceniającej.

# Warunki techniczne

Dla optymalnego udziału w usłudze zdalnej w czasie rzeczywistym, każdy uczestnik powinien dysponować: Stabilnym łączeminternetowym o minimalnej przepustowości łącza do pobierania: 10 Mb/s i wysyłania: 5 Mb/s (dla połączeń indywidualnych, w przypadkugrupowych zalecane wyższe parametry). Komputerem stacjonarnym lub laptopem z zainstalowanym i aktualnym systemem operacyjnym(Windows 10/11 lub macOS 10.15 i nowsze) oraz przeglądarką internetową (zalecana najnowsza wersja Google Chrome dla pełnejfunkcjonalności Meet, akceptowane są również Edge, Firefox lub Safari). Sprawnym mikrofonem i głośnikami/słuchawkami (zalecanesłuchawki z mikrofonem dla lepszej jakości dźwięku i eliminacji echa). Sprawną kamerą internetową (wbudowaną lub zewnętrzną)umożliwiającą transmisję obrazu. Brak konieczności instalacji dodatkowej aplikacji – Google Meet działa w pełni poprzez przeglądarkęinternetową. Wymagane jest jedynie posiadanie konta Google (Gmail) dołączonego do przeglądarki lub podanie e-maila, na który zostaniewysłane zaproszenie. Platforma Realizacji Usługi Wszystkie sesje usługi będą realizowane zdalnie, w czasie rzeczywistym, zapośrednictwem platformy Google Meet. Uczestnicy otrzymają unikalny link do dołączenia do dedykowanego spotkania Google Meet przedrozpoczęciem usługi. Link zostanie wysłany drogą elektroniczną (e-mail) lub poprzez udostępniony wcześniej kalendarz (np. GoogleCalendar). Prosimy o punktualne dołączanie do sesji, klikając w otrzymany link.

# Kontakt


## MATEUSZ ŚWIĄDER

**E-mail** swiadermateusz@gmail.com

**Telefon** (+48) 733 058 666