

PIĘĆ LAT DOŚWIADCZEŃ INSPEKTORA OCHRONY DANYCH. STOSOWANIE PRZEPISÓW. ANALIZA PRZYPADKÓW INCYDENTÓW I NARUSZEŃ OCHRONY DANYCH OSOBOWYCH

WAŻNE INFORMACJE:

Doświadczenia pięciu lat stosowania rozporządzenia ogólnego, w tym przebieg i wyniki kontroli organu nadzorczego w 2022 roku w zakresie wykonywania czynności IOD rozpoczęły szeroką dyskusję nad rozliczalnością czynności IOD poprzez wykazywanie się niezbędnymi instrumentami gwarantującymi prawidłowość ich wykonywania. Proponowane szkolenie stanowi retrospekcję doświadczeń Inspektora Ochrony Danych wykonującego czynności w podmiotach publicznych jak i innych podmiotach zobowiązanych do stosowania przepisów o ochronie danych osobowych. Podczas szkolenia:

- Przedstawimy wzorce działania IOD w oparciu o przepisy RODO a także wiele przykładowych dokumentów mających zastosowanie w wykazywaniu się zasadą rozliczalności w działalności IOD i jego zastępcy.
- Pokażemy praktyczne przykłady wykonywania czynności IOD w zakresie planistycznym i szkoleniowym oraz zasady dokumentowania czynności sprawdzających i audytowych a także wskażemy na udział IOD w tworzeniu i aktualizowaniu rejestrów.
- Omówimy także wady i zalety tworzenia regulaminu pracy IOD. Przedstawimy istotne przykłady naruszeń ochrony danych.

Zajęcia poprowadzi czynny Inspektor Ochrony Danych, ekspert i trener z zakresu ochrony danych osobowych.

CELE I KORZYŚCI:

- Wskazanie zasad prawidłowego i kompetentnego podejścia do wykonywania czynności IOD oraz postrzegania jego roli w organizacji.
- Nabycie praktycznych kompetencji w zakresie wykonywania czynności IOD zarówno w oparciu o zapisy RODO jak i wynikające z praktyki umiejętności stosowania przepisów.
- Zdobycie praktycznej wiedzy, jak skutecznie wykazywać się zasadą rozliczalności w działalności IOD oraz nabędą umiejętność opracowania i wdrożenia wewnętrznych dokumentów.
- Wskazanie jak realizować zadania szkoleniowe wynikające z polityk ochrony.
- Zdobycie wiedzy o zarządzaniu incydem dotyczącym naruszenia ochrony danych.
- Wskazanie, jak zorganizować punkt kontaktowy a także wspierać pracowników organizacji w wykonywaniu przepisów RODO.
- Poprzez analizę gotowych wzorów dokumentów przedstawimy wiele konkretnych rozwiązań organizacyjnych wspierających działanie IOD, jak plany pracy czy odpowiednio zredagowany regulamin pracy IOD. Wskażemy na właściwe umiejscowienia IOD w organizacji, prawidłowy sposób wymiany informacji, współpracy z urzędowym otoczeniem.
- Zaprezentowanie praktycznych rozwiązań w tym prezentacja gotowych wzorców dokumentów wypracowanych przez prowadzącego.
- Wskazanie przykładowych zaistniałych incydentów i zawiadomienia organu nadzorczego o naruszeniu bazując na doświadczeniach prowadzącego: błędy, złe nawyki wynikające z niewiedzy o zadaniach opisanych w RODO, postrzeganie IOD wyłącznie jako policjanta w ochronie danych często skutkują pojawianiem się przeterminowanych incydentów lub skarg składanych przez podmioty danych.

PROGRAM:

1. Analiza procesów przetwarzania a prowadzenie rejestru czynności przetwarzania:
 - Zarządzenie informacją niezbędna dla zidentyfikowania procesów.

- Właściciele aktywów a informacja o procesie.
2. Rejestr kategorii czynności jako wynik wielostronnej stronnej współpracy pracy nad umową powierzenia:
 - Badanie procesu powierzenia danych.
 - Udział IOD w tworzeniu umów powierzenie przetwarzania danych.
 - Rejestr umów powierzenia.
 - Audytowanie umów powierzenia.
 3. Aktualizacja dokumentacji:
 - Audyt dokumentacji ochrony danych w sferze doświadczeń IOD.
 - Analizy ryzyka.
 - Analiza incydentów.
 - Kiedy należy dokonać zmian polityki ochrony danych?
 4. Wykazywanie się klauzulami informacyjnymi – wykazywanie ich stosowanie w praktyce:
 - Klauzule w trybie art. 13 RODO.
 - Klauzule w trybie art. 14 RODO.
 - Zawieranie umów a obowiązki informacyjne.
 5. Regulamin pracy IOD – blaski i cienie skutecznego działania IOD:
 - Wzorzec regulaminu pracy IOD.
 - Zespół IOD – wsparcie IOD w wykonywaniu zasady rozliczalności. Doświadczenia pracy zespołu.
 6. Podsumowanie planów pracy IOD jako efektu działań IOD, czyli co sprawdzać i co audytować. Wyzwanie na kolejne lata.
 7. Inspektor Ochrony Danych szkoleniowcem i wykładowcą. Wnioski z wprowadzenia standaryzacji szkoleń z zakresu ochrony danych, KRI i cyberbezpieczeństwa.
 8. Incydent w RODO. Zarządzanie incydemem w organizacji.
 - Czy incydent to tylko problem IOD.
 - Dokumentowanie działań związanych z incydemem i współdziałanie osób funkcyjnych w identyfikacji i pracy z incydemem.
 9. Omówienie przebiegu incydemem w ciągu pięciolecia w praktyce prowadzącego.
 10. Podsumowanie. Dyskusja.

ADRESACI:

Osoby reprezentujące Administratora oraz Inspektorzy Ochrony Danych (Zastępcy IOD), specjaliści ds. ochrony danych.

PROWADZĄCY:

Absolwent Uniwersytetu Śląskiego i Studiów Podyplomowych na Wydziale Zarządzania Politechniki Śląskiej w Gliwicach. Audytor wewnętrzny Systemu Zarządzania Bezpieczeństwem Informacji zgodnie z normą PN ISO/IEC 27001:2017. Certyfikowany Menadżer Ryzyka w bezpieczeństwie informacji wg normy ISO/IEC 27005:2017 i PN ISO 31000:2012. Certyfikowany trener biznesu. Certyfikowany Compliance Officer. Audytor wewnętrzny Systemu Zarządzania Systemami Antykorupcyjnymi zgodnie z normą PN ISO/IEC 37001:2016. Projekt manager dla wdrażania projektów z zakresu ochrony danych osobowych w podmiotach przetwarzających. Współtwórca programów szkoleń dla kadr kierowniczych dla administracji państwowej. Asesor kompetencji zawodowych. Aktywny członek Administratorów Bezpieczeństwa Informacji. Współpracownik Fundacji Rozwoju Samorządu Lokalnego. Animator Forum Inspektorów Ochrony danych. Trener i wykładowca. Praktyk sponad dziesięcioletnim doświadczeniem w ochronie danych (ok. 2500 godzin szkoleniowych), mający wieloletnie doświadczenie w stosowaniu prawa ochrony danych osobowych, na co dzień zajmujący się wdrażaniem systemów zarządzania ochroną danych osobowych i polityk bezpieczeństwa informacji, ze szczególnym uwzględnieniem jednostek samorządu terytorialnego. Administrator Bezpieczeństwa Informacji a od maja 2018 Inspektor Ochrony Danych realizujący usługi outsourcingowe w wielu podmiotach samorządowych różnego szczebla. Projekt manager dla wdrażania projektów z zakresu ochrony danych osobowych w gminach, miastach i powiatach. Pracownik samorządowy szczebla powiatowego.

Pięć lat doświadczeń inspektora ochrony danych. Stosowanie przepisów. Analiza przypadków incydentów i naruszeń ochrony danych osobowych



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



18 lipca 2023 r.

Szkolenie w godzinach 10:00-14:00



Cena: 395 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:

Fundacja Rozwoju Demokracji Lokalnej Centrum Mazowsze;
ul. Żurawia 43, 00-680 Warszawa;
tel. 533 849 116;
szkolenia@frdl.org.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.frdl.mazowsze.pl oraz zawartej w nim Polityce prywatności i ochrony danych osobowych.

Zgłoszenia prosimy przysyłać do 12 lipca 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 _____