

BEZPIECZEŃSTWO DANYCH OSOBOWYCH W JST

WAŻNE INFORMACJE:

Przedmiotem proponowanego szkolenia z zakresu bezpieczeństwa danych osobowych jest omówienie zagadnień z zakresu prawidłowego postępowania z danymi osobowymi oraz ochrony ich poufności i integralności.

Ważną częścią zajęć jest:

- podniesienie świadomości uczestników na temat przepisów dotyczących ochrony danych osobowych, w szczególności RODO, oraz zrozumienie ich praw i obowiązków związanych z przetwarzaniem danych osobowych w urzędzie gminy,
- minimalizacja ryzyka naruszeń danych osobowych, zwiększenie kompetencji zawodowych, budowanie zaufania i reputacji instytucji oraz unikanie sankcji finansowych związanych z naruszeniem ochrony danych.

Podczas zajęć zaprezentujemy najczęściej popełniane błędy i nieprawidłowości związane z bezpieczeństwem danych osobowych oraz udzielimy odpowiedzi na najczęściej pojawiające się pytania i wątpliwości związane z tematem zajęć.

CELE I KORZYŚCI:

- Świadomość praw i obowiązków: zdobycie wiedzy na temat przepisów dotyczących ochrony danych osobowych, w szczególności RODO, w zakresie przetwarzania, przechowywania i ochrony danych osobowych.
- Podniesienie kompetencji zawodowych: zdobycie praktycznych umiejętności i poznanie narzędzi niezbędnych do prawidłowego postępowania z danymi osobowymi w urzędzie gminy. Zdobycie wiedzy na temat bezpiecznego przetwarzania danych, postępowania w przypadku wykrycia ataku na dane osobowe oraz im zapobiegania,
- Minimalizacja ryzyka naruszeń: zdobycie wiedzy na temat potencjalnych zagrożeń dla danych osobowych i poznanie skutecznych strategii minimalizowania ryzyka naruszeń. Zdobycie umiejętności identyfikacji potencjalnych luk w zabezpieczeniach oraz podejmowania odpowiednich działań w celu ochrony danych osobowych.
- Doskonalenie umiejętności zawodowych: możliwość poszerzenia swoich umiejętności i kompetencji w obszarze bezpieczeństwa danych osobowych.

PROGRAM:

1. Rodzaje ataków internetowych na dane osobowe:

- Przegląd typów ataków, w tym phishing, hasła, ransomware itp.
- Studia przypadków i przykłady rzeczywistych ataków.

2. Phishing i inżynieria społeczna:

- Definicja i mechanizm phishingu.

- Zidentyfikowanie fałszywych wiadomości e-mail i stron internetowych.
 - Sposoby ochrony przed phishingiem,
 - Ćwiczenia praktyczne i ilustracje phishingowe.
- 3. Bezpieczeństwo haseł i uwierzytelnianie dwuskładnikowe:**
- Wprowadzenie do zwykłego zarządzania użytkownikami.
 - Zasady tworzenia mocnych haseł.
 - Omówienie metod uwierzytelniania dwuskładnikowego.
 - Zastosowanie menedżerów haseł i narzędzi do uwierzytelniania dwuskładnikowego.
 - Ćwiczenia praktyczne związane z tworzeniem mocnych haseł.
- 4. Oprogramowanie antywirusowe i zabezpieczenia sieciowe:**
- Rola oprogramowania antywirusowego w ochronie danych osobowych.
 - Przegląd funkcji oprogramowania antywirusowego.
 - Zabezpieczenia sieciowe, takie jak firewalle i systemy włączone do intruzów (IDS/IPS).
 - Ćwiczenia praktyczne dotyczące instalacji i konfiguracji oprogramowania antywirusowego.
- 5. Bezpieczeństwo publiczne sieci Wi-Fi i sieci społecznościowych:**
- Zagrożenia związane z korzystaniem z publicznej sieci Wi-Fi.
 - Praktyki bezpieczeństwa podczas korzystania z sieci Wi-Fi.
 - Bezpieczne korzystanie z mediów społecznościowych i ochrona prywatności.
 - Ćwiczenia praktyczne dotyczące łączności Wi-Fi i zarządzania prywatnością w mediach społecznościowych.
- 6. Aktualizacje oprogramowania i efekty:**
- Ważność regularnych aktualizacji oprogramowania.
 - Rola świadomości w ochronie danych osobowych.
 - Tworzenie kultury bezpieczeństwa w miejscu pracy, jak również w życiu prywatnym.
 - Ćwiczenia praktyczne związane z identyfikacją zauważoną i zauważoną sytuację.
- 7. Podsumowanie i pytania.**

ADRESACI:

Inspektorzy Ochrony Danych Osobowych, osoby zajmujące się wsparciem Inspektora Ochrony Danych Osobowych, lub bezpośrednio zajmujące się zagadnieniem ochrony danych osobowych w kontakcie z klientem.

PROWADZĄCY:

Absolwent Wydziału Nauk Społecznych Akademii WSB w Dąbrowie Górniczej. Ukończył studia na kierunku Bezpieczeństwo Informacji w Administracji i Biznesie. Audytor Wiodący Systemu Zarządzania Bezpieczeństwem Informacji wg normy PN-EN ISO/IEC 27001 wydany przez TUV NORD. Audytor wewnętrzny Systemu Jakości PN-EN ISO/IEC 90001 wydany przez PCC Cert. Audytor i szkoleniowiec WCAG 2.1 dla sektora publicznego oraz biznesu. Trener i wykładowca z długoletnim doświadczeniem, propagator dostępności cyfrowej.

Bezpieczeństwo danych osobowych w JST



Szkolenie będziemy realizowali w formie webinarium on line.



30 sierpnia 2023 r.

Szkolenie w godzinach 9:00-14:30



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 Szkoleniowe w Łodzi
ul. Jaracza 74, 90-242 Łódź
tel. 535 175 301 biuro@frdl-lodz.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-lodz.pl oraz zawartej w nim Polityce prywatności i ochrony danych osobowych.

Zgłoszenia prosimy przesyłać do **24 sierpnia 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 _____