



SZKOLENIA ON-LINE

KORZYŚCI ZE SZKOLENIA:

- Wskazanie jak sprawnie i skutecznie tworzyć oraz zarządzać Systemem Zarządzania Bezpieczeństwa Informacji w kontekście stosowania przepisów o ochronie danych osobowych.
- Omówienie typowych błędów popełnianych przez Administratora Danych.
- Poznanie aktualnych wyników kontroli NIK i UODO zrealizowanych w latach 2014 – 2020, dotyczących wdrożenia Krajowych Ram Interoperacyjności oraz RODO.
 - Możliwość weryfikacji wiedzy i umiejętności w celu prawidłowego stosowania przepisów dotyczących ochrony danych osobowych i bezpieczeństwa informacji, w szczególności dotyczących haseł, zdalnego dostępu do zasobów.
 - Zdobywanie porad i wskazówek od praktyka, w celu prawidłowego wykonywania zadań, uniknięcia nieprawidłowości w bieżącej pracy i w przypadku kontroli.

BEZPIECZEŃSTWO INFORMACJI I OCHRONA DANYCH W ŚWIETLE KONTROLI NIK I UODO.

Typowe błędy popełniane przez Administratorów Danych

PROGRAM:

1. **Definicja podmiotu publicznego – do jakich jednostek organizacyjnych i w jakim zakresie mają zastosowanie:**
 - Krajowe Ramy Interoperacyjności,
 - Rozporządzenie Ogólne o Ochronie Danych Osobowych (RODO),
 - Krajowy System Cyberbezpieczeństwa.
2. **Przypomnienie podstawowych obowiązków związanych z zapewnieniem bezpieczeństwa informacji i ochrony danych w podmiotach publicznych:**
 - wymagana dokumentacja (polityki, instrukcje, rejestry i ewidencje),
 - osoby funkcyjne – personel bezpieczeństwa,
 - inwentaryzacja infrastruktury informatycznej i zasobów informacyjnych,
 - ocena ryzyka,
 - zabezpieczenia w podmiocie (poufność, integralność i dostępność),
 - użytkownicy (nadawanie uprawnień, szkolenia),
 - nadzór i kontrola oraz audyty wewnętrzne,
 - rejestrowanie i obsługa incydentów,
 - aktualizacja dokumentacji.
3. **Razem czy osobno? System Zarządzania Bezpieczeństwem Informacji a ochrona danych osobowych:**
 - wyznaczanie osób funkcyjnych odpowiedzialnych za bezpieczeństwo informacji i ochronę danych,
 - tworzenie wymaganej dokumentacji,
 - zabezpieczenie informacji i danych osobowych

Wskazanie:

- jak należy zabezpieczyć informacje i dane osobowe pod względem technicznym,
 - jak skutecznie nadzorować i kontrolować Systemy Zarządzania Bezpieczeństwem Informacji,
- jak skutecznie korzystać z urządzeń mobilnych,
- jak pracować i przechowywać dane w chmurze,
 - jak zabezpieczać nośniki danych,
- jak monitorować stan bezpieczeństwa systemów informatycznych,
- w jaki sposób monitorować działania użytkowników?

PREZACI:

Sekretarze gmin, miast i powiatów, inspektorzy ochrony danych osobowych, kierownicy jednostek organizacyjnych, osoby odpowiadające za bezpieczeństwo informacji, informatycy, audytorzy i kontrolerzy wewnętrzni, wszyscy zainteresowani tematyką szkolenia.

PROWADZĄCY:

Absolwent UMK w Toruniu oraz studiów podyplomowych WSAiB w Gdyni na kierunku zarządzanie bezpieczeństwem informacji, certyfikowany Inspektor Ochrony Danych, Menedżer Bezpieczeństwa Informacji oraz Auditor wewnętrzny systemu zarządzania bezpieczeństwem informacji. W latach 1992 - 2013 funkcjonariusz UOP/ABW, od 1999r. zajmuje się problematyką ochrony informacji niejawnych i innych danych prawnie chronionych, od 2009r. ekspert ABW z zakresu ochrony informacji niejawnych. Współorganizator konferencji poświęconych problematyce ochrony informacji oraz danych osobowych. W latach 2013 - 2017 pełnomocnik ds. ochrony informacji niejawnych w urzędzie wojewódzkim oraz innych jednostkach

(techniczne i organizacyjne środki ochrony),

- zarządzanie incydentami i ich zgłaszanie do właściwego organu,
- zapewnienie ciągłości działania,
- testowanie, mierzenie i ocena skuteczności ochrony danych,
- obowiązki związane z udostępnieniem lub powierzeniem danych.

4. Kontrole NIK i UODO zrealizowane w latach 2014 – 2020 dotyczące wdrożenia Krajowych Ram Interoperacyjności oraz RODO:

- zakres podmiotów objętych kontrolami,
- syntetyczne przedstawienie wyników kontroli,
- typowe błędy występujące w kontrolowanych jednostkach,
- analiza wybranych przypadków.

5. Praktyczne wskazówki dotyczące zapewnienia bezpieczeństwa elektronicznych zasobów informacyjnych:

- sześć złotych zasad bezpieczeństwa informacji,
- zagrożenia z Internetu: phishing, ransomware, poczta e-mail, strony www, serwisy społecznościowe,
- hasła do systemów informatycznych,
- bezpieczeństwo urządzeń mobilnych,
- informatyczne nośniki danych – pendrivy i pamięci zewnętrzne,
- zdalny dostęp do zasobów i korzystanie z urządzeń prywatnych pracowników,
- przechowywanie danych w chmurze i korzystanie z zewnętrznych dostawców usług informatycznych,
- oprogramowanie antywirusowe,
- aktualizacja programów i aplikacji,
- monitorowanie stanu bezpieczeństwa systemów informatycznych oraz działań użytkowników,
- udostępnianie dokumentacji podmiotom zewnętrznym oraz w trybie dostępu do informacji publicznej.

6. Konsultacje i odpowiedzi na pytania.

TERMIN SZKOLENIA:

8 grudnia 2020 r., godz. 10.00 – 14.00.

CENA:

290 zł netto/ os. Udział w szkoleniu zwolniony z VAT w przypadku finansowania szkolenia ze środków publicznych. Cena zawiera: udział w profesjonalnym szkoleniu on-line, materiały szkoleniowe przekazane w wersji elektronicznej, certyfikat ukończenia szkolenia, możliwość konsultacji z trenerem.

ZGŁOSZENIA:

Wypełnioną kartę zgłoszenia należy przesać mailem na adres: szkolenia@mistia.org.pl lub poprzez formularz zgłoszenia na www.mistia.org.pl do **3 grudnia 2020r.**

UWAGA: LICZBA MIEJSC OGRANICZONA!

DANE DO KONTAKTU:

Fundacja Rozwoju Demokracji Lokalnej im. Jerzego Regulskiego
NIP: 522-000-18-95

FRDL Małopolski Instytut Samorządu Terytorialnego i Administracji
ul. Floriańska, 31-019, Kraków
tel. +48 12 623 72 44
szkolenia@mistia.org.pl

Co to jest webinarium i jak będziemy je realizowali?

- Szkolenie to będzie realizowane w formie on-line. Udział pozwoli zapoznać się z tematem prezentowanym na żywo przez eksperta, zadać mu pytanie na czacie i porozmawiać z innymi uczestnikami.
- Nasze szkolenia on-line wyróżnia to, że prowadzone są z najlepszymi trenerami i ekspertami, praktykami w temacie szkolenia, których znają Państwo ze szkoleń stacjonarnych.
- Będą Państwo widzieli i słyszeli trenera oraz wyświetlane przez niego materiały, prezentacje, filmy instruktażowe, dokumenty.
- Zarówno przed spotkaniem, jak i w jego trakcie mogą Państwo zadawać pytania poprzez czat. Trener odpowiada na te pytania na bieżąco lub w drugiej części szkolenia w sesji pytań i odpowiedzi.
- Platforma, na której odbywa się webinarium, jest dostępna bezpośrednio przez przeglądarkę internetową, np. Google Chrome lub inną. Potrzebny jest komputer z dostępem do Internetu. Przydatne mogą być również słuchawki z mikrofonem, jeżeli chciałby Państwo zabierać głos a liczba uczestników na to pozwala. Kamera w komputerze nie jest konieczna.
- Po przesłaniu karty zgłoszenia otrzymają Państwo na wskazany adres e-mail unikalny link do webinarium (wirtualnej sali szkoleniowej). Wystarczy kliknąć w ten link w konkretnym terminie i godzinie w której planowane jest jego rozpoczęcie.
- Korzystanie z naszych webinarium jest bardzo proste. Jeżeli po raz pierwszy korzystają Państwo z naszego webinarium sugerujemy testowe połączenie we wskazanym przez nas terminie.
- Po spotkaniu otrzymają Państwo mailem elektroniczne materiały szkoleniowe a certyfikat ukończenia szkolenia zostanie przesłany, w zależności od Państwa preferencji, pocztą lub mailem. Płatność za szkolenie nastąpi na podstawie faktury przesłanej po szkoleniu mailem.

Dokonanie zgłoszenia na szkolenie jest równoznaczne z zapoznaniem się i zaakceptowaniem regulaminu szkoleń Fundacji Rozwoju Demokracji Lokalnej zamieszczonym na stronie Organizatora www.mistia.org.pl oraz zawartej w nim Polityce prywatności i ochrony danych osobowych.

KARTA ZGŁOSZENIA UCZESTNIKA:

Bezpieczeństwo informacji i ochrona danych w świetle kontroli NIK i UODO. Typowe błędy popełniane przez Administratorów Danych (zajęcia on-line) 8 grudnia 2020 r.

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

3. 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 certyfikat w formie:

Papierowej

Elektronicznej e mail.....

UWAGA Ilość miejsc ograniczona. O udziale w szkoleniu decyduje kolejność zgłoszeń. Zgłoszenie na szkolenie musi zostać potwierdzone przesłaniem do Ośrodka karty zgłoszenia (mail lub formularz na www.mistia.pl). Brak pisemnej rezygnacji ze szkolenia najpóźniej na trzy dni robocze przed terminem będzie równoznaczny z obciążeniem Państwa należnością za to szkolenie niezależnie od przyczyny rezygnacji. Płatność należy uregulować przelewem przed lub po szkoleniu (na przelewie prosimy podać nazwę szkolenia).

Podpis osoby upoważnionej
