



BEZPIECZEŃSTWO INFORMACJI I OCHRONA DANYCH W ŚWIETLE KONTROLI NIK I UODO. TYPOWE BŁĘDY POPEŁNIANE PRZEZ ADMINISTRATORÓW DANYCH

INFORMACJE O SZKOLENIU:

Kwestia bezpieczeństwa informacji oraz ochrony danych osobowych budzi wiele kontrowersji. Aby ustrzec się przed błędami i wyjaśnić kwestie problemowe, proponujemy Państwu uczestnictwo w szkoleniu, które pozwoli usystematyzować wiedzę na temat właściwego przetwarzania danych osobowych, wskazując w praktyczny sposób najczęściej popełniane błędy przez administratora danych w kontekście kontroli prowadzonych przez Najwyższą Izbę Kontroli oraz Urząd Ochrony Danych Osobowych. Podczas szkolenia, ekspert-praktyk podzieli się wiedzą z uczestnikami oraz swoimi doświadczeniami w zakresie ochrony danych osobowych, powierzania danych oraz ich prawidłowego zabezpieczania. Szkolenie polecamy osobom, chcącym podnieść wiedzę z tego zakresu, tym, które od niedawna zajmują się tą tematyką, jak i osobom z dłuższym stażem, które chcą rozwiązać problemy i wątpliwości.

CELE I KORZYŚCI:

- Omówienie prawnych i praktycznych aspektów bezpieczeństwa informacji i ochrony danych osobowych w świetle kontroli NIK oraz Urzędu Ochrony Danych Osobowych.
- Wskazanie jak sprawnie i skutecznie tworzyć oraz zarządzać Systemem Zarządzania Bezpieczeństwem Informacji w kontekście stosowania przepisów o ochronie danych osobowych.
- Analiza typowych błędów popełnianych przez Administratora Danych.
- Poznanie wyników kontroli NIK i UODO zrealizowanych w latach 2014 – 2022, dotyczących wdrożenia Krajowych Ram Interoperacyjności oraz RODO w zakresie problematyki spotkania.
- 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.
- Zdobycie porad i wskazówek od praktyka, w celu prawidłowego wykonywania zadań, uniknięcia nieprawidłowości w bieżącej pracy i w przypadku kontroli.

Uzyskanie odpowiedzi na pytania:

- 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 prawidłowo zabezpieczać nośniki danych?
- jak monitorować stan bezpieczeństwa systemów informatycznych?
- w jaki sposób monitorować działania użytkowników?

PROGRAM:

1. Wymagania prawne związane z przetwarzaniem informacji i danych osobowych przez Administratorów Danych:

- ochrona danych osobowych,
- Krajowe Ramy Interoperacyjności,
- cyberbezpieczeństwo,
- dostępność cyfrowa,
- informacja publiczna,

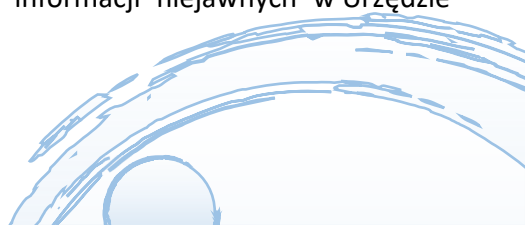
- prawo telekomunikacyjne,
 - ochrona sygnalistów,
 - ochrona informacji niejawnych.
- 2. Podstawowe obowiązki związane z zapewnieniem poufności, integralności i dostępności danych:**
- zabezpieczenia organizacyjne:
 - osoby funkcyjne – personel bezpieczeństwa,
 - obowiązki kadry kierowniczej oraz pozostałego personelu,
 - wymagana dokumentacja oraz jej aktualizacja (polityki, instrukcje, rejestry i ewidencje),
 - szkolenia personelu,
 - nadzór i kontrola oraz audyty wewnętrzne,
 - obowiązki informacyjne,
 - ocena ryzyka i dobór adekwatnych zabezpieczeń,
 - zabezpieczenia techniczne – środki bezpieczeństwa fizycznego,
 - zabezpieczenia informatyczne:
 - inwentaryzacja infrastruktury informatycznej i zasobów informacyjnych,
 - kontrola dostępu do zasobów informacyjnych,
 - użytkownicy (nadawanie i weryfikacja uprawnień, ewidencja osób uprawnionych),
 - prawidłowe oprogramowanie,
 - monitorowanie stanu bezpieczeństwa systemów i sieci informatycznych,
 - zarządzanie incydentami i ich zgłaszanie do właściwego organu,
 - zapewnienie ciągłości działania,
 - relacje z zewnętrznymi dostawcami i usługodawcami.
- 3. Kontrole NIK oraz UODO zrealizowane w latach 2018 - 2022 dotyczące bezpieczeństwa informacji i ochrony danych osobowych:**
- zakres podmiotów objętych kontrolami,
 - syntetyczne przedstawienie wyników kontroli,
 - omówienie typowych, powtarzających się błędów występujących w kontrolowanych jednostkach,
 - kary UODO nałożone na podmioty publiczne,
 - analiza wybranych przypadków.
- 4. Praktyczne wskazówki dotyczące zapewnienia bezpieczeństwa elektronicznych zasobów informacyjnych:**
- podstawowe wymagania dotyczące bezpieczeństwa informacji,
 - zagrożenia związane Internetem,
 - legalność oprogramowania,
 - bezpieczeństwo urządzeń mobilnych,
 - informatyczne nośniki danych – pendrivy i pamięci zewnętrzne,
 - zdalny dostęp do zasobów i korzystanie z urządzeń prywatnych pracowników,
 - oprogramowanie antywirusowe,
 - aktualizacja programów i aplikacji,
 - podstawowe zasady związane z korzystaniem z zewnętrznych dostawców usług informatycznych.
- 5. Konsultacje i odpowiedzi na pytania.**

ADRESACI:

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 OIN. Współorganizator szkoleń i konferencji poświęconych problematyce ochrony informacji oraz danych osobowych. W latach 2013 - 2017 pełnomocnik ds. ochrony informacji niejawnych w Urzędzie Wojewódzkim oraz innych jednostkach.



Bezpieczeństwo informacji i ochrona danych w świetle kontroli NIK i UODO. Typowe błędy popełniane przez administratorów danych



Szkolenie będziemy realizowali w formie webinarium on line.



14 lipca 2022 r.

Szkolenie w godzinach 9:00-13:00



Cena: 359 PLN 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 w wersji elektronicznej,
certyfikat ukończenia szkolenia,
możliwość konsultacji z trenerem.

DANE DO KONTAKTU:

Fundacja Rozwoju Demokracji Lokalnej Podkarpacki Ośrodek Samorządu
Terytorialnego
ul. Kolejowa 1, 35 – 073 Rzeszów
tel. 17 862 69 64
post@frdl.rzeszow.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 certyfikat w formie: Papierowej
Elektronicznej e mail.....

Proszę o przesłanie faktury 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.rzeszow.pl oraz zawartej w nim Polityce prywatności i ochrony danych osobowych.

Wypełnioną kartę zgłoszenia należy przestać poprzez formularz zgłoszenia na www.frdl.rzeszow.pl
do 12 lipca 2022r.

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 _____