Fundacja Rozwoju Demokracji Lokalnej
im. Jerzego Regulskiego

KURS ON-LINE 18,19,20 i 21 maja 2021

KURS: ZARZĄDZENIE BEZPIECZEŃSTWEM INFORMACJI ORAZ OCHRONA DANYCH OSOBOWYCH W JEDNOSTKACH SAMORZĄDU TERYTORIALNEGO

CELE I KORZYŚCI

Kurs umożliwi przygotowanie do praktycznej, efektywnej i skutecznej realizacji wyzwań z zakresu zarządzania bezpieczeństwem informacji i ochrony danych osobowych przez IOD lub osobę odpowiedzialną za bezpieczeństwo informacji w organizacji. Czterodniowe spotkanie przyczyni się nie tylko do podniesienia poziomu wiedzy, ale stanie się również okazją do wymiany doświadczeń, rozwiązań i dobrych praktyk pomiędzy uczestnikami szkolenia.

WAŻNE INFORMACJE O SZKOLENIU:

Zapraszamy Państwa na 4 dniowy kurs podczas którego dzięki naszym ekspertom zdobędą Państwo fachową i kompleksową wiedzę z w/w tematu. Pomocą w sprostaniu wyzwaniom związanym z minioną reformą prawa ochrony danych osobowych dla wszystkich administratorów jest posiadanie kompetentnego, posiadającego specjalistyczne przygotowanie inspektora ochrony danych, który na bieżąco aktualizuje swoją wiedzę.
Kurs jest przeznaczony nie tylko dla inspektorów ale również dla podmiotów, które chcą przetwarzać dane osobowe w sposób zgodny z przepisami.

PROGRAM SZKOLENIA

DZIEŃ 1: ZARZĄDZANIE OCHRONĄ DANYCH W JST

CELE I KORZYŚCI:

- Omówienie najważniejszych kwestii prawnych.
- Jak zbudować system ochrony danych i go nadzorować.
- Jak współpracować z własnym IOD lub zewnętrznym.
- Czego wymagać od zewnętrznego IOD.
- Kto odpowiada za stan ochrony danych.

PROGRAM:

1. **Podstawy prawne ochrony danych:**
   a. Rozporządzenie ogólne jako podstawowy dokument chroniący prawa osób na terenie unii Europejskiej – struktura prawna dokumentu i zakres obowiązywania.
   b. Dyrektywa DODO – jako dokument regulujących szczególny obszar przetwarzania danych.
   c. Polskie akty prawne dotyczące ochrony danych.
   d. Ustawa o informatyzacji działalności podmiotów realizujących zadania publiczne oraz rozporządzenie o krajowych ramach interoperacyjności.
   e. Podstawowe pojęcia w zakresie ochrony danych wynikające z art. 4 RODO oraz ustaw krajowych.
   f. Biblioteka Inspektora ochrony danych.
2. **Zarządzanie ochroną danych w podmiocie:**
   a. Obowiązki administratora opisane w RODO.
   b. Struktura zarządzania ochroną danych a kontekst organizacji.
   c. Inwentaryzacja procesów przetwarzania.
   d. Analiza ryzyka – podstawy.
   e. Wykazywanie się politykami.
   f. Powierzanie danych zgodnie z art.28 RODO.
   g. Retencja danych.
3. **Wyznaczenie IOD:**
   a. Zadania i uprawnienia IOD. Wykonywanie i dokumentowanie pracy.
   b. Obowiązek wyznaczenia IOD.
   c. Wdrożenie IOD we wszystkie istotnie działania podmiotu.
   d. Analiza wyznaczenia IOD a inwentaryzacja czynności przetwarzania.

e. Kompetencje IOD w świetle art. 39 RODO.
f. IOD audytorem ochrony danych.
g. Zorganizowanie współpracy IOD w komórkami organizacyjnymi w tym z działem IT. Umowa z podmiotem zewnętrznym. Warunki wymiany informacji o stanie ochrony danych.

DZIEŃ 2: AUDYT ZGODNOŚCI PRZETWARZANIA DANYCH OSOBOWYCH Z OBOWIĄZUJĄCYMI PRZEPISAMI PRAWA (RODO). PODEJŚCIE PRAKTYCZNE

CELE I KORZYŚCI:

- Omówienie w sposób szczegółowy kwestii związanych z przeprowadzeniem audytu wewnętrznego w zgodności z RODO.
- Uczestnikom przedstawiony zostanie przykładowy protokół poaudytowy.
- Zostaną omówione elementy składowe audytu oraz różnice miedzy audytem całościowym i audytem problemowym.
- Udział w szkoleniu pozwoli również na poznanie odmiennych form przeprowadzania audytu, a w konsekwencji realizacji obowiązków wynikających z RODO.
- Poruszane na szkoleniu zagadnienia oraz udostępnione materiały pozwolą uczestnikom na samodzielne przeprowadzenie audytu.

PROGRAM:

1. Podstawy przeprowadzenia audytu – wprowadzenie.
2. Zakres tematyczny audytu pod kątem zgodności z RODO - audyt całościowy, audyt problemowy (różnice w podejściu do zakresu czynności kontrolnych).
3. Formy realizacji audytu - (lista kontrolna, audyt opisowy) – jak przygotować plan audytu oraz jaką formę audytu wybrać - przykłady.
4. Praktyczne aspekty przeprowadzenia audytu – metodologia przeprowadzenia audytu – przykłady.
5. Zakres objęty audytem:
   a. weryfikacja procedur, regulaminów i instrukcji postępowania,
   b. diagnoza problemów związanych z przestrzeganiem zasady adekwatności, celowości oraz czasowości przetwarzania danych osobowych,
   c. uwzględnianie ochrony danych w fazie projektowania oraz ich domyślnej ochrony,
   d. przegląd systemów informatycznych pod kątem zastosowanych zabezpieczeń w procesie przetwarzania danych osobowych,
   e. umowy na świadczenie usług z podmiotami zewnętrznymi – uregulowanie zapisów pod kątem powierzania przetwarzania danych,
   f. analiza realizacji praw osób, których dane dotyczą,
   g. weryfikacja dokumentacji bezpieczeństwa teleinformatycznego i fizycznego w zakresie jej aktualności i kompletności oraz przestrzegania zapisów w niej zawartych.
6. Podsumowanie audytu i przygotowanie wniosków i zaleceń poaudytowych.
7. Panel dyskusyjny.

DZIEŃ 3: SZACOWANIE RYZYKA DLA OCHRONY DANYCH JAKO ELEMENT KLUCZOWY W PROCESIE ROZLICZALNOŚCI ADMINISTRATORA DANYCH Z ZASTOSOWANYCH ZABEZPIECZEŃ FIZYCZNYCH I ORGANIZACYJNYCH.

CELE I KORZYŚCI:

- Omówienie kwestii związanych z przeprowadzeniem oceny ryzyka dla operacji przetwarzania danych osobowych.
- Omówione zostaną w sposób praktyczny działania dotykające podejścia opartego na ryzyku z uwzględnieniem zasad identyfikacji obszaru wymagającego oceny ryzyka.
- Poznanie zasad przeprowadzania oceny ryzyka oraz analizy zagrożeń z jednoczesnym nabyciem umiejętności samodzielnego wykonania niniejszych zadań.
- Nabycie umiejętności dokonania oceny stopnia wdrożenia zasad bezpieczeństwa informacji oraz realizacji obowiązków wynikających z RODO.
- Wdrożenie procedur w związku z wykorzystaniem narzędzia do komunikacji zdalnej (komunikator internetowy) w pracy urzędu, w celu realizacji obowiązków wynikających z RODO (obniżenie ryzyka naruszenia praw i wolności osób fizycznych.

PROGRAM:

1. Przeprowadzenia szacowania ryzyka dla ochrony danych, jako elementu kluczowego w procesie rozliczalności Administratora danych z zastosowanych zabezpieczeń fizycznych i organizacyjnych przetwarzania danych osobowych. Kiedy należy przeprowadzić ocenę ryzyka. Na przykładzie omówione zostaną główne założenia szacowania ryzyka.

2. Wyrok TSUE w sprawie Schrems II, w kontekście oceny ryzyka związanego z przekazywaniem danych do państwa trzeciego, konsekwencje niedoszacowania wagi zagrożeń.
3. Ocena zagrożeń prawdopodobieństwo ich wystąpienia - kluczowe składowe szacowania ryzyka – jak je ustalić jak dokonać oceny wagi zagrożeń.
4. Wdrożenie procedur i instrukcji postępowania w celu minimalizacji wystąpienia ryzyka naruszenia ochrony danych osobowych w kontekście rozliczalności wdrożonych zabezpieczeń - na przykładzie zdefiniowanych procesów przetwarzania danych,
5. Ocena ryzyka, szczegółowe omówienie:
   a. Wybór metody analizy ryzyka (poruszone zostaną praktyczne aspekty przeprowadzenia szacowania ryzyka z przykładami i procedurami na podstawie wykorzystania metody CRAMM (CCTA Risk Analysis and Management Method).
   b. Identyfikacja i oszacowanie zasobów (aktywów).
   c. Identyfikacja i oszacowanie następstw wystąpienia incydentu - test równowagi.
   d. Opis środowiska – zabezpieczenia danych.
   e. Identyfikacja zagrożeń i określenie ich poziomu.
   f. Atrybuty uwzględniane w tabeli szacowania ryzyka dla ochrony danych: dostępność, poufność i integralność.
   g. Podatności na ryzyko, określenie poziomu ryzyka.
   h. Określenie warunków obniżenia ryzyk.
   i. Karty szacowania ryzyka.
   j. Ocena ryzyka – podsumowanie.
6. Przykładowe dokumenty z zakresu przeprowadzenia oceny ryzyka i ich omówienie.
7. Wprowadzenie zabezpieczeń na podstawie wyników przeprowadzonej oceny ryzyka: zabezpieczenia fizyczne, organizacyjne, oraz zabezpieczenia w systemach informatycznych służących do przetwarzania danych osobowych.
8. Wyrok TSUE w sprawie Schrems II, w kontekście oceny ryzyka związanego z przekazywaniem danych do państwa trzeciego, konsekwencje niedoszacowania wagi zagrożeń.
9. Przykładowa dokumentacja związana z wdrożeniem w urzędzie narzędzia do komunikacji zdalnej, na przykładzie jednego z dostępnych komunikatorów internetowych – omówienie procedury wdrożenia.
10. Panel dyskusyjny.

DZIEŃ 4: NARUSZENIA, KONTROLA OCHRONY DANYCH OSOBOWYCH, POSTĘPOWANIE W SPRAWACH Z ZAKRESU OCHRONY DANYCH ORAZ ZAKRES ODPOWIEDZIALNOŚCI

CELE I KORZYŚCI:

Naruszenia ochrony danych osobowych to moment krytyczny dla jednostki, podobnie rzecz się ma z kontrolą ochrony danych osobowych dokonywaną przez Prezesa UODO. To postępowanie, które wymaga szczególnej uwagi i przygotowania po stronie administratora lub podmiotu przetwarzającego. Warto przygotować się na wypadek kontroli oraz postępowania w przedmiocie naruszenia ochrony danych osobowych. Omówione zostaną zagadnienia dotyczące:

- postępowania kontrolnego Prezesa UODO,
- wiedzy o kompetencjach kontrolujących,
- zasad obsługi naruszeń ochrony danych osobowych,
- umiejętność rozróżnienia zakresów i zasad odpowiedzialności związanej z naruszeniami przepisów o ochronie danych osobowych.

PROGRAM:

1. Case study, jak postępować wewnątrz organizacji w przypadku stwierdzenia naruszenia ochrony danych osobowych.
2. Udzielanie informacji dotyczącej naruszenia ochrony danych osobowych Prezesowi UODO.
3. Jak przygotować się do kontroli Prezesa Urzędu Ochrony Danych Osobowych.
4. Przebieg kontroli i kompetencje kontrolujących.
5. Rola pracowników kontrolowanego w trakcie kontroli.
6. Dokumentowanie w trakcie kontroli i wykazywanie rozliczalności.
7. Protokół i zgłaszanie zastrzeżeń.
8. Odpowiedzialność karna w związku z kontrolą.
9. Postępowanie w przedmiocie naruszenia ochrony danych osobowych – praktyczne aspekty.
10. Odpowiedzialność administracyjnoprawna a odpowiedzialność cywilna, karna i prawno - pracownicza.

ADRESACI ›

Osoby wyznaczone w Jednostce do realizacji i nadzoru zadań z zakresu bezpieczeństwa informacji, ochrony danych osobowych (m.in. IOD, ASI), osoby pełniące funkcje kierownicze i/lub zatrudnione na samodzielnych stanowiskach pracy, zaangażowane w proces budowania i oceny stanu bezpieczeństwa przetwarzania informacji w Jednostce, w tym osoby bezpośrednio zaangażowane w proces organizacji pracy zdalnej, podmioty, które chcą przetwarzać dane osobowe w sposób zgodny z przepisami.

PROWADZĄCY

- Współtwórca i były wykładowca studiów podyplomowych z zakresu ochrony danych osobowych. 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. Expert Dekra Polska. Certyfikowany trener biznesu. Asesor kompetencji zawodowych. Członek Stowarzyszenia Praktyków Ochrony Danych. Praktyk sponad dziesięcioletnim doświadczeniem w ochronie danych, 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.

- Inspektor Ochrony Danych w jednostkach samorządowych, w tym oświatowych, oraz w innych jednostkach sektora publicznego, m.in. w podmiotach medycznych, zajmująca się wdrożeniami procedur ochrony danych osobowych w podmiotach sektora publicznego oraz prywatnego. Absolwentka Politechniki Opolskiej Wydziału Elektrotechniki i Automatyki kierunek Informatyka, oraz studiów podyplomowych w Wyższej Szkole Biznesu w Dąbrowie Górniczej na kierunku: „Ochrona danych osobowych w administracji i biznesie - Inspektor ochrony danych" realizowanym we współpracy z Generalnym Inspektorem Ochrony Danych Osobowych oraz Krajowym Stowarzyszeniem Ochrony Informacji Niejawnych. Posiada certyfikat Auditora wewnętrznego QMS i ISMS Wojskowej Akademii Technicznej im. Jarosława Dąbrowskiego w Warszawie.

- Jest doktorem nauk prawnych, radcą prawnym, wiceprezesem SBC Inspektor Sp. z o.o. oraz redaktorem naczelnym kwartalnika "ABI Expert", członkinią kadry naukowej Instytutu Prawa Nowych Technologii i Ochrony Danych Osobowych na Uczelni Łazarskiego. Specjalizuje się w ochronie danych osobowych, dostępie do informacji publicznej, ponownym wykorzystywaniu informacji sektora publicznego, prawie konstytucyjnym i samorządowym. Jest autorką kilkudziesięciu publikacji z zakresu ochrony danych osobowych i prawa informacyjnego, w tym pierwszej na rynku książki o tematyce ochrony danych w pracy zdalnej – „Ochrona danych osobowych w warunkach pracy zdalnej", Wolters Kluwer, 2020. Pod jej redakcją powstał komentarz do RODO – „Ogólne rozporządzenie o ochronie danych osobowych", C.H. Beck 2018. Bierze czynny udział w konferencjach naukowych oraz branżowych seminariach poświęconych ww. problematyce. Jest autorką koncepcji merytorycznych cyklicznych forów branżowych. Wykłada na Uniwersytecie Łódzkim, Uniwersytecie Wrocławskim, Uniwersytecie Kardynała Stefana Wyszyńskiego, w Polskiej Akademii Nauk, w Uczelni Łazarskiego, Akademii Leona Koźmińskiego, w Wyższej Szkole Bankowej w Poznaniu oraz w Górnośląskiej Wyższej Szkole Handlowej. Jako ABI organizowała i nadzorowała system ochrony danych osobowych, obecnie uczestniczy we wdrożeniach i audytach systemów ochrony danych osobowych.

- Radca prawny i partner w Sakowska-Baryła, Czaplińska Kancelarii Radców Prawnych Sp.p. specjalizującej się sprawach z zakresu ochrony danych osobowych, prawa autorskiego i informacyjnego, prezes w SBC Inspektor Sp. z o.o., doktorantka w Katedrze Prawa Gospodarczego i Handlowego na Wydziale Prawa i Administracji Uniwersytetu Łódzkiego, przygotowuje dysertację na temat odpowiedzialności cywilnej na gruncie RODO. W ramach świadczenia pomocy prawnej współpracuje z podmiotami gospodarczymi i jednostkami sektora finansów publicznych. Na co dzień zajmuje się wdrożeniami ochrony danych osobowych, przygotowując podmioty gospodarcze i jednostki sektora finansów publicznych do stosowania zabezpieczeń zgodnych z wymogami RODO. Prowadzi szkolenia i warsztaty – ma za sobą kilkadziesiąt autorskich szkoleń. Autorka publikacji w prasie branżowej w tym w „ABI Expert" - magazynie poświęconym ochronie danych i informacji, współautorka monografii „Miasto w budowie. Prawne problemy inwestycji komunalnych" oraz „Samorządowe centra usług wspólnych".

.

Fundacja Rozwoju Demokracji Lokalnej
im. Jerzego Regulskiego

INFORMACJE ORGANIZACYJNE I KARTA ZGŁOSZENIA

KURS: ZARZĄDZENIE BEZPIECZEŃSTWEM INFORMACJI ORAZ OCHRONA DANYCH OSOBOWYCH W JEDNOSTKACH SAMORZĄDU TERYTORIALNEGO

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

18, 19, 20 oraz 21 maja 2021 r. Kurs w godzinach: 9.00 – 13.00

Cena: 890 PLN netto/os.
Udział w kursie 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:	FRDL 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……

Dokonanie zgłoszenia na kurs 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 przesłać poprzez formularz zgłoszenia na www.frdl.rzeszow.pl lub mailem na adres post@frdl.rzeszow.pl do 13 maja 2021 r.

UWAGA **Liczba miejsc ograniczona**. O udziale w kursie decyduje kolejność zgłoszeń. Zgłoszenie na kurs 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 _____