Fundacja Rozwoju Demokracji Lokalnej
im. Jerzego Regulskiego

SZKOLENIE ON LINE
23-24 marca 2022 r.

BEZPIECZEŃSTWO INFORMACJI I OCHRONA DANYCH OSOBOWYCH W ADMINISTRACJI. PRACA ZDALNA, CYBERBEZPIECZEŃSTWO, ZAGADNIENIA PRAKTYCZNE

WAŻNE INFORMACJE O SZKOLENIU:

Celem proponowanego szkolenia jest przypomnienie obowiązujących i znowelizowanych przepisów i wynikających z nich zasad bezpieczeństwa informacji, w tym ochrony danych osobowych, przy realizacji zadań w administracji oraz podniesienie kwalifikacji i świadomości pracowników co do odpowiedzialności w tym zakresie. Ważnym elementem szkolenia jest zwrócenie uwagi na nowe wymagania stawiane przez RODO, także w związku z pracą zdalną tj. poza obszarem przetwarzania danych (w miejscu zamieszkania a także poza nim). Zajęcia prowadzone będą częściowo w formie wykładu, warsztatów a także dyskusji angażującej uczestników przy rozwiązywaniu przypadków przygotowanych w oparciu o faktyczne zaistniałe sytuacje. Przed szkoleniem uczestnicy rozwiązują test samosprawdzający, a w trakcie warsztatów sami konfrontują udzielone przez siebie odpowiedzi ze stanem faktycznym. W części warsztatowej przeprowadzone zostaną ćwiczenia z zakresu klasyfikacji informacji oraz analizę decyzji administracyjnych wydanych przez Prezesa Urzędu Ochrony Danych Osobowych, po przeprowadzonych kontrolach w administracji.

CELE I KORZYŚCI:

- Zdobycie praktycznej wiedzy z zakresu zasad bezpieczeństwa informacji i przetwarzania danych osobowych w jednostce.
- Zapoznanie z najnowszymi przepisami obowiązującymi zakresie bezpieczeństwa informacji i ochrony danych osobowych.
- Uzyskanie praktycznych umiejętności z przedmiocie prawidłowego stosowania zasad bezpieczeństwa informacji i przetwarzania danych osobowych na swoim stanowisku pracy, w jednostce i poza nią, w przypadku konieczności pracy zdalnej.
- Uzyskanie praktycznej wiedzy na temat ryzyka incydentów związanych z cyberbezpieczeństwemm sposobu rozpoznawania i prawidłowego postępowania po ich zidentyfikowaniu.

PROGRAM:

Dzień I

1. **Podstawowe pojęcia związane z realizacja polityki bezpieczeństwa informacji w JST**.
   - Informacja: poufność, integralność, dostępność - incydenty.
2. **Bezpieczeństwo informacji a wymagania prawne - przykłady uregulowań ustawowych.**
   - Ustawa o ochronie informacji niejawnych.
   - RODO oraz ustawa o ochronie danych osobowych
   - Ustawa o dostępie do informacji publicznej.
   - KPA i ordynacja podatkowa.
   - Ustawa o rachunkowości.
   - Ustawa o zwalczaniu nieuczciwej konkurencji.
   - Prawo zamówień publicznych.
   - Ustawa o pracownikach samorządowych.
   - Prawo prasowe.
   - Ustawa o statystyce publicznej.
   - Kodeks pracy.
3. **Ochrona informacji niejawnych - podstawowe informacje.**
   - Klasyfikacja : „ściśle tajne”, „tajne”, „poufne”, „zastrzeżone”.
   - Zasady dostępu do informacji niejawnych, dopuszczenia do informacji „zastrzeżonych”, przykładowy obieg informacji „zastrzeżonej”.
   - Rola i zadania kierownika jednostki i pełnomocnika ds. Ochrony informacji niejawnych.
   - Poświadczenia bezpieczeństwa.

4. **Ochrona danych osobowych, najważniejsze definicje RODO** - znaczenie praktyczne w administracji (dane osobowe, przetwarzanie, ograniczenie przetwarzania, profilowanie, zbiór danych, administrator, podmiot przetwarzający, odbiorca, zgoda, naruszenie ochrony danych osobowych, dane biometryczne, dane dot. zdrowia, organ nadzorczy).
5. **Zasady przetwarzania danych osobowych** - szczegóły obsługi klienta, na które należy zwrócić szczególną uwagę, Kserowanie dokumentów tożsamości do dokumentacji sprawy.
6. **Legalność przetwarzania danych osobowych - przesłanki** - zgoda osoby, której dane dotyczą /w tym wyrażenie zgody przez dziecko/; wykonanie umowy, której stroną jest osoba, której dane dotyczą; wypełnienie obowiązku prawnego ciążącego na administratorze; ochrona żywotnych interesów osoby, której dane dotyczą; wykonanie zadania realizowanego w interesie publicznym; prawnie uzasadnione interesy realizowane przez administratora - wyłączenia organów administracji publicznej.
7. **Zgoda na przetwarzanie danych osobowych** - warunki wyrażenia zgody, przejrzystość formuły, przykłady stosowanych formuł w administracji. Kiedy zgoda nie jest potrzebna ? Najczęstsze błędy popełniane przy pozyskiwaniu zgód w trakcie postępowań administracyjnych.
8. **Przetwarzanie danych szczególnych kategorii danych osobowych - wrażliwych** - kategorie tych danych wg RODO, przesłanki ich przetwarzania.

Dzień II

9. **Zasady prowadzenia monitoringu wizyjnego** - kodeks pracy, ustawa o samorządzie gminnym i powiatowym oraz ustawa prawo oświatowe. Monitoring wizyjny a prawo do ochrony własnego wizerunku.
10. **Obowiązek informacyjny administratora danych** - informacje na wniosek osoby, której dane są przetwarzane a informacje przekazywane „z urzędu". Zakres informacji, które należy przekazać osobom, których dane będą przetwarzane; przejrzystość przekazywanych informacji; praktyczna realizacja obowiązku informacyjnego w przypadku zbierania danych od osoby, której dane dotyczą oraz w przypadku innego trybu ich pozyskania.- wzór klauzuli informacyjnej. Okoliczności, w których administrator jest zwolniony z obowiązku informacyjnego. Przykłady stosowanych formuł. Realizacja w BIP. Czy podpis pod klauzulą informacyjną jest niezbędny.
11. **Prawa osoby, której dane dotyczą** - prawo dostępu do swoich danych i ich poprawiania, „prawo do bycia zapomnianym", prawo do ograniczenia przetwarzania danych, prawo do przenoszenia danych, prawo do sprzeciwu, prawa związane z profilowaniem - czy zawsze mają zastosowanie, czy informować o wszystkich prawach w klauzuli informacyjnej?
12. **Podmiot przetwarzający dane w imieniu administratora** - obowiązki i odpowiedzialność podmiotu przetwarzającego dane w imieniu administratora - umowa o powierzeniu przetwarzania danych podmiotowi przetwarzającemu przez administratora danych. Niezbędne elementy umowy i z jakimi podmiotami należy ją podpisać? Z jakimi podmiotami taka umowa nie jest potrzebna?
13. **Zapewnienie bezpieczeństwa danych osobowych** - upoważnienia do przetwarzania danych osobowych. Kto powinien uzyskać upoważnienie.? Przykłady stosowanych upoważnień. Czy pracownicy działów gospodarczych powinni posiadać upoważnienia? Umowa o powierzeniu czy upoważnienie do przetwarzania danych osobowych.
14. **Obowiązek zgłaszania naruszenia ochrony danych osobowych organowi nadzorczemu** - informacje, które powinny znaleźć się w zgłoszeniu. Kiedy zgłoszenie jest obligatoryjne? (przykłady).
15. **Obowiązki pracowników administracji w zakresie realizacji RODO** - wobec klientów, stron postępowania administracyjnego, obowiązki pracodawcy wobec pracowników.
16. **RODO a stan zagrożenia epidemiologicznego lub epidemii** - zagadnienia praktyczne. zasady ochrony informacji podczas pracy zdalnej.
17. **Ochrona danych osobowych a KPA.**
18. **Ochrona danych osobowych a udostępnianie informacji publicznej.**
19. **Cyberbezpieczeństwo, zabezpieczanie urządzeń końcowych**.
20. **Analiza wybranych decyzji Prezesa Urzędu Ochrony Danych Osobowych jako wynik przeprowadzonych kontroli w jednostkach administracji.**
21. **Absurdy RODO -** przykłady zbędnych praktyk.

ADRESACI:

Pracownicy administracji samorządowej i rządowej, w szczególności osoby zajmujące się przetwarzaniem danych osobowych, IODO.

PROWADZĄCY:

Specjalista z zakresu procedur administracyjnych (KPA, ochrona danych osobowych, informacji publicznej, szkolenia radnych)i systemów zarządzania w jednostkach samorządu terytorialnego. Wykładowca na wielu unijnych programach szkoleniowych (m.in. „Expert - Urzędnik"," Urząd na miarę Europy"). Doświadczony trener oraz samorządowiec-praktyk, szkolący od kilkunastu lat pracowników administracji samorządowej i rządowej na terenie całego kraju. (urzędy miast i gmin, starostwa powiatowe, urzędy marszałkowskie, jednostki organizacyjne JST, urzędy wojewódzkie, NFZ, IPN, KWP, UKE, KAS). Rocznie przeprowadza ok.100-150 szkoleń z w/w tematów na terenie całej Polski.

Fundacja Rozwoju Demokracji Lokalnej
im. Jerzego Regulskiego

INFORMACJE ORGANIZACYJNE I KARTA ZGŁOSZENIA

Bezpieczeństwo informacji i ochrona danych osobowych w administracji. Praca zdalna, cyberbezpieczeństwo- zagadnienia praktyczne

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

23-24 marca 2022 r. **Szkolenie w godzinach 9:30-14:00**

Cena: 599 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 Centrum Mazowsze ul. Żurawia 43, 00-680 Warszawa tel. (42) 307 32 65, fax: (42) 288 12 86 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 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.mazowsze.pl** oraz zawartej w nim Polityce prywatności i ochrony danych osobowych.

Wypełnioną kartę zgłoszenia należy przesłać poprzez formularz zgłoszenia na www.frdl.mazowsze.pl do 18 marca 2022 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 _____