

## **RODO OKIEM PRAKTYKA. CO TRZEBA WIEDZIEĆ, ABY PRAWIDŁOWO CHRONIĆ DANE OSOBOWE W INSTYTUCJI?**

### **WAŻNE INFORMACJE:**

Właściwe stosowanie przepisów o RODO jest dość skomplikowane, choć od momentu wejścia ich w życie upłynęło już kilka lat, prawidłowość stosowania regulacji prawnych w praktyce nadal budzi wiele problemów. Unaocznili to raport Najwyższej Izby Kontroli o nieprawidłowościach w ochronie danych osobowych w jednostkach samorządu terytorialnego, którego skala jest ogromna. W celu poprawnego stosowania przepisów proponujemy Państwu uczestnictwo w praktycznych zajęciach z zakresu ochrony danych osobowych w instytucji.

#### Podczas zajęć:

- **Wskażemy, jak prawidłowo należy przetwarzać dane osobowe, w tym dane w pracowników oraz dane w procesach rekrutacyjnych.**
- **Podpowiemy, jakie stosować środki bezpieczeństwa w jednostce.**
- **Przypomnimy, kto odpowiada za przestrzeganie danych osobowych w instytucji, jaka jest rola IOD.**
- **Umożliwimy weryfikację wiedzy i umiejętności w celu prawidłowego stosowania przepisów dotyczących ochrony danych osobowych i bezpieczeństwa informacji.**
- **Przedstawimy nieprawidłowości w zakresie ochrony danych osobowych po kontroli NIK.**

Prowadzący, praktyk z wieloletnim doświadczeniem zawodowym w UOP/ABW, przedstawi w sposób przejrzysty, na podstawie konkretnych rozwiązań, pomocne przykłady dotyczące właściwego stosowania przepisów o RODO w instytucji z uwzględnieniem wyników raportu NIK o nieprawidłowościach w ochronie danych osobowych w jednostkach samorządu terytorialnego.

### **CELE I KORZYŚCI ZE SZKOLENIA:**

- Poszerzenie i przypomnienie wiedzy dotyczącej prawnych i praktycznych aspektów ochrony danych osobowych.
- Omówienie prawidłowej realizacji uprawnień, obowiązków i procedur związanych z przestrzeganiem RODO w jednostce.
- Zdobycie niezbędnej wiedzy oraz praktycznych umiejętności dotyczących przepisów o RODO, w szczególności zasad przetwarzania danych, zabezpieczeń danych zarówno w wersji papierowej, jak i elektronicznej, monitoringu wizyjnego.
- Nabycie kompetencji i praktycznych umiejętności w zakresie ochrony danych osobowych w instytucji.
- Przypomnienie i wskazanie na przykładach, jakie są zasady i środki zabezpieczenia danych osobowych.
- Możliwość zapoznania się z praktycznym stosowaniem przepisów, uzyskania odpowiedzi na najczęściej pojawiające się kwestie problemowe z tematyki szkolenia, wyeliminowania błędów i nieprawidłowości w bieżącej pracy.
- Uzyskanie odpowiedzi na pytania:
  - Kto ponosi odpowiedzialność za bezpieczeństwo danych osobowych w jednostce?
  - Jak prawidłowo należy przetwarzać dane osobowe, w tym dane w pracowników oraz dane w procesach rekrutacyjnych?
  - Jak stosować środki bezpieczeństwa w jednostce?
  - Jak oceniać zagrożenia?
  - Czym różni się pseudonimizacja od anonimizacji danych?
  - Jak stosować zasady przetwarzania danych w praktyce?
  - Jakie zadania ma Administrator Danych Osobowych (ADO) i Inspektor Ochrony Danych?
  - Jak rejestrować czynności przetwarzania danych?
  - Jak poprawnie zgłaszać naruszenia ochrony danych do organu nadzorczego? Jakie są procedury? Jak reagować na incydenty?
  - Jak właściwie zabezpieczyć komputer, pocztę elektroniczną?

- W jaki sposób można monitorować pracowników?
- Czy pracodawca może mieć wgląd do służbowych maili pracowników?

## **PROGRAM:**

- 1. System prawa ochrony danych osobowych po wejściu w życie rozporządzenia RODO.**
- 2. Zakres podmiotowy i przedmiotowy RODO.**
- 3. Podstawowe pojęcia z zakresu ochrony danych osobowych:**
  - Dane osobowe.
  - Przetwarzanie danych.
  - Profilowanie danych.
  - Pseudonimizacja i anonimizacja danych.
  - Zbiór danych.
  - Administrator danych osobowych (ADO).
  - Inspektor ochrony danych (DPO/IOD).
  - Osoba upoważniona do przetwarzania danych.
- 4. Ogólne zasady przetwarzania danych na gruncie RODO:**
  - Legalność i przejrzystość.
  - Celowość (ograniczenie celu)
  - Adekwatność (minimalizacja),
  - Merytoryczna poprawność.
  - Ograniczenie czasowe.
  - Poufność i integralność danych.
  - Rozliczalność.
- 5. Prawa osób, których dane dotyczą - zasady realizacji uprawnień, obowiązki i procedury:**
  - Prawo do przejrzystości danych.
  - Prawo dostępu do danych.
  - Prawo do sprostowania i usunięcia danych.
  - Prawo do ograniczenia przetwarzania.
  - Prawo do przenoszenia danych.
  - Prawo do sprzeciwu.
  - Prawa związane z profilowaniem danych.
  - Prawo skargi do organu nadzorczego.
- 6. Organizacja systemu ochrony danych – podstawowe obowiązki Administratora Danych:**
  - Powołanie Inspektora Ochrony Danych.
  - Stosowanie mechanizmów ochrony danych (privacy by design, privacy by default).
  - Rejestrowanie czynności przetwarzania danych.
  - Zgłaszanie naruszeń ochrony danych do organu nadzorczego.
  - Zawiadamianie osób, których dane dotyczą o naruszeniach.
  - Zabezpieczenie danych osobowych (wewnętrzne polityki, techniczne i organizacyjne środki ochrony danych, zapewnienie poufności, integralności, dostępności).
  - Zapewnienie ciągłości działania.
  - Testowanie, mierzenie i ocena skuteczności ochrony danych.
  - Ocena skutków dla ochrony danych.
  - Szacowanie ryzyka.
  - Obowiązki związane z powierzeniem danych.
- 7. Podstawy prawne legalizujące przetwarzanie danych osobowych w procesach kadrowych:**
  - Przesłanki prawne legalizujące przetwarzanie danych osobowych zwykłych, szczególnych kategorii danych oraz danych na temat karalności (art. 6, 9 i 10 RODO).
  - Warunki korzystania ze zgody pracownika przez pracodawcę.
- 8. Procesy rekrutacji i naboru:**
  - Ogłoszenia o naborze, obowiązek informacyjny oraz rekrutacje ukryte.
  - Gromadzenie i udostępnianie CV kandydatów.
  - Profilowanie kandydatów i weryfikacja informacji z CV w oparciu o dane ogólnodostępne.
  - Zasady postępowania z CV kandydatów po zakończonym naborze.
  - CV otrzymane doraźnie (poza procedurą naboru).
  - Wykorzystywanie otrzymanych CV przy kolejnych rekrutacjach.

## 9. Dokumentacja kadrowo – płacowa w trakcie zatrudnienia:

- Pojęcie „danych służbowych”.
- Dane i dokumenty, jakie pracodawca może żądać od pracownika.
- Akta osobowe pracowników.
- Listy obecności i grafiki zmianowe.
- Outsourcing danych kadrowych na przykładzie badań profilaktycznych.
- Przetwarzanie danych kadrowych przy okazji ubezpieczeń grupowych oraz benefitów pracowniczych.
- Wykorzystanie wizerunku pracownika oraz zdjęcia na identyfikatorach.
- Gromadzenie szczególnych kategorii danych w związku z ZFŚS oraz PKZP.
- Postępowanie z wnioskami ze strony uprawnionych organów (policja, prokuratura, urzędy) o udostępnienie danych osobowych.
- Przesyłanie danych osobowych do odbiorców zewnętrznych oraz udzielanie informacji na telefon.
- Przetwarzanie danych osobowych po ustaniu stosunku pracy.

## 10. Monitoring w zakładzie pracy:

- Formy monitoringu i cele ich stosowania.
- Wymogi formalne związane z wprowadzeniem monitoringu.
- Wgląd do służbowych e-maili pracowników.
- Ocena pracownika na podstawie jego aktywności w Internecie.
- Dopuszczalność śledzenia pracowników w sieciach społecznościowych, monitoring byłych pracowników.
- Śledzenie mobilnych pracowników (GPS, telefony komórkowe).

## 11. Jak należy skutecznie zabezpieczyć dane osobowe w wersji papierowej i elektronicznej?

- Zasady:
  - Zasada wiedzy uzasadnionej.
  - Zasada czystego ekranu.
  - Zasada czystego biurka.
  - Zasada czystych drukarek.
  - Zasada czystej tablicy.
  - Zasada czystego kosza.
- Środki zabezpieczenia danych osobowych:
  - Zasady dostępu do pomieszczeń.
  - Bezpieczeństwo pasywne.
  - Procedura zarządzania kluczami od pomieszczeń.
  - Loginy.
  - Polityka haseł.
  - Wygaszacze ekranów.
  - Komputery przenośne i "praca na odległość".
  - Komputerowe nośniki danych.
  - Kopie bezpieczeństwa.
  - Zabezpieczenia przed szkodliwym oprogramowaniem.
  - Zabezpieczenia kryptograficzne.
  - Procedury reagowania na incydenty.

## 12. Przedstawienie wyników raportu NIK o nieprawidłowościach w ochronie danych osobowych w jednostkach samorządu terytorialnego.

## 13. Pytania i konsultacje indywidualne.

### ADRESACI:

Inspektorzy ochrony danych, specjaliści ds. ochrony danych osobowych i bezpieczeństwa informacji, osoby obsługujące prawnie sektor publiczny i jednostki organizacyjne sektora publicznego.

### 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.

## RODO okiem praktyka. Co trzeba wiedzieć, aby prawidłowo chronić dane osobowe w instytucji?



Szkolenie będziemy realizowali w formie webinarium on line.



**18 czerwca 2024 r.**

**Szkolenie w godzinach 9:00-13:30**



**Cena: 435 PLN netto/os. Przy zgłoszeniu do 4 czerwca 2024 r. cena wynosi: 399 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:

FRDL Małopolski Instytut Samorządu Terytorialnego i Administracji  
ul. Floriańska 31, 31-019, Kraków  
**Magdalena Stawiarska**, Kierownik zespołu ds. szkoleń  
tel. +48 12 623 72 44, 575 850 930, [szkolenia@mistia.org.pl](mailto:szkolenia@mistia.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 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.mistia.org.pl](http://www.mistia.org.pl) oraz zawartej w nim Polityce prywatności i ochrony danych osobowych.

**Wypełnioną kartę zgłoszenia należy przesać poprzez formularz zgłoszenia  
na [www.mistia.org.pl](http://www.mistia.org.pl) lub mailem na [szkolenia@mistia.org.pl](mailto:szkolenia@mistia.org.pl) do 13 czerwca 2024 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 \_\_\_\_\_