PEŁNI WIEDZY

Kurs Inspektora Ochrony Danych Osobowych (IOD)

Szkolenie online

Data: 25.01.2027 - 27.01.2027 godz. 09:00 - 15:00 **Cena:** **1799 zł** (netto)

Na ostatniej stronie naszej oferty umieściliśmy interaktywny formularz zgłoszeniowy. Jeżeli preferujesz wersję papierową, prosimy o wypełnienie go na **komputerze** lub **drukowanymi literami**, aby zapewnić jak największą czytelność. Skan podpisanego formularza prosimy przesłać na adres **biuro@pelniwiedzy.pl**

Inspektor Ochrony Danych (IOD) to pełni kluczową funkcję w organizacjach przetwarzających dane osobowe. Jego zadaniem jest zapewnienie **zgodności działań organizacji z przepisami** RODO oraz krajowymi regulacjami. Funkcja ta wymaga wszechstronnej wiedzy z zakresu prawa, zarządzania bezpieczeństwem informacji oraz umiejętności praktycznego wdrażania procedur ochrony danych w codziennej działalności firmy.

Kurs IOD został stworzony z myślą o osobach, które chcą profesjonalnie pełnić tę funkcję lub zdobyć wiedzę niezbędną do efektywnego zarządzania ochroną danych osobowych w swojej instytucji.

Podczas szkolenia uczestnicy poznają podstawy prawne ochrony danych osobowych, a także dowiedzą się, jakie obowiązki spoczywają na administratorze danych, procesorze oraz innych podmiotach przetwarzających dane. Przedstawimy również **rolę i zadania Inspektora Ochrony Danych** – od formalnego powołania, poprzez nadzór nad przestrzeganiem przepisów, aż po współpracę z organami nadzorczymi i działami organizacji.

Uczestnicząc w szkoleniu nauczysz się również, jak prowadzić audyty zgodności, analizować ryzyko związane z przetwarzaniem danych oraz wdrażać zasady „privacy by design” i „privacy by default”. Kurs obejmuje szczegółowe omówienie dokumentacji wymaganej przez RODO, w tym rejestrów czynności przetwarzania, polityk ochrony danych oraz umów powierzenia danych.
Dzięki praktycznym warsztatom zdobędziesz umiejętności potrzebne do tworzenia i wdrażania klauzul informacyjnych, reagowania na naruszenia ochrony danych oraz realizacji praw osób, których dane są przetwarzane.

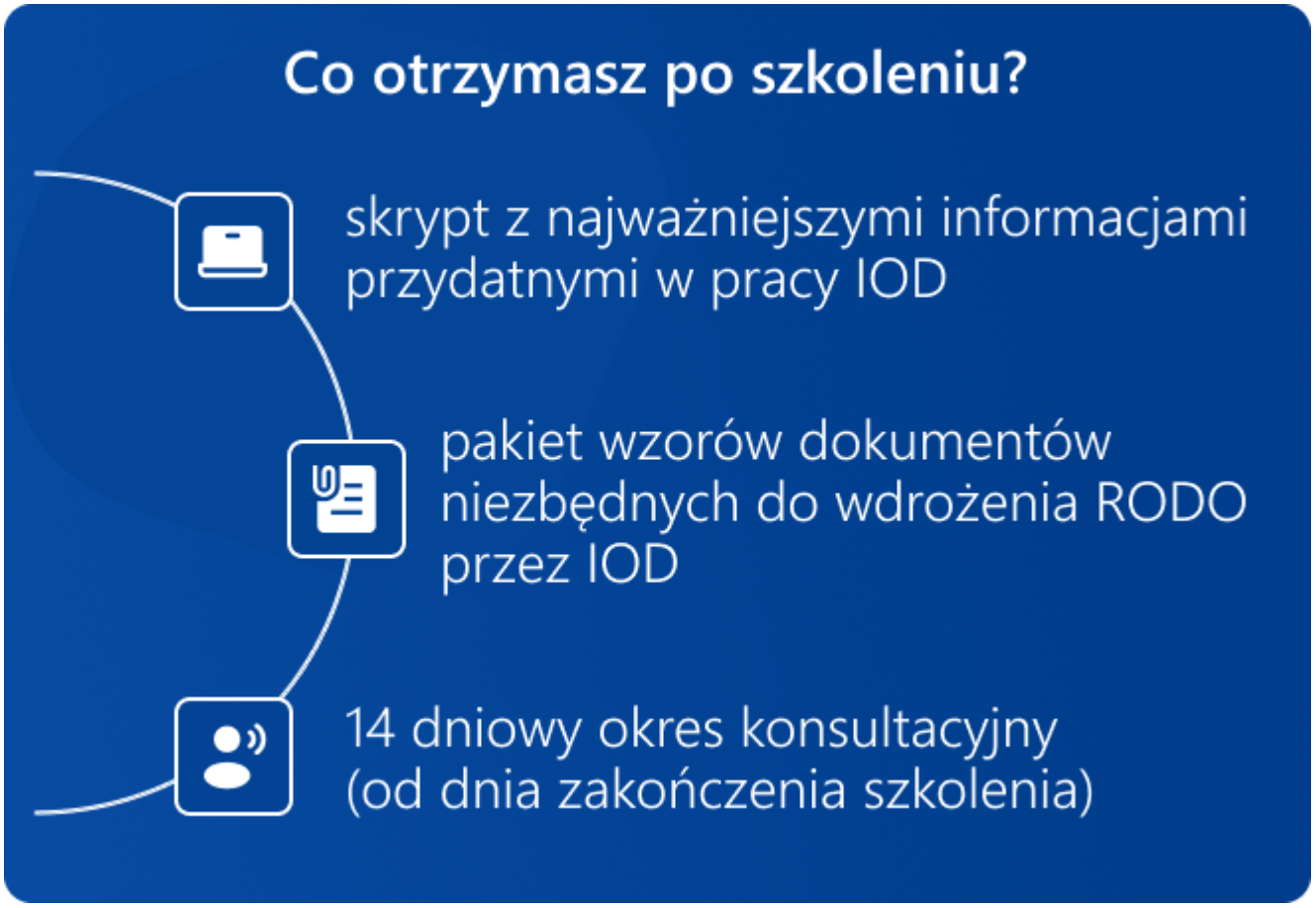
Korzyści z uczestnictwa w szkoleniu IOD:

Uczestnicząc w naszym kursie:

1. Zdobędziesz umiejętność **analizy i praktycznego stosowania przepisów RODO.**
2. Poznasz wszystkie **obowiązki Inspektora Ochrony Danych**, od monitorowania przestrzegania przepisów, przez prowadzenie audytów, po współpracę z organami nadzorczymi.
3. Nauczysz się identyfikować **podstawy prawne przetwarzania danych**, w tym różnice między przetwarzaniem danych zwykłych a szczególnych kategorii.
4. Dowiesz się, jak **projektować procesy przetwarzania danych** w sposób zapewniający bezpieczeństwo i minimalizację ryzyka.
5. Poznasz **techniki analizy ryzyka, oceny skutków dla ochrony danych (DPIA)** oraz wdrażania działań zabezpieczających dane osobowe.
6. Zrozumiesz, jak **identyfikować naruszenia, zgłaszać je do organu nadzorczego** oraz informować osoby, których dane dotyczą.
7. Nauczysz się, jak **obsługiwać wnioski o dostęp do danych**, sprostowanie, przenoszenie czy usunięcie danych, zgodnie z przepisami RODO.
8. Zrozumiesz, jak **planować, przeprowadzać i dokumentować audyty zgodności** oraz oceniać wyniki pod kątem wymagań prawnych.
9. Nauczysz się **wdrażać środki zabezpieczające**, takie jak pseudonimizacja, szyfrowanie danych czy ograniczanie dostępu, zgodnie z zasadami RODO.

Wszystkie prawa zastrzeżone. Materiały szkoleniowe oraz program prezentowany w naszej ofercie są chronione prawem autorskim. Jakiekolwiek nieautoryzowane kopiowanie, reprodukcja, dystrybucja lub wykorzystanie tych materiałów bez wyraźnej zgody jest ściśle zabronione.

PEŁNI WIEDZY



Wybierając nasz kurs online, zyskujesz:

- Bezpośredni kontakt z prowadzącym;
- Możliwość dyskusji i zadawania pytań na bieżąco;
- Komplet materiałów szkoleniowych w cenie;
- Certyfikat od Instytucji Szkoleniowej po zakończeniu nauczania, będący potwierdzeniem zdobytych umiejętności i wiedzy.

Program szkolenia:

Dzień 1:

I. **Wstęp i źródła prawa**

1. Reforma ochrony danych osobowych – z czego wynika, jakie jest jej znaczenie?
2. Jak czytać RODO?
3. Ustawa o ochronie danych osobowych. z 10 maja 2018 r.
4. Ustawa o zmianie niektórych ustaw w związku z zapewnieniem stosowania rozporządzenia 2016/679.
5. Zmiany sektorowe – gdzie odnaleźć sektorowe przepisy o ochronie danych osobowych?

II. **Przepisy dostosowujące do RODO – po 4 maja.**

1. Zminy w kodeksie pracy – co należy o nich wiedzieć?
2. Rekrutacja zgodna z RODO.

Wszystkie prawa zastrzeżone. Materiały szkoleniowe oraz program prezentowany w naszej ofercie są chronione prawem autorskim. Jakiekolwiek nieautoryzowane kopiowanie, reprodukcja, dystrybucja lub wykorzystanie tych materiałów bez wyraźnej zgody jest ściśle zabronione.

3. Kwestionariusze osobowe, akta osobowe, listy obecności regulaminy pracy – jak pozostać w zgodności z nowymi przepisami?
4. Zgoda pracownika na przetwarzanie jego danych osobowych?
5. Wdrażanie monitoringu wizyjnego – obowiązki względem pracowników i osób zewnętrznych.
6. Inne formy monitoringu.

III. **Podstawowe pojęcia i informacje z zakresu Ochrony Danych Osobowych**

1. Czy każdy powinien stosować przepisy RODO?
2. Najważniejsze definicje w RODO.
3. Czym są “dane osobowe”, “przetwarzanie”, „profilowanie”, „pseudoanonimizacja”
4. Kiedy „przetwarzamy dane osobowe”?
5. Kto to jest Administrator i współadministrator danych osobowych?

IV. **Obowiązki Administratora i Podmiotu przetwarzającego, współadministrowanie danymi osobowymi.**

1. Administrator danych, procesor i osoba upoważniona do przetwarzania danych – role w procesie przetwarzania danych osobowych, a zmiany z RODO.
2. Obowiązki Administratora danych.
3. Obowiązki Podmiotu przetwarzającego (procesora).
4. Zmiany w umowach powierzenia danych osobowych.
5. Współadministrowanie danymi osobowych – nowa instytucja RODO.

V. **Kiedy przetwarzamy dane osobowe zgodnie z prawem?**

1. Rodzaje danych osobowych – dane “zwykłe” oraz “szczególne kategorie danych”, w tym biometryczne.
2. Kiedy możemy przetwarzać dane osobowe “zwykłe”, a kiedy “szczególne kategorie danych”?
3. Wymogi dotyczące przetwarzania danych osobowych dzieci.
4. Kiedy jest wymagana zgoda na przetwarzanie danych osobowych?
5. Warunki wyrażenia zgody na przetwarzanie danych osobowych wg RODO.

VI. **Zasady przetwarzania danych osobowych.**

1. Legalność przetwarzania danych osobowych – praktyczne aspekty kryteriów prawnych.
2. Celowość i minimalizm w przetwarzaniu danych osobowych wg RODO.
3. Poprawność merytoryczna przetwarzanych danych.
4. Zasada ograniczonego przechowywania (retencja danych) – omówienie najważniejszych przykładów, praktyczne rozwiązania.
5. Integralność i poufność przetwarzania danych osobowych.
6. Rozliczalność – nadrzędna zasada RODO, jej konsekwencje dla IT.
7. Nowe zasady “privacy by design oraz “privacy by default” i ich praktyczne zastosowanie.

VII. **Prawa osób, których dane osobowe są przetwarzane.**

1. Prawo dostępu do danych oraz prawo uzyskania kopii danych osobowych.
2. Prawo do sprostowania danych.
3. Prawo do bycia zapomnianym.
4. Prawo do ograniczenia przetwarzania.

Wszystkie prawa zastrzeżone. Materiały szkoleniowe oraz program prezentowany w naszej ofercie są chronione prawem autorskim. Jakiekolwiek nieautoryzowane kopiowanie, reprodukcja, dystrybucja lub wykorzystanie tych materiałów bez wyraźnej zgody jest ściśle zabronione.

5. Prawo do przenoszenia danych osobowych.
6. Prawo do sprzeciwu.
7. Prawa osób profilowanych.
8. Jak postępować z żądaniami osób, których dane dotyczą?

VIII. **Obowiązek informacyjny (klauzule informacyjne dotyczące przetwarzania).**

1. Obowiązek informacyjny przy przetwarzaniu danych osobowych – ustawy krajowe oraz RODO.
2. Wymogi formalne z praktycznym omówieniem.
3. Obowiązek informacyjny przy uzyskaniu zgody na przetwarzanie danych osobowych.
4. Obowiązek informacyjny przy wyznaczeniu IOD.
5. Obowiązek informacyjny przy przekazaniu danych osobowych poza EOG.
6. Praktyczny przykład klauzuli informacyjnej z omówieniem.
7. Obowiązek informacyjny w przypadku zbierania danych nie od osoby, której te dane dotyczą.
8. Chwila powstania obowiązków informacyjnych.

IX. **Bezpieczeństwo przetwarzania danych osobowych – przykładowe aspekty praktyczne w kontekście RODO.**

1. Organizacyjne środki zabezpieczenia danych osobowych – ich wybór i dostosowanie zgodnie z RODO, w ujęciu praktycznym.
2. Techniczne środki bezpieczeństwa, ze szczególnym uwzględnieniem wymaganego przez RODO zapewnienia poufności, integralności, dostępności i odporności systemów i usług przetwarzania, pseudonimizacji oraz szyfrowania.
3. Analiza ryzyka przy przetwarzaniu danych osobowych – przykłady praktyczne.
4. Ocena skutków dla ochrony danych osobowych – kiedy jest wymagana.
5. Uprzednie konsultacje z organem nadzorczym.

X. **Naruszenia ochrony danych osobowych**

1. Identyfikacja naruszeń bezpieczeństwa danych osobowych.
2. Co robić w przypadku naruszenia?
3. Obowiązek zgłaszania incydentów z danymi, wynikający z RODO (zasada 72 godzin).
4. Obowiązek powiadamiania osób, których dane osobowe podlegają naruszeniu.
5. Rejestr naruszeń ochrony danych osobowych.

XI. **Odpowiedzialność związana z przetwarzaniem danych osobowych.**

1. Kary finansowe do 4% rocznego obrotu / 20 000 000 EUR – czy to jedyna forma działania organu nadzorczego, czy należy się ich spodziewać?
2. Odpowiedzialność odszkodowawcza.
3. Jak postępować, aby zmniejszyć wymiar potencjalnej kary za naruszenie ochrony danych, w przypadku jego wystąpienia.
4. Sankcje dla podmiotów publicznych.

XII. **Podsumowanie**.

1. Jak podzielić prace wdrożeniowe?

Wszystkie prawa zastrzeżone. Materiały szkoleniowe oraz program prezentowany w naszej ofercie są chronione prawem autorskim. Jakiekolwiek nieautoryzowane kopiowanie, reprodukcja, dystrybucja lub wykorzystanie tych materiałów bez wyraźnej zgody jest ściśle zabronione.

2. Na czym skupić się w pierwszej kolejności?
3. Jak wdrożyć RODO w 6-ciu krokach, w oparciu o wiedzę ze szkolenia oraz materiały szkoleniowe?

III. **Pytania uczestników, dyskusja.**

Dzień 2:

I. **Inspektor Ochrony Danych (IOD)**

1. Kim jest Inspektor Ochrony Danych?
2. Kto może zostać IOD?
3. Kiedy należy wyznaczyć IOD?
4. Powiadomienie PUODO o wyznaczeniu Inspektor Ochrony Danych
   - wypełnianie formularza oraz zgłoszenia
5. Zadania IOD w kontekście RODO, a rzeczywistość.
   - Informowanie o obowiązkach wynikających z przepisów prawa.
   - Nadzór nad przestrzegania przepisów prawa.
   - Szkolenia.
   - Audyty.
   - Współpraca z organem nadzorczym.
   - Pełnie funkcji punktu kontaktowego.
   - Konsultacje w zakresie oceny skutków dla ochrony danych.
6. Współpraca IOD z administratorem danych.
7. Współpraca IOD z działem IT, kadr i innych.
8. Konsultacje w zakresie oceny skutków dla ochrony danych.
9. Status IOD w organizacji.
10. Odpowiedzialność administratora i osób upoważnionych do przetwarzania danych w perspektywie powołania IOD.
11. Formalne powołanie IOD wewnątrz organizacji.
12. IOD zatrudniony czy zewnętrzny? / współpraca z IOD.
13. IOD w grupie kapitałowej.
14. Ubezpieczenia dla IOD i administratora – czy warto z nich korzystać? Analiza umów ubezpieczeniowych – na jakie wyłączenia w szczególności należy zwrócić uwagę.
15. Odpowiedzialność Inspektor Ochrony Danych

II. **Realizacja bieżących obowiązków IOD.**
OBOWIĄZKI INFORMACYJNE.

1. Poprawne definiowanie podstaw przetwarzania danych osobowych – art. 6, art. 9 i art. 10 RODO w praktyce – case study.
2. Dodatkowe obowiązki informacyjne w przypadku współadministrowania danymi – wyzwania płynące z art. 26 RODO.
3. Obowiązki informacyjne – wdrażanie w praktyce. Zalecane formy oraz miejsca ich spełniania. Dobre praktyki.

Wszystkie prawa zastrzeżone. Materiały szkoleniowe oraz program prezentowany w naszej ofercie są chronione prawem autorskim. Jakiekolwiek nieautoryzowane kopiowanie, reprodukcja, dystrybucja lub wykorzystanie tych materiałów bez wyraźnej zgody jest ściśle zabronione.

4. Strona internetowa, BIP – ważne źródło wiedzy o tym, w jaki sposób przetwarzamy dane osobowe.
5. Konstruowanie obowiązków informacyjnych – warsztat.

III. **Kontrola przepływu danych.**

1. Powierzenie a udostępnienie danych osobowych – jak odróżnić te dwie formy przekazywania danych “na zewnątrz”.
2. Najczęstsze przypadki powierzania danych osobowych.
3. Na jakiej podstawie możemy udostępniać dane osobowe?
4. Udostępnienie danych – przykłady praktyczne.
5. Obowiązkowe i fakultatywne elementy umowy powierzenia.
6. Konstruowanie oraz weryfikacja umów powierzenia – warsztat.
7. Przepływ danych między współadministratorami.
8. Rejestry powierzeń i udostępnień.

IV. Postępowania związane z realizacją uprawnień osób, których dane dotyczą

1. Forma składania żądań przez osoby, których dane dotyczą.
2. Z jakimi żądaniami w praktyce spotykamy się najczęściej?
3. Jak przygotować firmę / instytucję do realizacji uprawnień osób, których dane dotyczą, w aspekcie organizacyjnym oraz informatycznym? Główne praktyczne problemy.
4. W jaki sposób realizować uprawnienia osób, których dane dotyczą? Jak poprawnie prowadzić korespondencję?
5. Analiza zasadności roszczeń – case study.

V. **Realizacja bieżących obowiązków IOD - ciąg dalszy**.
POSTĘPOWANIE Z NARUSZENIAMI.

1. Procedura wewnętrznego zgłaszania naruszeń / incydentów. Forma komunikacji z osobami upoważnionymi do przetwarzania danych osobowych.
2. Prowadzenie wewnętrznego rejestru naruszeń – case study.
3. Zgłaszanie naruszeń do organu nadzorczego – kiedy jest obowiązkowe? Czy termin 72 godzin jest nieprzekraczalny?
4. Wypełnianie formularza zgłoszeniowego oraz zgłaszanie naruszeń poprzez e-PUAP – warsztat.
5. Obowiązek zawiadomienia osoby, której dane dotyczą, o naruszeniu ochrony danych osobowych. W jakich przypadkach i w jakiej formie informować o naruszeniach?

VI. **Bezpieczeństwo danych osobowych.**

1. Bezpieczeństwo danych osobowych a bezpieczeństwo informacji.
2. Zagrożenia związane z bezpieczeństwem danych osobowych.
3. Co to jest zagrożenie?
4. Rodzaje zagrożeń i sposoby przeciwdziałania.
5. Zarządzanie incydentami związanymi z bezpieczeństwem danych osobowych.
6. Bezpieczeństwo fizyczne i środowiskowe.
7. Bezpieczeństwo osobowe.
8. Bezpieczeństwo teleinformatyczne.

VII. **Wdrażanie RODO.**

Wszystkie prawa zastrzeżone. Materiały szkoleniowe oraz program prezentowany w naszej ofercie są chronione prawem autorskim. Jakiekolwiek nieautoryzowane kopiowanie, reprodukcja, dystrybucja lub wykorzystanie tych materiałów bez wyraźnej zgody jest ściśle zabronione.

1. Przygotowanie planu wdrożenia.
2. Uwzględnianie ochrony danych w fazie projektowania (zasada “privacy by design” w praktyce).
3. Wdrażanie domyślnej ochrony danych (zasada “privacy by default” w praktyce”).
4. Polityka Ochrony Danych – w jakim zakresie jest obowiązkowa? Praktyczne rady, w jaki sposób konstruować wewnętrzną dokumentację oraz system przetwarzania danych osobowych w organizacji.
5. Formułowanie wewnętrznych procedur w zakresie przetwarzania i bezpieczeństwa danych osobowych – warsztat; analiza wzorcowych procedur, udostępnionych przez organizatora.
6. W jaki sposób skonstruować upoważnienia do przetwarzania danych osobowych?
7. Przydatne pod kątem rozliczalności ewidencje i rejestry.

VIII. **Wizerunek a RODO.**

1. Definicja “wizerunku”. W jakim zakresie wizerunek to dane osobowe?
2. Rozpowszechnianie wizerunku w perspektywie art. 81 ustawy o prawie autorskim i prawach pokrewnych – case study w oparciu o orzecznictwo.
3. Czy zgodę na rozpowszechnianie wizerunku można cofnąć w dowolnym momencie?
4. Jak powinna wyglądać zgoda na utrwalenie i upowszechnianie wizerunku – case study, w oparciu o orzecznictwo.
5. Uzasadniony interes administratora jako podstawa prawna przetwarzania wizerunku pracownika.
6. Odpowiedzialność za niezgodne z prawem przetwarzanie wizerunku na gruncie RODO, prawa autorskiego oraz kodeksu cywilnego.

IX. **Podsumowanie.**

X. **Pytania uczestników, dyskusja.**

Dzień 3:

I. **Audyt zgodności.**

1. Istota przeprowadzenia audytu i jego rodzaje.
2. Plan audytu i jego zakres.
3. Zasady prowadzenie audytu..
4. Ocena wyników zebranych podczas audytu.

II. **Obowiązki Administratora i Podmiotu przetwarzającego, współadministrowanie danymi osobowymi.**

1. Administrator danych, procesor i osoba upoważniona do przetwarzania danych – role w procesie przetwarzania danych osobowych, a zmiany z RODO.
2. Obowiązki Administratora danych.
3. Obowiązki Podmiotu przetwarzającego (procesora).
4. Współadministrowanie danymi osobowych – nowa instytucja RODO.

III. **Polityka ochrony danych osobowych**

1. Dotychczasowa dokumentacja – Polityka bezpieczeństwa i Instrukcja Zarządzania Systemem Informatycznym w perspektywie aktualnych wymogów RODO.
2. Obowiązki dokumentacyjne w RODO – Polityka Ochrony Danych.

Wszystkie prawa zastrzeżone. Materiały szkoleniowe oraz program prezentowany w naszej ofercie są chronione prawem autorskim. Jakiekolwiek nieautoryzowane kopiowanie, reprodukcja, dystrybucja lub wykorzystanie tych materiałów bez wyraźnej zgody jest ściśle zabronione.

3. Budowanie procedur wewnętrznego systemu zapewniającego bezpieczeństwo danych osobowych w kontekście nowych wymogów RODO.
    - Wskazówki dot. przygotowania i wdrożenia wewnętrznych polityk.
    - Omówienie przykładowych polityk.
        - Polityka stosowania urządzeń mobilnych zawierających dane osobowe.
        - Polityka czystego biurka i czystego ekranu.
        - Polityka zarządzania nośnikami wymiennymi zawierającymi dane osobowe.
        - Polityka kontroli dostępu do danych osobowych.
        - Polityka stosowania zabezpieczeń kryptograficznych.
        - Polityka przesyłania danych osobowych.

IV. **Rejestr czynności przetwarzania oraz rejestr kategorii czynności przetwarzania.**

1. Obowiązkowe elementy rejestrów przetwarzania.
2. Jak prowadzić rejestr czynności przetwarzania (rejestr administratora), wymagany przez RODO?
3. Praktyczny przykład rejestru czynności przetwarzania na danych wraz z omówieniem.
4. Kiedy i jak prowadzić rejestr kategorii czynności przetwarzania (rejestr procesora)?
5. Praktyczna forma rejestrów, różnice pomiędzy nimi.

V. **Analiza ryzyka na podstawie Rejestru Czynności Przetwarzania.**

1. Analiza ryzyka przy przetwarzaniu danych osobowych – przykłady praktyczne.
2. Analiza ryzyka – kiedy jest wymagana.
3. Zagadnienia związane z matrycą analizy ryzyka
4. Określanie wartości ryzyka – bezpieczny poziom
5. Część praktyczna na wybranym rejestrze

VI. **Obowiązek informacyjny (klauzule informacyjne dotyczące przetwarzania).**

- Obowiązek informacyjny przy przetwarzaniu danych osób art. 13 oraz art. 14
- Chwila powstania obowiązków informacyjnych.
- Obowiązek informacyjny przy przetwarzaniu danych osobowych – ustawy krajowe oraz RODO.
- Wymogi formalne z praktycznym omówieniem.
- Obowiązek informacyjny przy uzyskaniu zgody na przetwarzanie danych osobowych.
- Obowiązek informacyjny przy wyznaczeniu IOD.
- Obowiązek informacyjny przy przekazaniu danych osobowych poza EOG.
- Praktyczny przykład klauzuli informacyjnej z omówieniem.
    - Klauzula informacyjna
    - Klauzula monitoringu
    - Klauzula do pracownika /umowa o pracę/umowa zlecenia/ stażyści / praktykanci
    - Klauzula rekrutacyjna
- Obowiązek informacyjny w przypadku zbierania danych nie od osoby, której te dane dotyczą.

VII. **Umowa powierzenia przetwarzania danych osobowych**

Wszystkie prawa zastrzeżone. Materiały szkoleniowe oraz program prezentowany w naszej ofercie są chronione prawem autorskim. Jakiekolwiek nieautoryzowane kopiowanie, reprodukcja, dystrybucja lub wykorzystanie tych materiałów bez wyraźnej zgody jest ściśle zabronione.

1. Podstawy prawne i charakter prawny oraz konstrukcja umowy
2. Kiedy stosujemy powierzenie?
3. Przykładowe typy umowy powierzenia dla określonych działalności
4. Tworzenie umowy powierzenia

VIII. **Upoważnienia do przetwarzania danych osobowych**

1. Organizacyjne środki zabezpieczenia danych osobowych – ich wybór i dostosowanie zgodnie z RODO, w ujęciu praktycznym.
2. Techniczne środki bezpieczeństwa, ze szczególnym uwzględnieniem wymaganego przez RODO zapewnienia poufności, integralności, dostępności i odporności systemów i usług przetwarzania, pseudonimizacji oraz szyfrowania.
3. Analiza ryzyka przy przetwarzaniu danych osobowych – przykłady praktyczne.
4. Ocena skutków dla ochrony danych osobowych – kiedy jest wymagana.
5. Uprzednie konsultacje z organem nadzorczym.

IX. **Tworzenie i prowadzenie ewidencji oraz rejestrów**

1. Ewidencja osób upoważnionych do przetwarzania danych osobowych.
2. Wykaz zabezpieczeń
3. Rejestr umów powierzenia

X. **Dokumentowanie incydentów**

1. Identyfikacja naruszeń bezpieczeństwa danych osobowych.
2. Co robić w przypadku naruszenia?
3. Obowiązek zgłaszania incydentów z danymi, wynikający z RODO (zasada 72 godzin).
4. Obowiązek powiadamiania osób, których dane osobowe podlegają naruszeniu.
5. Rejestr naruszeń ochrony danych osobowych

XI. **Podsumowanie.**

XII. **Pytania uczestników, dyskusja.**

Trener

Przemysław Kilian

Doświadczony trener i szkoleniowiec z ponad 15-letnim stażem w branży edukacyjnej i doradczej. Studiował na Wydziału Prawa i Administracji Uniwersytetu Szczecińskiego, posiada rozległą wiedzę i praktyczne umiejętności w zakresie RODO oraz cyberbezpieczeństwa. Jego bogate doświadczenie zawodowe obejmuje prowadzenie setek szkoleń, na których przeszkolonych zostało tysiące osób, zarówno w sektorze publicznym, jak i prywatnym.
Przemysław Kilian jest Inspektorem Ochrony Danych Osobowych, gdzie odpowiada za wdrażanie i monitorowanie zgodności z przepisami o ochronie danych w różnych organizacjach. Jako Audytor Wewnętrzny oraz Audytor Wiodący Systemu Zarządzania Bezpieczeństwem Informacji, specjalizuje się w ocenie i doskonaleniu systemów zarządzania bezpieczeństwem informacji, zapewniając najwyższe standardy ochrony danych i informacji.
Jego szkolenia cechują się praktycznym podejściem, bogatym w rzeczywiste przykłady i studia przypadków, co sprawia, że uczestnicy zyskują nie tylko teoretyczną wiedzę, ale również praktyczne umiejętności. Przemysław Kilian cieszy się uznaniem wśród swoich kursantów za profesjonalizm, zaangażowanie i umiejętność przekazywania skomplikowanych zagadnień w przystępny sposób.

Ważne informacje zanim zaczniemy

Wszystkie prawa zastrzeżone. Materiały szkoleniowe oraz program prezentowany w naszej ofercie są chronione prawem autorskim. Jakiekolwiek nieautoryzowane kopiowanie, reprodukcja, dystrybucja lub wykorzystanie tych materiałów bez wyraźnej zgody jest ściśle zabronione.

PEŁNI WIEDZY

Kiedy otrzymam link do szkolenia?

Zaproszenie wysyłamy na 1 dzień roboczy przed terminem szkolenia. Nadawcą zaproszenia jest platforma Clickmeeting. Jeżeli nie możesz znaleźć wiadomości w skrzynce odbiorczej, sprawdź folder SPAM. Jeżeli nadal nie widzisz wiadomości, zadzwoń do nas.

Faktura. Kiedy mam zapłacić za szkolenie?

Na wskazany adres e-mail wyślemy fakturę do 2 dni roboczych po zakończeniu szkolenia. Skupiamy się na nauce, a potem na płatnościach :)

Szkolenie się odbyło, a ja nie mam materiałów, certyfikatu albo faktury.

Wszystkie dokumenty wysyłamy do dwóch dni roboczych po zakończonym szkoleniu. Wiadomości z załącznikami często trafiają do folderu SPAM, Oferty, Promocje itp. Jeżeli po sprawdzeniu tych folderów nadal nie widzisz dokumentów skontaktuj się z nami

Wszystkie prawa zastrzeżone. Materiały szkoleniowe oraz program prezentowany w naszej ofercie są chronione prawem autorskim. Jakiekolwiek nieautoryzowane kopiowanie, reprodukcja, dystrybucja lub wykorzystanie tych materiałów bez wyraźnej zgody jest ściśle zabronione.

+48 510 810 990
biuro@pelniwiedzy.pl
pelniwiedzy.pl

PW SOLUTIONS Sp z o. o. Ul. Chopina 41/2, 20-023 Lublin
NIP: 712-344-79-89

PEŁNI WIEDZY

Karta zgłoszeniowa

Prosimy wypełnić formularz drukowanymi literami lub na komputerze dla większej czytelności.

Nazwa

Kurs Inspektora Ochrony Danych Osobowych (IOD)

Data (dd.mm.yyyy)

25.01.2027

Kod rabatowy (jeśli dotyczy)

Forma (prosimy zaznaczyć jedną pozycję)

☐ Online ☐ Stacjonarne ☐ Hybrydowe

Uczestnicy szkolenia

Imię i Nazwisko | Telefon do uczestnika | E-mail do uczestnika

Imię i Nazwisko | Telefon do uczestnika | E-mail do uczestnika

Stanowisko (uczestnik 1) | Stanowisko (uczestnik 2)

Dane do faktury

Nabywca

Nazwa | NIP

Adres | Kod pocztowy | Miasto

Odbiorca

Nazwa | NIP

Adres | Kod pocztowy | Miasto

Wypełniony formularz prosimy przesłać na adres biuro@pelniwiedzy.pl

Zgody i pozostałe informacje

☐ **Akceptuje regulamin organizacji szkoleń i wyrażam zgodę na przetwarzanie moich danych osobowych w celu realizacji uczestnictwa w szkoleniu.**

☐ Chce otrzymywać informację o ofercie i promocjach. Wycofanie zgody możliwe jest w każdej chwili.

☐ Oświadczam, że uczestnictwo w szkoleniu jest finansowane w co najmniej 70 % ze środków publicznych w rozumieniu ustawy o finansach publicznych. Niniejsze oświadczenie ma na celu możliwość zastosowania stawki zwolnionej VAT zgodnie z art.43 ust.1 pkt 29c ustawy o podatku od towarów i usług.

Rezygnacji można dokonać do 5 dni roboczych przed datą szkolenia. Brak uczestnictwa należy zgłosić poprzez adres e-mail biuro@pelniwiedzy.pl wypełniając formularz odstąpienia.
Nieobecność nie oznacza rezygnacji ze szkolenia. W przypadku braku wysłania do nas wiadomości o rezygnacji zostaną Państwo obciążeni kosztem szkolenia zgodnie z wypełnionym z formularzem. Organizator szkolenia zastrzega sobie prawo do zmiany miejsca i terminu szkolenia. Ostateczna lokalizacja szkolenia zostanie podana w potwierdzeniu udziału..

INFORMACJA DOTYCZACA OCHRONY DANYCH OSOBOWYCH

- Administratorem Państwa danych jest PW SOLUTIONS Sp z o. o
- Podanie danych osobowych jest dobrowolne, lecz niezbędne do wykonania usługi szkoleniowej.
- Przekazane przez Państwa dane osobowe nie będą udostępnianie innym podmiotom.
- Zgoda na przetwarzanie danych może zostać wycofana w dowolnym momencie, nie ma to jednak wpływu na zgodność przetwarzania, dokonanego a jej podstawie przed wycofaniem zgody.
- W każdej chwili mają Państwo prawo dostępu do swoich danych, ich sprostowania, usunięcia bądź ograniczenia przetwarzania, prawo sprzeciwu, prawo do przenoszenia danych, jak również prawo do cofnięcia zgody w dowolnym momencie oraz prawo do wniesienia skargi do organu nadzorczego.
- Państwa dane osobowe będą przetwarzane do czasu zgłoszenia wycofania zgody.

Wypełniony formularz prosimy przesłać na adres biuro@pelniwiedzy.pl

....

Pieczątka instytucji oraz podpis osoby upoważnionej

Podpis uczestnika szkolenia