Możliwość dofinansowania

ODO 24 sp. z o.o.

4,5 / 5

3 oceny

Praktyczny kurs IOD

Numer usługi 2025/08/07/7492/2928711

zdalna w czasie rzeczywistym

Usługa szkoleniowa

32 h

20.10.2025 do 23.10.2025

3 198,00 PLN brutto

2 600,00 PLN netto

99,94 PLN brutto/h

81,25 PLN netto/h

Informacje podstawowe

Kategoria	Prawo i administracja / Prawo Unii Europejskiej
Grupa docelowa usługi	Praktyczny kurs IOD ma zapewnić Ci gruntowną wiedzę i dostarczyć praktyczne rozwiązania, dzięki którym będziesz móc skutecznie sprawować funkcję Inspektora Ochrony Danych. Plan zajęć zaprojektowaliśmy tak, aby każdego dnia skupiać Twoją uwagę wokół innego zagadnienia. Szkolenie skierowane jest do: • osób pełniących lub planujących objęcie funkcji Inspektora Ochrony Danych (IOD), • pracowników działów prawnych, HR, IT oraz compliance, • administratorów danych (ADO) i osób odpowiedzialnych za zgodność z RODO, • właścicieli firm i menedżerów chcących zrozumieć obowiązki w zakresie ochrony danych, • wszystkich, którzy chcą zdobyć praktyczne kompetencje w zakresie RODO i ochrony danych osobowych.
Minimalna liczba uczestników	6
Maksymalna liczba uczestników	12
Data zakończenia rekrutacji	17-10-2025
Forma prowadzenia usługi	zdalna w czasie rzeczywistym
Liczba godzin usługi	32
Podstawa uzyskania wpisu do BUR	Certyfikat systemu zarządzania jakością wg. ISO 9001:2015 (PN-EN ISO 9001:2015) - w zakresie usług szkoleniowych

Cel

Cel edukacyjny

Kurs ma na celu przygotowanie uczestników do efektywnego pełnienia funkcji inspektora ochrony danych. Uczestnicy zdobędą kompetencje niezbędne do wspierania organizacji w zapewnieniu zgodności z przepisami o ochronie danych osobowych, w tym w zakresie prowadzenia audytów, szacowania ryzyka, opracowywania dokumentacji oraz obsługi naruszeń i zapytań osób, których dane dotyczą. Dodatkowo kurs obejmuje zagadnienia związane z oceną zgodności przetwarzania danych osobowych przez systemy AI

Efekty uczenia się oraz kryteria weryfikacji ich osiągnięcia i Metody walidacji

Efekty uczenia się	Kryteria weryfikacji	Metoda walidacji
Uczestnik zna podstawowe pojęcia RODO, zasady przetwarzania danych, role ADO/IOD/procesora, prawa osób, których dane dotyczą oraz obowiązki administratora. Uczestnik potrafi zorganizować system ochrony danych osobowych w organizacji, zna zadania IOD, rozumie przepływy danych, potrafi zaplanować audyt RODO. Uczestnik potrafi przeprowadzić ocenę skutków dla ochrony danych (DPIA) i szacować ryzyko zgodnie z wymaganiami RODO. Uczestnik zna główne zagrożenia w systemach informatycznych, zna zasady bezpieczeństwa zgodnego z RODO i potrafi wdrażać środki ochrony danych. Uczestnik potrafi zorganizować system ochrony danych osobowych w organizacji, zna zadania IOD, rozumie przepływy danych, potrafi zaplanować audyt RODO. Uczestnik potrafi przeprowadzić ocenę skutków dla ochrony danych (DPIA) i szacować ryzyko zgodnie z wymaganiami RODO. Uczestnik zna główne zagrożenia w systemach informatycznych, zna zasady bezpieczeństwa zgodnego z RODO i potrafi wdrażać środki ochrony danych.	Poprawnie definiuje pojęcia (np. administrator, dane szczególne). Klasyfikuje podstawy prawne przetwarzania. Wskazuje sytuacje wymagające powołania IOD. Zna zasady raportowania naruszeń. Identyfikuje rolę i zadania IOD. Opracowuje plan audytu (zespół, dokumenty, arkusze). Ocena zgodności z zasadami RODO (np. przejrzystość, minimalizacja). Rozpoznaje sytuacje wymagające DPIA. Ocenia kontekst przetwarzania danych. Identyfikuje ryzyka i podatności. Określa próg akceptowalności ryzyka i proponuje działania. Rozpoznaje cyberzagrożenia (np. DDoS, spoofing). Dobiera zabezpieczenia techniczne i organizacyjne. Tworzy dokumentację techniczną (np. polityki haseł). Bezpiecznie korzysta z usług chmurowych.	Test teoretyczny

Cel biznesowy

Celem usługi jest przygotowanie uczestników do wsparcia administratora danych (ADO) we wdrożeniu, utrzymaniu i nadzorowaniu systemu ochrony danych osobowych zgodnego z RODO w organizacji – w ciągu 3 miesięcy od zakończenia kursu.

Uczestnicy rozwiną praktyczne kompetencje w zakresie:
• realizacji zadań wspierających zgodność z RODO,
• doradztwa w zakresie przetwarzania danych osobowych,
• prowadzenia audytów i analiz ryzyka,
• przygotowywania dokumentacji,
• reagowania na naruszenia,
• a także oceny zgodności systemów wykorzystujących sztuczną inteligencję z przepisami AI Act.

Cel realizowany będzie poprzez czterodniowe szkolenie zakończone testem wiedzy,
z uwzględnieniem zastosowania zdobytej wiedzy w środowisku pracy.

Efekt usługi

Efekt usługi (rezultat szkolenia)

Po ukończeniu kursu uczestnik:

- Otrzymuje komplet wzorów dokumentów niezbędnych do wdrożenia i utrzymania systemu ochrony danych zgodnego z RODO.
- Potrafi zaplanować i przeprowadzić podstawowy audyt RODO z wykorzystaniem dostarczonych materiałów.
- Posiada praktyczne umiejętności identyfikacji zagrożeń, analizy podatności oraz oceny ryzyka związanego z przetwarzaniem danych osobowych.
- Umie opracować rekomendacje działań minimalizujących ryzyko.
- Potrafi przygotować raport z oceny zgodności i analizy ryzyka na podstawie dostarczonych narzędzi i danych.
- Zna zasady wdrażania polityk i procedur ochrony danych i potrafi je dostosować do organizacji.
- Zna procedury postępowania w przypadku naruszenia danych oraz potrafi przygotować odpowiednią dokumentację i zgłoszenia do organów nadzorczych.
- Wspiera administratora danych w prowadzeniu dokumentacji związanej z ochroną danych osobowych, korzystając z dostarczonych wzorów i narzędzi.
- Wspiera administratora danych w zarządzaniu procesem identyfikacji i oceny ryzyka oraz we wdrażaniu działań minimalizujących ryzyko.
- Jest przygotowany do wspierania administratora danych we wdrażaniu środków technicznych i organizacyjnych zgodnych z RODO.

Metoda potwierdzenia osiągnięcia efektu usługi

Efekty zostaną potwierdzone poprzez samodzielnie opracowane przez uczestników elementy dokumentacji RODO, tworzone na podstawie przekazanych szablonów – w ramach zadań indywidualnych i zespołowych. Dokumentacja ta stanowi dowód nabycia kompetencji i gotowości do ich praktycznego zastosowania w organizacji. Dodatkową metodą weryfikacji będzie test końcowy (post-test) sprawdzający wiedzę teoretyczną uczestników.

Kwalifikacje

Kompetencje

Usługa prowadzi do nabycia kompetencji.

Warunki uznania kompetencji

Pytanie 1. Czy dokument potwierdzający uzyskanie kompetencji zawiera opis efektów uczenia się?

TAK

Pytanie 2. Czy dokument potwierdza, że walidacja została przeprowadzona w oparciu o zdefiniowane w efektach uczenia się kryteria ich weryfikacji?

TAK

Pytanie 3. Czy dokument potwierdza zastosowanie rozwiązań zapewniających rozdzielenie procesów kształcenia i szkolenia od walidacji?

TAK

Program

RODO od podstaw

Cel: Tego dnia nauczą się Państwo „widzieć” dane osobowe w swojej organizacji, poznają zasady ich przetwarzania, dowiedzą się w jaki sposób organizować ich skuteczną ochronę oraz jakie procedury należy wdrożyć, aby móc wykazać przestrzeganie RODO.

I. Zgodność z RODO - co to oznacza?

II. Wyjaśnienie najważniejszych pojęć m.in.

- dane osobowe
- przetwarzanie
- profilowanie
- pseudominizacja
- administrator
- podmiot przetwarzający
- odbiorca danych
- strona trzecia

III. Zasady przetwarzania danych osobowych i sposoby ich realizacj:

- zgodność z prawem i przejrzystość
- ograniczenie celu
- minimalizacja danych
- prawidłowość
- ograniczenie przechowywania
- integralność i poufność
- rozliczalność

IV. Status inspektora ochrony danych:

- obligatoryjne wyznaczenie inspektora ochrony danych (IOD)
- pozycja IOD
- zadania IOD
- konflikt interesów – jakich zadań nie powinien wykonywać IOD
- odpowiedzialność IOD

V. Prawa osób, których dane dotyczą i sposoby ich realizacji:

- prawo do uzyskania informacji (obowiązek informacyjny)
- prawo dostępu do danych
- prawo do sprostowania danych
- prawo do usunięcia danych („prawo do bycia zapomnianym”)
- prawo do ograniczenia przetwarzania
- prawo do przenoszenia danych
- prawo do sprzeciwu.

VI. Obowiązki administratora danych:

- uwzględnianie ochrony danych w fazie projektowania oraz domyślna ochrona danych
- status i obowiązki współadministratorów danych

- przetwarzanie danych z upoważnienia administratora lub podmiotu przetwarzającego
- rejestrowanie czynności przetwarzania
- bezpieczeństwo przetwarzania
- głaszanie naruszeń ochrony danych do organu nadzorczego, w tym omówienie formularza powiadomienie Prezesa UODO
- zawiadamianie osób, których dane dotyczą o naruszeniach
- ocena skutków dla ochrony danych (DPIA)

VI. Obowiązki podmiotu przetwarzającego:

VII. Przekazywanie danych do państw trzecich i organizacji międzynarodowych

IX. Prezes Urzędu Ochrony Danych Osobowych (Prezes UODO)

- status Prezesa UODO
- obowiązki Prezesa UODO
- ontrola i postępowanie w sprawie naruszenia ochrony danych
- uprawnienia naprawcze Prezesa UODO
- certyfikacja i akredytacja
- administracyjne kary pieniężne, w tym kryteria ustalenia wysokości kar

IOD w praktyce

Cel:W trakcie szkolenia skonfrontujesz wiedzę teoretyczną z praktycznymi aspektami tego, jak prowadzić rejestr czynności przetwarzania, przeprowadzać audyt, zarządzać naruszeniami oraz realizować prawa osób, których dane dotyczą.

I. Jak zarządzać systemem ochrony danych:

- kiedy system ochrony danych jest efektywny
- rzecznictwo na rzecz ochrony danych i wsparcie kierownictwa
- model i zakres zarządzania systemem ochrony danych
- skompletowanie zespołu ds. prywatności

II. Pozycja, praca i kwalifikacje inspektora ochrony danych (IOD):

- IOD w organizacji - niezależność, brak konfliktu interesów i zasoby
- kiedy wyznaczyć IOD i kogo wybrać na to stanowisko
- co obejmują, a czego nie obejmują zadania IOD
- kwalifikacje IOD – jak je rozwijać i uwzględnić interdyscyplinarność ochrony danych

III. Inwentaryzacja i zrozumienie organizacji:

- jak zrozumieć i zinwentaryzować przepływy danych
- jak prowadzić przydatny rejestr czynności przetwarzania
- ćwiczenie: jak dobrze zacząć pracę jako IOD

IV. Przygotowanie i przeprowadzenie audytu zgodności:

- audyt zgodności a inne analizy z zakresu ochrony danych osobowych
- przygotowanie działań audytowych i ustalenia organizacyjne
- przygotowanie dokumentów roboczych, w tym listy kontrolnej
- jak zachowywać się podczas audytu
- ćwiczenie: jak przeprowadzić rozmowę audytową
- jak ocenić zgodność, przygotować i przedstawić raport z audytu
- jak zaplanować i wpłynąć na realizację rekomendacji

V. Utrzymanie i zarządzaniem systemu „na co dzień”:

- jak zapewnić rozliczalność
- co uwzględnić w dokumentacji ochrony danych
- ćwiczenie: jak w praktyce realizować wymóg privacy by design

- świadomość pracowników – klucz do utrzymania zgodności z RODO
- obsługa żądań i realizacja praw osób fizycznych
- jak wybrać i zweryfikować podmiot przetwarzający
- jak zarządzać naruszeniami ochrony danych
- ćwiczenie: ocena wagi naruszenia

VI. Jak osiągnąć gotowość do kontroli organu nadzorczego:

- przygotowanie do kontroli jako najlepszy sposób na zgodność
- jak postępować po otrzymaniu zawiadomienia o kontroli
- jak przygotować dokumenty, lokalizację i pracowników
- formalne i merytoryczne przygotowanie pełnomocników
- ćwiczenie: przygotowanie do kontroli w przykładowym stanie faktycznym
- przebieg kontroli: wyjaśnienia, przesłuchanie pracowników i oględziny
- protokół kontroli, zgłaszanie zastrzeżeń i dalsze kroki

DPIA i analiza ryzyka

Cel: W formie ćwiczeń, przeprowadzimy inwentaryzację zasobów, które biorą udział w operacjach przetwarzania. Nauczysz się szacować dla nich ryzyko. Dzięki temu będziesz w stanie ustalić adekwatne, dla swojej organizacji, zabezpieczenia.

I. Wprowadzenie do zarządzania ryzykiem ochrony danych osobowych:

- podstawowe pojęcia
- organizacja procesu szacowania ryzyka
- omówienie wybranych metodyk szacowania ryzyka niezbędne elementy procesu DPIA

II. Badanie kontekstu przetwarzania danych osobowych:

- ustalanie kontekstu zewnętrznego
- ustalanie kontekstu wewnętrznego

III. Zabezpieczenia minimalizujące ryzyko według RODO/GDPR.

IV. Co to jest ocena skutków dla ochrony danych (DPIA):

- cel wykonania DPIA,
- sytuacje, w których przeprowadzenie DPIA jest obligatoryjne
- niezbędne elementy procesu DPIA
- inwentaryzacja procesów przetwarzania
- ustalenie zasobów związanych z przetwarzaniem wiążącym się z dużym prawdopodobieństwem spowodowania wysokiego ryzyka naruszenia praw lub wolności osób fizycznych

V. Wykonanie oceny skutków dla ochrony danych oraz szacowanie ryzyka dla zasobu przetwarzającego dane osobowe:

- cel szacowania ryzyka,
- korzyści z wykonania szacowania ryzyka
- kryteria oceny ryzyka
- szacowanie ryzyka
- poziom ryzyka

VI. Ćwiczenia z zakresu wykonania analizy ryzyka:

- szacowanie prawdopodobieństwa wystąpienia zagrożenia
- identyfikacja podatności
- identyfikacja istniejących zabezpieczeń
- identyfikacja efektywności istniejących zabezpieczeń
- szacowanie następstw
- identyfikacja ryzyka
- określanie poziomu ryzyka
- określanie progu akceptowalności ryzyka

VII. Ćwiczenia z identyfikacji zasobów i zabezpieczeń:

- ustalenie wartości ryzyka procesu dla zasobu
- oszacowanie prawdopodobieństwa wystąpienia zagrożenia
- identyfikacja podatności
- identyfikacja istniejących zabezpieczeń
- identyfikacja efektywności istniejących zabezpieczeń
- szacowanie następstw
- identyfikacja ryzyka
- określanie poziomu ryzyka
- określanie progu akceptowalności ryzyka

VII. Przygotowanie planu postępowania z ryzykiem:

- obniżanie ryzyka
- redukcja ryzyka
- uniknięcie ryzyka
- transfer ryzyka

IX. Konsultacje z organem nadzorczym:

- zakres informacji dla organu nadzorczego
- uprawniania organu nadzorczego

RODO w IT

Cel: Poznasz funkcjonalności bezpieczeństwa, które muszą realizować wykorzystywane przez Ciebie systemy informatyczne. Nauczysz się, w jaki sposób realizować prawa osób, których dane dotyczą. Przedstawimy Ci oraz omówimy rekomendowane przez Prezesa UODO procedury IT oraz ciągłości działania.

I. Systemy informatyczne – funkcjonalności bezpieczeństwa:

- identyfikacja systemów informatycznych
- zarządzanie dostępem użytkownikami
- kontrola dostępu do systemów i aplikacji
- dostęp do sieci i usług sieciowych,
- zarządzanie informacjami uwierzytelniającymi użytkowników
- zabezpieczenia kryptograficzne

II. Systemy informatyczne – prawa osób, których dane dotyczą:

- prawo do bycia zapomnianym – możliwe sposoby realizacji
- prawo do przeniesienia danych – możliwe sposoby realizacji
- prawo dostępu do danych osobowych – możliwe sposoby realizacji
- prawo do ograniczenia przetwarzania – możliwe sposoby realizacji
- domyślna ochrona danych i ochrona danych w fazie projektowania

III. Techniczne środki ochrony danych osobowych:

- kontrola dostępu
- infrastruktura serwerowa
- stacje robocze, urządzenia mobilne
- systemy wydruku
- pozyskiwanie, rozwój i utrzymanie systemów
- zarządzanie zasobami i usługami IT
- relacje z dostawcami

IV. Zarządzanie naruszeniami ochrony danych osobowych.

VI. Zarządzanie ciągłością działania:

- plan ciągłości działania
- procedury awaryjno-odtworzeniowe

VI. Dokumentacja przetwarzania danych osobowych:

- wymagane polityki ochrony danych
- przegląd polityk ochrony danych

Harmonogram

Liczba przedmiotów/zajęć: 4

Przedmiot / temat zajęć	Prowadzący	Data realizacji zajęć	Godzina rozpoczęcia	Godzina zakończenia	Liczba godzin
1 z 4 RODO od podstaw	Marta Bogusz	20-10-2025	09:00	17:00	08:00
2 z 4 IOD w praktyce	Radosław Radwan	21-10-2025	09:00	17:00	08:00
3 z 4 DPIA i analiza ryzyka	Tomasz Ochocki	22-10-2025	09:00	17:00	08:00
4 z 4 RODO w IT	Przemysław Stasiak	23-10-2025	09:00	17:00	08:00

Cennik

Cennik

Rodzaj ceny	Cena
Koszt przypadający na 1 uczestnika brutto	3 198,00 PLN
Koszt przypadający na 1 uczestnika netto	2 600,00 PLN
Koszt osobogodziny brutto	99,94 PLN
Koszt osobogodziny netto	81,25 PLN

Prowadzący

Liczba prowadzących: 7

1 z 7

Katarzyna Szczypińska

Absolwentka Uniwersytetu Mikołaja Kopernika w Toruniu na kierunkach prawo oraz ekonomia. Ukończyła aplikację radcowską przy Okręgowej Izbie Radców Prawnych w Warszawie, od 2017 r. wpisana na listę radców prawnych.

Perfekcjonistka, która chce dokładnie zrozumieć
procesy przetwarzania u klientów. Specjalizuje się w:
- ustalaniu ról podmiotów w procesie przetwarzania danych (art. 4 RODO),
-podstawach prawnych przetwarzania (art. 6 i 9 RODO),
- umowach powierzenia (art. 28 RODO),
-śledzeniu rozstrzygnięć w przedmiocie nałożenia kar pieniężnych (art. 83 RODO).

Przykłady zrealizowanych projektów:
1. Regulacja przetwarzania plików cookie dla międzynarodowej grupy kapitałowej.
2. Regulacja stosowania powiadomień push w księgarni internetowej.
3. Regulacja stosowania monitoringu wizyjnego w firmie produkcyjnej.
4. Negocjacje umowy powierzenia z firmą niszczącą dyski twarde i dokumenty papierowe.
5. Komunikacja z organami ścigania w kwestii udostępnienia danych klientów i pracowników.

2 z 7

Przemysław Stasiak

Absolwent Informatyki na Politechnice Łódzkiej. Dodatkowo ukończył studia podyplomowe o kierunku „Zarządzanie systemami Linux". Posiada certyfikaty dotyczące bezpieczeństwa sieci i aplikacji, ochrony danych osobowych i znajomości rozwiązań chmurowych. Ukończył kurs pedagogiczny.Audytor wiodący systemu zarządzania bezpieczeństwem informacji (ISO/IEC 27001).

Zawsze z głową w chmurach, przede wszystkim w AZURE, AWS, Google. Specjalizuje się w:
- procedurach bezpieczeństwa (art. 24 ust. 2 RODO),
- ochronie danych w fazie projektowania (art. 25 RODO),
- analizie ryzyka (art. 32 ust. 1 RODO)
- bezpieczeństwie usług chmurowych (art. 32 ust. 1 lit. b RODO).

Przykłady zrealizowanych projektów:
1. Rozwój aplikacji do analizy ryzyka – Doktor RODO.
2. Analiza ryzyka dla nowo powstałej aplikacji do płatności internetowych.
3. Zaplanowanie procesu integracji systemów informatycznych dwóch łączących się firm.
4. Weryfikacja środków bezpieczeństwa stosowanych przez procesorów.
5. Zapewnienie firmie programistycznej zgodności z RODO w trakcie kodowania.

3 z 7

Karolina Kukielska

Ukończyła studia prawnicze i odbyła aplikację radcowską, a po zdanym egzaminie na radcę prawnego została wpisana na listę radców prawnych Okręgowej Izby Radców Prawnych w Olsztynie. Swoją kancelarię prowadzi od 2019 roku. Doświadczenie zdobywała również w administracji publicznej, jako specjalista ds. organizacyjno-prawnych.

Lubi znajdować rozwiązanie najbardziej skomplikowanych problemów. Specjalizuje się w:
-retencji danych (art. 5 ust. 1 lit. e RODO),
- przetwarzaniu danych osobowych dotyczących wyroków skazujących (art. 10 RODO),

- obowiązku informacyjnym (art. 13 i 14 RODO),
- współadministrowaniu (art. 26 RODO).

Przykłady zrealizowanych projektów:
1. Przygotowanie regulaminów świadczenia usług drogą elektroniczną dla firmy programistycznej.
2. Przygotowanie procedury ochrony danych osobowych dla międzynarodowego CUW-u.
3. Regulacja czasu przetwarzania danych osobowych wolontariuszy dla organizacji pożytku publicznego.
4. Analiza wniosków klientów dotyczących usunięcia ich danych.
5. Przeprowadzenie testu równowagi dla przekazania danych osobowych pracowników nowemu pracodawcy.

4 z 7

Marta Bogusz

Adwokat z wieloletnim doświadczeniem procesowym, ukończyła prawo na Wydziale Prawa i Administracji Uniwersytetu Łódzkiego, a następnie aplikację adwokacką przy Izbie Adwokackiej w Warszawie.

W tematach prawnych działa twórczo. Specjalizuje się w:
- ustalaniu podstaw przetwarzania (art. 6 RODO),
- zadaniach IOD (art. 39 RODO),
-obsłudze zawiadomień, zgłoszeń i rejestracji naruszeń ochrony danych osobowych (art. 33-34 RODO),
- tworzeniu i opiniowaniu umów powierzenia przetwarzania danych osobowych (art. 28 RODO).

Przykłady zrealizowanych projektów:
1. Pomoc przy wdrożeniu nowej aplikacji (data protection by design) do zarządzania personelem.
2. Dostosowanie procesu kredytu konsumenckiego do wymagań RODO.
3. Przygotowanie regulaminu zakładowego funduszu świadczeń socjalnych w części dotyczącej ochrony danych osobowych.
4. Regulacja współpracy z agencją pracy tymczasowej.
5. Przygotowanie polityki prywatności i plików cookie dla firmy motoryzacyjnej.

5 z 7

Radosław Radwan

Absolwent prawa na Uniwersytecie Jagiellońskim, a także studiów podyplomowych z zakresu prawa własności intelektualnej na Uniwersytecie Warszawskim. W ramach studiów prawniczych ukończył Szkołę Prawa Amerykańskiego. Członek Izby Adwokackiej w Warszawie jako adwokat wykonujący zawód.

Specjalizuje się w:
- prostym i przyjaznym dla odbiorcy „języku” RODO (art. 12 RODO),
- ochronie danych osobowych w fazie projektowania (art. 25 RODO),
- obsłudze żądań i naruszeń (art. 15 -21 RODO, art. 33 i 34 RODO),
- utrzymywaniu wysokiej wiedzy o RODO wśród pracowników naszych klientów (art. 39 RODO).

Przykłady zrealizowanych projektów:
1. Ocena ryzyka związana z transferem danych osobowych do Rosji i USA.
2. Opiniowanie możliwości wykorzystania biometrii do identyfikacji klienta.
3. Uregulowanie dostępu firmy ochroniarskiej do monitoringu wizyjnego.
4. Dostosowanie do RODO procesu przetwarzania danych osobowych studia SPA & Wellness.
5. Dostosowanie do RODO procesu współadministrowania danymi osobowymi uczestników studiów podyplomowych.

6 z 7

Justyna Pergałowska

Od 2020 roku wpisana na listę radców prawnych przy Okręgowej Izbie Radców Prawnych w Warszawie. Ukończyła studia podyplomowe z zakresu ochrony danych osobowych i informacji niejawnych na Akademii Leona Koźmińskiego. Jest członkiem Sekcji Prawa Ochrony Danych Osobowych przy ORA Warszawa.Autorka publikacji o tematyce ochrony danych osobowych w magazynach branżowych.

Jestem zadaniowcem, dla którego nie ma problemów, są tylko wyzwania. Specjalizuje się w:

- opiniowaniu umów powierzenia (art. 28 RODO),
- obsłudze naruszeń i zawiadamianiu osób, których dane dotyczą, o naruszeniu ochrony danych osobowych (art. 33 i 34 RODO)
- projektowaniu klauzul informacyjnych (art. 13 i 14 RODO),
- przeprowadzaniu audytów w zakresie zgodności z przepisami o ochronie danych osobowych (art. 24 RODO).

Przykłady zrealizowanych projektów:
1. Realizacja KPI w zakresie ochrony danych osobowych w spółkach energetycznych.
2. Wdrożenie RODO w spółce z branży stomatologicznej.
3. Przygotowanie polityki prywatności i plików cookie dla największego w Polsce dystrybutora środków ochrony roślin.
4. Obsługa naruszeń w firmie księgowo-konsultingowej.
5. Przeprowadzenie audytów w stowarzyszeniu oraz spółkach i firmach z branży energetycznej, HR, medycznej i dystrybucyjnej

7 z 7

Tomasz Ochocki

Absolwent Akademii Obrony Narodowej na kierunku „Bezpieczeństwo narodowe” (specjalizacja zarządzanie kryzysowe). Ukończył studia podyplomowe z zakresu analizy bezpieczeństwa i zagrożeń terrorystycznych (Collegium Civitas) oraz ochrony danych osobowych i informacji niejawnych (Uniwersytet Kardynała Stefana Wyszyńskiego). Doktorant Szkoły Głównej Handlowej (Kolegium Ekonomiczno-Społeczne). Audytor wiodący systemu zarządzania bezpieczeństwem informacji (ISO/IEC 27001), systemu zarządzania ciągłością działania (ISO 22301) oraz audytor wewnętrzny systemu zarządzania informacjami o prywatności (ISO/IEC 27701). Współautor komentarza do ustawy o ochronie danych osobowych przetwarzanych w związku z zapobieganiem i zwalczaniem przestępczości.

Odpowiada za pracę i rozwój zespołu merytorycznego. Specjalizuje się w:

- ochronie danych w fazie projektowania (art. 25 RODO),
- analizie ryzyka (art. 32 RODO),
- ocenie skutków dla ochrony danych (art. 35 RODO),
- zarządzaniu naruszeniami (art. 33 i 34 RODO).

Przykłady zrealizowanych projektów:
1. Stworzenie narzędzia do analizy ryzyka i DPIA.
2. Stworzenie narzędzia do ochrony danych osobowych w fazie projektowania.
3. Współtwórca narzędzia do oceny ryzyka związanej z transferem danych do państw trzecich (TIA).
4. Rozwój dokumentacji ochrony danych i bezpieczeństwa informacji.
5. Współtwórca RODO i DODO Nawigatora.

Informacje dodatkowe

Informacje o materiałach dla uczestników usługi

KAŻDY UCZESTNIK OTRZYMUJE

• Certyfikat IOD - wydrukowany lub w wersji elektronicznej.

• Poszkoleniowe wsparcie - Pomoc ODO 24.

• Skrypt prezentacji - wydrukowany lub w wersji elektronicznej.

• Poradniki RODO - wydrukowane lub w wersji elektronicznej.

• Dostęp do nagrań cyklicznie odbywających się webinarów.

• Wzory dokumentacji pozwalającej wykazać zgodność z RODO.

• 90 dniowy testowy dostęp do aplikacji Dr RODO.

Warunki techniczne

Aby zapewnić efektywny udział w kursie, uczestnik powinien dysponować:

1. **Sprzętem komputerowym:**

- komputerem stacjonarnym lub laptopem z systemem operacyjnym Windows, macOS lub Linux,
- działającą kamerą internetową oraz mikrofonem i głośnikami lub zestawem słuchawkowym (headset),

2. **Oprogramowaniem:**

- aktualną wersją przeglądarki internetowej (np. Google Chrome, Microsoft Edge, Firefox),
- zainstalowaną aplikacją **Microsoft Teams** lub dostępem do wersji przeglądarkowej (logowanie wymagane),
- zainstalowanym pakietem biurowym umożliwiającym pracę na plikach Excel i Word (np. Microsoft Office, LibreOffice lub Google Workspace),
- możliwością otwierania plików PDF.

3. **Łącznością internetową:**

- **stabilnym łączem internetowym** o minimalnej prędkości:
  - **pobieranie:** 10 Mbps,
  - **wysyłanie:** 2 Mbps,
- połączenie kablowe (Ethernet) jest rekomendowane, jednak stabilne Wi-Fi również będzie wystarczające.

Kontakt

Dominik Kantorowicz

E-mail d.kantorowicz@odo24.pl

Telefon (+48) 690 004 852