

KURS INSPEKTORÓW OCHRONY DANYCH

2-DNIOWE SZKOLENIE

Kompleksowe szkolenie, które krok po kroku przygotowuje zarówno teoretycznie jak i praktycznie do samodzielnego wdrożenia RODO w organizacji oraz pełnienia funkcji Inspektora Ochrony Danych. Uczestnicy kursu zdobywają wiedzę i niezbędne umiejętności praktyczne, które efektywnie budują kompetencje osób zajmujących się ochroną danych osobowych w organizacji. Kurs prowadzony jest wyłącznie przez doświadczonych praktyków – czynnych IOD, audytorów wiodących ISO 27 001, ekspertów w dziedzinie IT i bezpieczeństwa informacji. Dzięki ich doświadczeniu Uczestnicy szkolenia mają możliwość zdobyć wiedzę dotyczącą najbardziej adekwatnych rozwiązań w procesach przetwarzania danych osobowych w swojej organizacji. W części praktycznej kursu omawiane są m.in. przykładowe dokumenty, procedury postępowania, zasady bezpieczeństwa danych osobowych.



TEMAT SZKOLENIA:	KURS INSPEKTORÓW OCHRONY DANYCH
CEL SZKOLENIA:	Celem kursu jest zdobycie wiedzy i praktycznych umiejętności, które pozwolą w sposób efektywny i samodzielny zapewnić zgodność organizacji z wymogami prawnymi dotyczącymi ochrony danych osobowych.
ADRESACI:	Kurs skierowany jest do przyszłych i obecnych Inspektorów Ochrony Danych, osób odpowiedzialnych za wdrożenie RODO w organizacji, osób zajmujących się ochroną danych osobowych w organizacji, w których nie został powołany IOD, administratorów danych oraz przedstawicieli szczebla kierowniczego administratora, specjalistów odpowiedzialnych za bezpieczeństwo informacji w swojej organizacji, małych i średnich przedsiębiorców, którzy chcą poznać swoje obowiązki wynikające z aktualnych przepisów prawa, dla wszystkich zainteresowanych tematyką ochrony danych osobowych.
POZIOM SZKOLENIA:	Szkolenie kompleksowe, przeznaczone zarówno dla osób początkujących, jak i mających już doświadczenie, lecz chcących usystematyzować lub zaktualizować posiadaną wiedzę.
METODYKA:	Szkolenie ma charakter wykładu interaktywnego uzupełnianego poprzez prezentację multimedialną. W trakcie zajęć pojawiają się również - panel dyskusyjny, studium przypadków, krótkie ćwiczenia, quizy (pre i post) mierzące przyrost wiedzy.
TERMINY SZKOLEŃ:	Łódź – 28-29 I 2020, Katowice – 28-29 I 2020, Wrocław – 4-5 II 2020, Gdańsk – 6-7 II 2020, Kraków – 11-12 II 2020, Katowice – 18-19 II 2020, Łódź – 18-19 II 2020, Poznań – 20-21 II 2020, Warszawa – 25-26 II 2020, Wrocław – 3-4 III 2020, Gdańsk – 5-6 III 2020, Kraków – 10-11 III 2020, Łódź – 17-18 III 2020, Rzeszów – 17-18 III, 2020, Poznań – 19-20 III 2020, Warszawa – 24-25 III 2020, Katowice – 31 III-1 IV 2020, Wrocław – 6-7 IV 2020, Gdańsk – 7-8 IV 2020, Kraków – 14-15 IV 2020, Łódź – 21-22 IV 2020, Rzeszów – 21-22 IV 2020, Poznań – 23-24 IV 2020, Katowice – 27-28 IV 2020, Warszawa – 27-28 IV 2020, Wrocław – 5-6 V 2020, Gdańsk – 7-8 V 2020, Kraków – 12-13 V 2020, Łódź – 19-20 V 2020, Rzeszów – 19-20 V 2020, Poznań – 21-22 V 2020, Katowice – 26-27 V 2020, Warszawa – 26-27 V 2020, Wrocław – 2-3 VI 2020, Gdańsk – 4-5 VI 2020, Kraków – 15-16 VI 2020, Łódź – 16-17 VI 2020, Poznań – 18-19 VI 2020, Warszawa – 23-24 VI 2020, Katowice – 30 VI-1 VII 2020
KOSZT:	990 zł netto (1217,70 zł brutto) 990 zł zw. z VAT dla opłacających szkolenie w 70% lub całości ze środków publicznych Cena obejmuje: uczestnictwo w kursie, materiały szkoleniowe, piśmiennicze, przerwy kawowe, obiad, certyfikat.
ZAKŁADANE EFEKTY KURSU:	<ul style="list-style-type: none"> • Znajomość kluczowych pojęć dotyczących ochrony danych osobowych • Zapoznanie się z aktualnymi przepisami mającymi wpływ na procesy przetwarzania danych (m.in. RODO, prawo pracy, ustawa o prawach autorskich i prawach pokrewnych, prawo telekomunikacyjne itp.) • Umiejętność właściwej identyfikacji, kto jest kim w procesie przetwarzania danych (administrator, procesor, ASI itp.) • Zdobycie wiedzy i umiejętności, jak dostosować organizację do przepisów RODO • Zdobycie wiedzy, jakie obowiązki nakłada RODO na administratora danych oraz podmioty przetwarzające dane • Uzyskanie wiedzy, jak realizować zadania przypisane IOD • Umiejętność opracowania i wdrożenia wewn. polityk bezpieczeństwa oraz innych kluczowych dokumentów w procesie wdrażania RODO • Zapoznanie się z metodykami szacowania ryzyka • Umiejętność identyfikacji zagrożeń, podatności • Uzyskanie wiedzy, w jaki sposób zapewnić bezpieczeństwo danych osobowych • Zdobycie praktycznej umiejętności rozwiązywania typowych problemów dot. danych osobowych
ZAMÓWIENIE SZKOLENIA:	Podstawą uczestnictwa w kursie jest zapoznanie się z <i>Regulaminem Szkoleń</i> oraz przesłanie zgłoszenia na wybrane szkolenie poprzez formularz rejestracyjny on-line dostępny na stronie internetowej www.proxymo.pl . Formularz rejestracji na szkolenie można także pobrać w formacie DOC, wypełnić i wysłać na adres e-mail: szkolenia@proxymo.pl
REZYGNACJA ZE SZKOLENIA:	Rezygnację z uczestnictwa w kursie należy zgłosić Organizatorowi drogą mailową na adres: szkolenia@proxymo.pl . W przypadku rezygnacji z uczestnictwa w terminie do 5 dni roboczych przed datą rozpoczęcia szkolenia, a szkolenie zostało już opłacone, wpłacona kwota zostanie zwrócona w całości. Rezygnacja z uczestnictwa niezgłoszona na 5 dni roboczych przed rozpoczęciem szkolenia nie zwalnia od zapłaty. W takim wypadku Zamawiający zobowiązuje się do poniesienia opłaty w wysokości 100% ceny szkolenia.
POZOSTAŁE INFORMACJE:	<ul style="list-style-type: none"> • Każdy uczestnik otrzymuje Pakiet RODO MAX w wersji elektronicznej, na który składa się 120 szablonów, autorskich materiałów i wzorcowych dokumentów • Każdy uczestnik objęty jest indywidualnym bezpłatnym wsparciem po szkoleniu (wsparcie jest nielimitowane przez okres 30 dni po szkoleniu) • Uczestnicy szkolenia otrzymują imienne certyfikaty potwierdzające udział w szkoleniu • Każdy kolejny uczestnik zgłoszony na szkolenie z tego samego podmiotu otrzyma 5% rabatu, a dla Klientów decydujących się na udział w kolejnych szkoleniach udzielamy 10% rabatu



PROGRAM KURSU INSPEKTORÓW OCHRONY DANYCH

I DZIEŃ KURSU

9:00 - 10:30

BLOK I WSTĘPNE ZAGADNIENIA DOTYCZĄCE RODO

1. RODO - unijna reforma ochrony danych osobowych
2. Kluczowe zmiany wynikające z RODO
3. Gdzie RODO ma zastosowanie?
4. Kogo RODO nie dotyczy?
5. Pozostałe źródła prawa dot. ochrony danych: ustawa o ochronie danych osobowych, ustawa sektorowa
6. Kodeksy dobrych praktyk

BLOK II PODSTAWOWE POJĘCIA Z ZAKRESU OCHRONY DANYCH OSOBOWYCH

1. Co to jest dana osobowa?
2. Osoba zidentyfikowana i możliwa do zidentyfikowania
3. Kiedy informacje nie są danymi osobowymi?
4. Przykłady danych osobowych - **case study**
5. Kategorie danych - dane "zwykłe" oraz szczególne kategorie danych
6. Biometryczne dane osobowe oraz dane dotyczące stanu zdrowia - **case study**
7. Przetwarzanie danych - cykl życia danych osobowych
8. Na czym polega profilowanie. Karty lojalnościowe, remarketing, telematyka, automatyczny mailing - **case study**
9. Pseudonimizacja a anonimizacja - różnice i cel stosowania
10. Zbiór danych osobowych - automatyczne i ręczne przetwarzanie uporządkowanych zestawów danych
11. Kim jest administrator danych?
12. Odbiorca danych, czyli kto?
13. Inspektor Ochrony Danych i jego rola

10:30 - 10:45

PRZERWA KAWOWA

10:45 - 12:30

BLOK III ZASADY DOTYCZĄCE PRZETWARZANIA DANYCH OSOBOWYCH

1. Legalność, rzetelność i przejrzystość przetwarzania danych
2. Celowość przetwarzania danych
3. Minimalizm danych - adekwatność ze względu na cel przetwarzania. **Studium przypadku**
4. Zasada poprawności merytorycznej danych osobowych
5. Retencja danych osobowych - zasada ograniczenia przechowywania
6. Zasady zapewnienia integralności i poufności przetwarzanych danych
7. Zasada rozliczalności - jak wykazać zgodność z RODO?

BLOK IV PODSTAWY PRAWNE PRZETWARZANIA DANYCH OSOBOWYCH

1. Kiedy legalnie możemy przetwarzać dane "zwykłe" oraz szczególne kategorie danych?
2. Prawnie uzasadniony interes administratora w oparciu o test równowagi
3. Zasady wyrażania zgody na przetwarzanie danych
4. Praktyczne przykłady klauzul zgód z omówieniem
5. Jednoznaczna potwierdzająca czynność jako forma wyrażenia zgody
6. **Studium przypadku:** rekrutacja, zatrudnienie, monitoring, marketing, zawarcie umowy, wykorzystanie wizerunku

BLOK V UPRAWNIENIA OSÓB, KTÓRYCH DANE DOTYCZĄ

1. Omówienie procedury realizacji praw osób, których dane dotyczą - **studium przypadku**
2. Prawo dostępu do danych i uzyskiwania kopii danych
3. Prawo do sprostowania danych
4. Prawo do bycia zapomnianym
5. Prawo do ograniczenia przetwarzania
6. Prawo do przenoszenia danych
7. Prawo do sprzeciwu
8. Prawo do niepodlegania profilowaniu



12:30 - 13:00

PRZERWA OBIADOWA

13:00 – 16:00

**BLOK VI
OBOWIĄZEK INFORMACYJNY**

1. O czym i kiedy informować?
2. Źródła pochodzenia danych, a obowiązek informacyjny
3. Kiedy nie powstaje obowiązek informowania?
4. Praktyczne przykłady sposobu realizacji obowiązku informacyjnego - **studium przypadku**
5. Omówienie przykładowych wzorców klauzul informacyjnych

**BLOK VII
BEZPIECZEŃSTWO DANYCH OSOBOWYCH**

1. Stosowanie wewnętrznych regulacji dotyczących bezpieczeństwa danych osobowych
2. Wdrożenie technicznych i organizacyjnych środków ochrony danych
3. Zapewnienie poufności, integralności, dostępności i odporności systemów i usług
4. Zapewnienie ciągłości działania
5. Testowanie, mierzenie i ocena skuteczności ochrony danych
6. Wykorzystanie modelu PDCA (Plan, Do, Check, Act)
7. Analiza ryzyka względem zasobów przetwarzania danych
8. Ocena skutków dla ochrony danych (DPIA) - kiedy należy ją przeprowadzić?
9. Stosowanie mechanizmów ochrony danych: privacy by design/by default - **studium przypadku**

**BLOK VIII
UDOSTĘPNIENIE I POWIERZENIE PRZETWARZANIA DANYCH OSOBOWYCH**

1. Na czym polega udostępnianie danych osobowych?
2. Przesłanki legalnego udostępniania danych osobowych
3. Odpowiedzialność związana z udostępnianiem danych osobowych
4. Przykłady udostępnienia danych - **studium przypadku**
5. Na czym polega powierzenie przetwarzania danych osobowych?
6. Warunki powierzenia przetwarzania danych osobowych
7. Obowiązki podmiotu przetwarzającego w imieniu administratora
8. Odpowiedzialność podmiotu przetwarzającego
9. Omówienie kluczowych różnic między udostępnianiem a powierzeniem przetwarzania danych
10. Przykłady powierzenia przetwarzania danych - **studium przypadku**

**BLOK IX
REJESTROWANIE CZYNNOŚCI PRZETWARZANIA**

1. Kto i kiedy powinien prowadzić rejestr czynności przetwarzania danych (RCPD)?
2. Obowiązkowe elementy RCPD
3. Praktyczne przykłady zapisów w RCPD z omówieniem - **studium przypadku**
4. Wskazówki dotyczące prowadzenia RCPD
5. Kto i kiedy powinien prowadzić rejestr kategorii czynności przetwarzania
6. Obligatoryjne elementy rejestru
7. Różnice między rejestrem kategorii czynności przetwarzania a RCPD

**BLOK X
NARUSZENIA OCHRONY DANYCH OSOBOWYCH**

1. Identyfikacja incydentów - **studium przypadku**
2. Ocena skutków wystąpienia incydentu
3. Obowiązek zgłaszania naruszeń ochrony danych osobowych
4. Obligatoryjne elementy zgłoszenia naruszenia
5. Obowiązek powiadamiania osób, których dane podlegają naruszeniu
6. Obligatoryjne elementy powiadomienia
7. Kiedy nie ma obowiązku zgłaszania naruszeń
8. Dokumentowanie naruszeń ochrony danych osobowych



**BLOK XI
ODPOWIEDZIALNOŚĆ ZA NARUSZENIE PRZEPISÓW**

1. Administracyjne kary finansowe
2. Wysokość administracyjnych kar finansowych dla podmiotów publicznych
3. Odpowiedzialność odszkodowawcza
4. Odpowiedzialność karna

16:00

ZAKOŃCZENIE PIERWSZEGO DNIA KURSU**II DZIEŃ KURSU**

9:00 - 10:30

**BLOK XII
WSTĘPNE ZAGADNIENIA DOTYCZĄCE INSPEKTORA OCHRONY DANYCH**

1. Kim jest Inspektor Ochrony Danych (IOD)
2. IOD jako pracownik, zleceniobiorca lub pracownik podmiotu przetwarzającego
3. Kompetencje IOD: fachowa wiedza i doświadczenie zawodowe
4. Cechy osobowe Inspektora Ochrony Danych
5. Kto zobligowany jest do wyznaczenia IOD?
6. IOD wewnętrzny czy zewnętrzny - zalety i wady
7. IOD w grupie przedsiębiorstw

**BLOK XIII
STATUS INSPEKTORA OCHRONY DANYCH**

1. Pozycja IOD w ramach organizacji
2. Organizacyjna autonomiczność IOD - **studium przypadku**
3. Kto i dlaczego nie może być IOD - konflikt interesów
4. Udział IOD w zagadnieniach dot. ochrony danych osobowych - **studium przypadku**
5. Jakże zasoby powinny mieć zapewnione IOD?
6. Czy IOD powinien otrzymywać instrukcje dot. wykonywania jego zadań?
7. Odwoływanie i karanie IOD
8. IOD jako punkt kontaktowy
9. Tajemnica zawodowa IOD

10:30 - 10:45

PRZERWA KAWOWA

10:45 - 12:30

**BLOK XIV
WYZNACZENIE INSPEKTORA OCHRONY DANYCH**

1. Formalne wyznaczenie IOD
2. Dokumentacja związana z formalnym wyznaczeniem IOD
3. Zawiadomienie o wyznaczeniu IOD do organu nadzorczego
4. Zawiadomienie o wyznaczeniu IOD przez pełnomocnika
5. ePUAP czy biznes.gov.pl - jak wysłać zawiadomienie o nowym IOD
6. Wyznaczenie zastępcy inspektora ochrony danych
7. Odpowiedzialność IOD
8. Ubezpieczenie OC inspektora ochrony danych
9. Pozostałe formalności związane z wyznaczeniem IOD

**BLOK XV
FUNKCJE I ZADANIA INSPEKTORA OCHRONY DANYCH**

1. Informowanie i doradzanie w zakresie obowiązków wynikających z RODO
2. Monitorowanie przestrzegania RODO - jak przeprowadzić audit?
3. Uświadamianie i szkolenie personelu przetwarzającego dane osobowe
4. Udzielanie zaleceń w zakresie DPIA
5. Współpraca IOD z organem nadzorczym
6. Pełnienie funkcji punktu kontaktowego
7. Wsparcie w prowadzeniu rejestru czynności przetwarzania danych



	<p>BLOK XVI WPROWADZENIE DO BEZPIECZEŃSTWA DANYCH OSOBOWYCH</p> <ol style="list-style-type: none"> 1. Co to jest bezpieczeństwo? 2. Bezpieczeństwo informacji a bezpieczeństwo danych osobowych 3. Co to jest zagrożenie? 4. Różnica między zagrożeniem a podatnością 5. Rodzaje zagrożeń i sposoby przeciwdziałania - studium przypadku 6. Zarządzanie incydentami 7. Praktyczne wskazówki dotyczące bezpieczeństwa fizycznego i środowiskowego 8. Jak zapewnić bezpieczeństwo osobowe 9. Kluczowe aspekty bezpieczeństwa teleinformatycznego 10. Stosowanie norm i kodeksów dobrych praktyk
12:30 - 13:00	<p>PRZERWA OBIADOWA</p>
13:00 – 16:00	<p>BLOK XVII WENĘTRZNE POLITYKI BEZPIECZEŃSTWA DANYCH OSOBOWYCH</p> <ol style="list-style-type: none"> 1. O czym i kiedy informować? 2. Wskazówki dot. przygotowania i wdrożenia wewnętrznych polityk 3. Polityka stosowania urządzeń mobilnych - studium przypadku 4. Polityka czystego biurka i ekranu - studium przypadku 5. Polityka czystego kosza i drukarki - studium przypadku 6. Polityka zarządzania nośnikami wymiennymi - studium przypadku 7. Polityka kontroli dostępu do danych osobowych - studium przypadku 8. Polityka przesyłania danych osobowych - studium przypadku 9. Ciągłość działania w oparciu o model PDCA <p>BLOK XVIII UPOWAŻNIENIA DO PRZETWARZANIA DANYCH OSOBOWYCH</p> <ol style="list-style-type: none"> 1. Kto powinien być upoważniony do przetwarzania danych osobowych? 2. Formy upoważnień 3. Kto może wydawać upoważnienia w imieniu administratora? 4. Praktyczne wskazówki dotyczące wydawania upoważnień 5. Omówienie przykładowych wzorców upoważnień 6. Rejestrowanie upoważnień do przetwarzania danych osobowych 7. Oświadczenia dotyczące zachowania danych w poufności 8. Jak i gdzie przechowywać dokumentację związaną z upoważnieniami? <p>BLOK XIX WPROWADZENIE DO ANALIZY RYZYKA</p> <ol style="list-style-type: none"> 1. Co to jest ryzyko? 2. Kto powinien uczestniczyć w procesie analizy ryzyka 3. Kontekst organizacyjny - określenie czynników zewnętrznych i wewnętrznych 4. Identyfikacja i ocena aktywów 5. Identyfikacja i ocena potencjalnych zagrożeń 6. Identyfikacja i ocena stosowanych zabezpieczeń 7. Identyfikacja i ocena podatności na zagrożenia 8. Identyfikacja i ocena skutków wystąpienia zagrożeń 9. Omówienie przykładowych matryc ryzyka 10. Plan postępowania z ryzykiem 11. Co to jest ryzyko szczątkowe? 12. Analiza ryzyka - podsumowanie
16:00	<p>ZAKOŃCZENIE KURSU. WYDANIE CERTYFIKATÓW</p>



FORMULARZ ZGŁOSZENIA NA SZKOLENIE**MIEJSCE I DATA SZKOLENIA:**

--

DANE ZGŁASZAJĄCEGO:

Lp.	Imię i nazwisko	Telefon	E-mail
1.			

UCZESTNICZY SZKOLENIA:

Lp.	Imię i nazwisko	Telefon	E-mail
1.			
2.			
3.			

DANE PODMIOTU (DO FAKTURY):

PEŁNA NAZWA PODMIOTU:			
ADRES:			
KOD POCZTOWY:		MIEJSCOWOŚĆ:	
NUMER NIP:			

WARUNKI ZGŁOSZENIA:

- Formularz należy wypełnić, podpisać i wysłać na adres e-mail: **szkolenia@proxymo.pl**.
- Odbiór zgłoszenia na szkolenie zostanie potwierdzony drogą mailową, na adres wskazany w zgłoszeniu.
- Zgłoszenie uczestnictwa w szkoleniu należy przesyłać najpóźniej na 5 dni roboczych przed rozpoczęciem wybranych zajęć. Ilość miejsc jest ograniczona, decyduje data wpłynięcia zgłoszenia.
- Rezygnacja z uczestnictwa niezgłoszona na 5 dni roboczych przed rozpoczęciem szkolenia nie zwalnia od zapłaty. W takim wypadku Zamawiający zobowiązuje się do poniesienia opłaty w wysokości 100% ceny szkolenia.
- Zamawiający przesyłając zgłoszenie udziału w szkoleniu, akceptuje warunki określone w Regulaminie Szkoleń zamieszczonym na stronie www.proxymo.pl.

DATA I CZYTELNY PODPIS ZGŁASZAJĄCEGO:

	<p>Upraszamy informujemy, iż podane w formularzu dane osobowe będą przetwarzane przez firmę Proxymo Ochrona Danych Osobowych - Robert Zgarda (dalej: Proxymo) z siedzibą w Krakowie, ul. Szlak 77/222 w celach realizacji usługi szkoleniowej, kontaktowania się w sprawach dotyczących szkolenia, windykacji należności, dla celów archiwizacyjnych oraz zapewnienia rozliczalności na podstawie przepisów prawa. Dane osobowe będą przetwarzane przez okres niezbędny do zrealizowania usługi. W celu wykazania rozliczalności dane osobowe będą przechowywane przez okres, w którym Proxymo jest zobowiązana do ich przechowywania w postaci elektronicznej lub papierowej, dla udokumentowania spełnienia wymagań wynikających z przepisów prawa oraz w celu umożliwienia kontroli przez uprawnione podmioty.</p> <p>Posiada Pani/Pan prawo dostępu do treści swoich danych oraz prawo ich sprostowania, usunięcia, ograniczenia przetwarzania, prawo do przenoszenia danych, prawo wniesienia sprzeciwu, a także prawo wniesienia skargi do organu nadzorczego (PUODO) gdy uzna, iż przetwarzanie jej danych osobowych narusza przepisy RODO. Podanie danych jest dobrowolne, ale niezbędne do zrealizowania usługi szkoleniowej. W razie pytań dotyczących zasad prywatności i przetwarzania danych osobowych możesz skontaktować się z nami pod adresem e-mail: proxymo@proxymo.pl.</p>
PIECZĄTKA FIRMY:	

