

Akademia Inspektora Ochrony Danych dla Banków 2026 3 dniowy kurs zakończony egzaminem i certyfikatem

Terminy kursu online:

Część I 11 marca 2026 r. godz. 9.00-12.00

Część II 20 marca 2026 r. godz. 9.00-12.00

Część III 1 kwietnia 2026 r. godz. 12.30-15.30

Cel szkolenia

1. Przypomnieć i usystematyzować zakres przepisów w zakresie ochrony danych osobowych związanych z działalnością banku
 2. Rozpoznać problemy wynikające z wdrożenia przepisów dotyczących ochrony danych osobowych
 3. Umieć rozpoznać i ocenić obszary ryzyka zgodności oraz ryzyka przetwarzania danych osobowych i odpowiednio ująć to w nadzorze lub kontroli wewnętrznej IOD lub komórki Compliance
1. **KORZYŚCI Z UCZESTNICTWA W SEMINARIUM:**
 2. Uzyskanie wiedzy przydatnej na zajmowanym stanowisku
 3. Uzyskanie przykładowych regulacji, raportów, dokumentów dotyczących compliance

Adresaci

1. Inspektorzy Ochrony Danych
2. Członkowie Zarządu nadzorujący bezpieczeństwo informacji / ryzyko ICT
3. Pracownicy komórek ds. bezpieczeństwa (SBI, ABI)
4. Pracownicy komórek ds. ryzyka i analiz
5. Pracownicy komórek ds. zgodności (ryzyka braku zgodności)
6. Pracownicy komórek ds. kontroli wewnętrznej
8. **WYMAGANIA WSTĘPNE DLA UCZESTNIKÓW:**
9. Ogólna znajomość praktyki działania banku spółdzielczego

Program szkolenia



Na zakończenie szkolenia otrzymujecie Państwo:

1. Polityka bezpieczeństwa informacji i inne regulacje wewnętrzne stanowiące element „polityk ochrony danych”
Instrukcja / zasady ochrony danych osobowych, w tym:
 - 1) procedury oceny ryzyka ochrony danych,
 - 2) procedury DPIA,
2.
 - 3) polityka monitoringu
 - 4) polityka retencji danych
 - 5) polityka w zakresie AI
 - 6) procedury audytu i oceny ryzyka podmiotu przetwarzającego
3. Rejestr czynności przetwarzania - wypełniony przykład
4. Rejestr kategorii czynności przetwarzania - wypełniony przykład
5. Raporty z oceny ryzyka ochrony danych osobowych oraz DPIA - wypełnione przykłady
6. Metodyka dotycząca ryzyka naruszeń ochrony danych, w tym metodyka oceny ryzyka naruszenia oraz odpowiednie narzędzie Excel oraz rejestr naruszeń
8. Umowy powierzenia dla podmiotów realizujących umowy powierzenia - publiczna strona www, serwer poczty elektronicznej, serwis monitoringu wizyjnego, itp

PROGRAM:

Część.1 - Zasady ogólne ochrony danych osobowych i dokumentacja ochrony danych

1. Podstawowe przepisy prawne i normy dotyczące ochrony danych osobowych
2. Role banku w procesach przetwarzania: administrator, podmiot przetwarzający
3. Zasady przetwarzania danych osobowych oraz obowiązki Banku wg przepisów RODO
4. Prawne podstawy przetwarzania danych osobowych w banku
5. Czy zgoda na przetwarzanie zawsze jest podstawą wymaganą i dopuszczalną?
6. Zasada rozliczalności i obowiązki dowodowe banku
7. Struktura regulacji wewnętrznych w zakresie ochrony danych i informacji
8. Rejestry czynności przetwarzania i kategorii przetwarzania
9. Typowe wady w rejestrach prowadzonych zgodnie z RODO
10. Pozostała dokumentacja RODO i w zakresie zapewniania przestrzegania przepisów
11. Typowe wady dokumentacji RODO
12. Rola i zadania IOD w Banku
13. Obowiązek niezwłocznego włączenia IOD w sprawę ochrony danych osobowych
14. Typowe problemy i wady w zakresie zadań IOD

Część.2 - Nadzór IOD nad ryzykiem przetwarzania danych osobowych

1. Obowiązek zapewniania bezpieczeństwa danych przez Bank i mechanizmy zabezpieczające w RODO:
2. organizacyjne,
3. techniczne
4. Zasady rozwoju systemów i zapewnienie ochrony danych osobowych (wymogi RODO)
5. Metodyka analizy ryzyka przetwarzania danych osobowych i raporty z oceny ryzyka
6. Metodyka oceny skutków przetwarzania (DPIA) i raporty z DPIA
7. Polityka i zasady monitoringu wizyjnego i innych form monitoringu
8. **Regulacje wewnętrzne dotyczące stosowania mechanizmów sztucznej inteligencji**
9. Metodyka testu równowagi
10. Procedury nadawania upoważnień i rejestr upoważnień
11. Umowy powierzenia przetwarzania - obligatoryjne elementy umowy, typowe wady
12. Procedury powierzania czynności i wymagania wobec podmiotu przetwarzającego
13. Monitoring podmiotu przetwarzającego
14. Typowe problemy dotyczące zabezpieczeń technicznych i organizacyjnych spotykane w bankach

Część.3 - Zapewnienie realizacji praw osób, kontrola wewnętrzna

1. Regulacje i procedury w zakresie realizacji praw podmiotu danych
2. Typowe wady w procedurach dotyczących realizacji praw osoby, której dane dotyczą
3. Polityka retencji danych i inne regulacje w zakresie zapewnienia retencji danych
4. Typowe problemy zapewnienia prawidłowej retencji danych
5. Procedury w zakresie zgłaszania naruszeń ochrony danych i metodyka oceny naruszenia

6. Rejestr naruszeń ochrony danych osobowych
 7. Przykładowe naruszenia ochrony danych
 8. Kontrola wewnętrzna sprawowana przez Inspektora Ochrony Danych w zakresie ochrony danych osobowych
 - Plan kontroli
 - Metodyka kontroli
 - Raporty pokontrolne
 9. Najczęściej występujące nieprawidłowości w zakresie przestrzegania przepisów o ochronie danych osobowych
 10. Raport roczny Inspektora Ochrony Danych
-

Warunki uczestnictwa i regulamin



Warunki uczestnictwa

po otrzymaniu zgłoszenia prześlemy potwierdzenie przyjęcia zgłoszenia, a na około 2 dni przed terminem szkolenia zostaną wysłane wiadomości organizacyjne wraz z linkiem do szkolenia oraz materiałami szkoleniowymi. Płatności po szkoleniu, zwykle w tym samym dniu po szkoleniu prześlemy do Państwa faktury do zapłaty wraz z zaświadczeniem drogą mailową.

Regulamin

rezygnację przyjmujemy najpóźniej na 3 dni przed szkoleniem w formie pisemnej. Rezygnacja w późniejszym terminie wiąże się z koniecznością pokrycia kosztów w 100%. Nieobecność na szkoleniu nie zwalnia z dokonania opłaty. W przypadku braku możliwości wzięcia udziału w danym terminie jest możliwość przesłania nagrania ze szkolenia online.

Promocja

1290 + VAT
za każdą kolejną osobę z firmy

1390 + VAT | za osobę

NADCHODZĄCE TERMINY
