PROGRAM SZKOLENIA: SKUTECZNY INSPEKTOR OCHRONY DANYCH

9:00 - 10:30	**BLOK I** **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 II **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. Jakie zasoby powinien 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 III** **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 IV **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
	BLOK V **WPROWADZENIE DO BEZPIECZEŃSTWA DANYCH OSOBOWYCH** 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

	BLOK VI **WPROWADZENIE DO BEZPIECZEŃSTWA DANYCH OSOBOWYCH** 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	**PRZERWA OBIADOWA**
13:00 – 16:00	**BLOK XVII** **WEWNĘTRZNE POLITYKI BEZPIECZEŃSTWA DANYCH OSOBOWYCH** 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
	BLOK XVIII **UPOWAŻNIENIA DO PRZETWARZANIA DANYCH OSOBOWYCH** 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?
	BLOK XIX **WPROWADZENIE DO ANALIZY RYZYKA** 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	**ZAKOŃCZENIE SZKOLENIA. WYDANIE CERTYFIKATÓW**