PROGRAM SZKOLENIA:

9:00 - 09:15	**POWITANIE UCZESTNIKÓW SZKOLENIA.**
09:15 - 10:30	**BLOK I** **CO TO JEST RODO I CO OZNACZA DLA IT?** 1. Format RODO 2. Kluczowe pojęcia z zakresu ochrony danych osobowych 3. Zasady przetwarzania danych osobowych w systemach IT 4. Obowiązki Administratora Danych a rola obszaru IT 5. Wdrożenie RODO w organizacji 6. Wsparcie kierownictwa 7. Plan projektu dostosowania organizacji do wymogów RODO 8. Role we wdrożeniu RODO w organizacji: a. Menadżer bezpieczeństwa IT (CISO, CDO) b. Administrator bezpieczeństwa IT c. Właściciel (biznesowy) zasobu d. Audytor IT e. Inspektor Ochrony Danych f. Administrator IT g. Użytkownik
10:30 - 10:45	**PRZERWA KAWOWA**
10:45 – 12:30	**BLOK II** **PRZETWARZANIA DANYCH W SYSTEMACH INFORMATYCZNYCH - WYBRANE ZAGADNIENIA** 1. Zbieranie danych osobowych 2. Co powinna zawierać Polityka Prywatności? 3. Użytkowanie danych osobowych 4. Wewnętrzne udostępnianie danych współpracownikom 5. Udostępnianie danych na zewnątrz organizacji 6. Retencja danych osobowych 7. Kasowanie danych osobowych 8. Autoryzacja 2FA w systemach IT 9. Mechanizmy ochrony danych w systemach IT
	BLOK III **NARZĘDZIA WSPOMAGAJĄCE PRACĘ ASI** 1. Dokumentacja i role związane z jej utrzymywaniem 2. Zarządzanie tożsamością w systemach IT 3. Zdalny dostęp, BYOD, VPN ... 4. Dostęp do komputera 5. Szyfrowanie - co należy rozważyć? 6. Szyfrowanie: a. zabezpieczenie rekordu bazy danych b. pliki c. metody 7. Automatyczne systemy pozyskujące dane i audyty 8. Ochrona przed utratą danych (DLP) 9. Kopie zapasowe

Proxymo Ochrona Danych Osobowych
ul. Szlak 77/222
31-153 Kraków

tel.: +48 503 838 386
e-mail: szkolenia@proxymo.pl
www.proxymo.pl

12:30- 13:00	**PRZERWA OBIADOWA**
13:00 – 15:45	**BLOK IV** **METODYKA ZARZĄDZANIA RYZYKIEM W OCHRONIE DANYCH OSOBOWYCH** 1. Czym jest podejście oparte na ryzyku? 2. Jak stosować podejście oparte na ryzyku? 3. Proces zarządzania ryzykiem - założenia, opis, efekty 4. Ustanowienie kontekstu organizacyjnego 5. Mechanizmy kontrolne 6. Proces szacowania ryzyka 7. Postępowanie z ryzykiem, monitorowanie i przegląd 8. Ogólna ocena ryzyka a ocena skutków dla ochrony danych
	BLOK V **MONITOROWANIE I NADZÓR** 1. Audyt ochrony danych osobowych - praca na programie audytu 2. Zarządzanie danymi i ich zbieranie 3. Umowy z dostawcami w obszarze IT 4. Bezpieczeństwo danych osobowych 5. Zarządzanie incydentami bezpieczeństwa danych osobowych
15:45 – 16:00	**ZAKOŃCZENIE SZKOLENIA. WYDANIE CERTYFIKATÓW.**