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

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 – 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. 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 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

	BLOK XVI **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 KURSU. WYDANIE CERTYFIKATÓW**