



PROGRAM TRZYDNIOWEGO KURSU DLA IOD - JAK DOSTOSOWAĆ ORGANIZACJĘ DO WYMOGÓW OGÓLNEGO ROZPORZĄDZENIA O OCHRONIE DANYCH (RODO/GDPR)

TEMAT	SZCZEGÓLNE ZAGADNIENIA
Część 1 – Wprowadzenie do RODO	<ul style="list-style-type: none">✓ Krótkie wprowadzenie✓ Omówienie podstawa prawnych:<ul style="list-style-type: none">• RODO• Ustawa o ochronie danych osobowych• Pakiet reformujący UE• Przegląd przepisów wprowadzających o• Inne akty prawne mające znaczenie z punktu widzenia ochrony danych osobowych: ustawa o świadczeniu usług drogą elektroniczną, prawo telekomunikacyjne, ustawa o prawach autorskich i prawach pokrewnych✓ Podstawowe definicje:<ul style="list-style-type: none">• dane osobowe: zwykłe, szczególne kategorie danych osobowych, dane dotyczące wyroków skazujących oraz czynów zabronionych• przetwarzanie danych osobowych• administratora danych osobowych• zbiór danych, a czynność przetwarzania (proces)✓ Powierzenie, udostępnienie, a może współadministrowanie?<ul style="list-style-type: none">• studium przypadków, w których dochodzi do przekazania danych podmiotowi zewnętrznemu





- obowiązki spoczywające na stronach w związku z powierzeniem przetwarzania danych osobowych
- na jakich warunkach można dane udostępnić
- omówienie pojęć: odbiorca danych, podmiot przetwarzający
- współadministrowanie: kiedy do niego dochodzi i jakie obowiązki spoczywają na współadministratorach
- ✓ Inspektor ochrony danych osobowych:
 - kto może być IODem
 - +/- powołanie IODa wewnątrz organizacji i skorzystania z usług zewnętrznych
 - obowiązkowe wyznaczenie Inspektora ochrony danych – analiza
 - wymagania oraz status Inspektora
 - zadania Inspektora względem Administratora danych osobowych, Regulatora i osób, których dane dotyczą,
 - zespół IOD
 - IOD w grupie kapitałowej
- ✓ **Warsztaty:**
 - Analiza, które z przedstawionych informacji stanowią dane osobowe, a które nie i dlaczego (20 minut)
 - Wyodrębnianie zbiorów danych osobowych i czynności przetwarzania (procesów), w oparciu o przedstawiony stan faktyczny (30 minut)
 - Analiza zapisów umowy powierzenie przetwarzania danych osobowych (30 minut)





Część 2 – Legalność przetwarzania danych osobowych	<ul style="list-style-type: none">✓ Zasady przetwarzania danych osobowych:<ul style="list-style-type: none">• zgodność z prawem, rzetelność, przejrzystość• ograniczenie celu• minimalizacja o prawidłowość• ograniczenie przechowywania• integralność i poufność• rozliczalność✓ Przesłanki legalności przetwarzania danych osobowe:<ul style="list-style-type: none">• kiedy i po spełnieniu jakich warunków możemy przetwarzać dane osobowe: zwykłe, szczególne kategorie danych osobowych oraz dane dotyczące wyroków skazujących i czynów zabronionych• analiza przesłanki zgody - elementy ważnej zgody: dobrowolność, konkretność, świadomość, jednoznaczność✓ Przekazywanie danych osobowych do Państwa trzecich lub organizacji międzynarodowych✓ Warsztat:<ul style="list-style-type: none">• Określanie podstaw prawnych przetwarzania danych osobowych na podstawie konkretnych przykładów (20 minut)
Część 3 - Świadomość	<ul style="list-style-type: none">✓ Jaka jest istota świadomości?✓ Kto oraz w jakiej formie powinien przeprowadzać szkolenia:<ul style="list-style-type: none">• metody szkolenia✓ Świadomość roli IODa w organizacji✓ Audyt i wdrożenie przepisów RODO:<ul style="list-style-type: none">• jak przygotować plan audytu• jaki powinien być zakres audytu





	<ul style="list-style-type: none">• jakie dokumenty oraz procedury należy przeanalizować• jak usystematyzować i przeanalizować zebrane informacje• Organ Ochrony Danych Osobowych:<ul style="list-style-type: none">• status i zadania• kontrole organu - uwarunkowania prawne kontroli, rodzaje i techniki kontroli, jak w praktyce wygląda kontrola, przygotowanie organizacji i pracowników do kontroli• Warsztaty:<ul style="list-style-type: none">• Opracowywanie zakresu tematycznego szkolenia pracowników (20 minut)• Opracowanie planu audytu, zakresu tematów i dokumentów niezbędnych do jego przeprowadzenia w oparciu o przedstawiony stan faktyczny, omówienie uchybień przedstawionych w stanie faktycznym (40 minut)
Część 4 – Prawa osób, których dane dotyczą	<ul style="list-style-type: none">• Przejrzystość:<ul style="list-style-type: none">• czym jest i jak ją realizować?• elementy przejrzystości• Prawa osób, których dane dotyczą:<ul style="list-style-type: none">• prawo dostępu do danych• prawa do sprostowania danych• prawo do usunięcia danych ("prawo do bycia zapomnianym")• prawo do ograniczenia przetwarzania• prawo do przenoszenia danych• prawo do sprzeciwu





	<ul style="list-style-type: none">• prawo do niepodlegania decyzji opartej na zautomatyzowanym przetwarzaniu, w tym profilowaniu• wykonywanie prawa osób, których dane dotyczą✓ Obsługa żądań podmiotów danych – jak powinna wyglądać procedura oraz jak zapewnić zgodność z RODO✓ Obowiązek informacyjny – kiedy i o czym informować:<ul style="list-style-type: none">• obowiązek informacyjny pierwotny• obowiązek informacyjny wtórny• warstwowy obowiązek informacyjny✓ Podstawy i rodzaje odpowiedzialności✓ Czynniki brane pod uwagę przy decyzji o nałożeniu kary oraz jej wymiarze✓ Warsztaty:<ul style="list-style-type: none">• Analiza kiedy, które prawa przysługują w oparciu o przedstawione stany faktyczne (20 minut),• Przygotowywanie odpowiedzi na żądanie osoby, której dane dotyczą (30 minut)• Przygotowywanie klauzul realizujących obowiązek informacyjny w oparciu o przedstawiony stan faktyczny oraz przygotowywanie klauzuli zgody (49 minut)
Część 5 - Zabezpieczenia i obowiązki względem organu nadzorczego	<ul style="list-style-type: none">✓ Zabezpieczenia fizyczne – w tej części dowiesz się między innymi:<ul style="list-style-type: none">• jak zabezpieczyć budynek/pomieszczenia przed skutkami zagrożeń, takich jak pożar czy zalanie• sposobach na stworzenie systemu kontroli dostępu• jak zabezpieczyć najbardziej newralgiczne miejsca





- ✓ Zabezpieczenia techniczne – systemy informacyjne zgodne z RODO, w tym:
 - przykłady zabezpieczeń systemów informacyjnych i infrastruktury technicznej, jakie należy stosować
 - definicje i przykłady anonimizacji oraz pseudonimizacji danych
- ✓ Zabezpieczenia organizacyjne:
 - Polityka Ochrony Danych Osobowych
 - rekomendowane procedury np. procedura reagowania na naruszenia, procedura realizacji praw osób, których dane dotyczą
 - osoby odpowiedzialne za ochronę danych osobowych w organizacji
 - rejestrowanie czynności przetwarzania i kategorii czynności przetwarzania
- ✓ **Warsztaty:**
 - Polityka Ochrony Danych Osobowych – przygotowanie argumentów za wdrożeniem polityki i procedur związanych z ochroną danych osobowych? (20 minut)
 - przykładowy Rejestr Czynności Przetwarzania (1 godzina)
- ✓ Zgłaszanie danych kontaktowych Inspektora Ochrony Danych
- ✓ Analiza ryzyka
 - podejście oparte na ryzyku – punkt wyjścia do zapewnienia adekwatności stosowanych zabezpieczeń





	<ul style="list-style-type: none">• privacy by design i privacy by default – co należy uwzględnić przy projekcie przetwarzania danych osobowych?• Ogólna ocena ryzyka, a ocena skutków dla ochrony danych,• konsultowanie innowacyjnych procesów z organem nadzoru <p>✓ Warsztat:</p> <ul style="list-style-type: none">• Przeprowadzenie ogólnej ocena ryzyka dla pracy zdalnej (1 godzina) <p>✓ Zgłaszanie incydentów – zdobędziesz informacje dotyczące:</p> <ul style="list-style-type: none">• anatomii incydentów – jakie są główne źródła wycieków oraz przykłady najbardziej znanych incydentów• horyzontu czasowego zarządzania incydemem – terminów przewidziane w RODO• analizy incydemu i kiedy incydem należy zgłosić do Prezesa Urzędu Ochrony Danych Osobowych• w jaki sposób dokonać zgłoszenia incydemu• kiedy powiadamiać osoby, których dane dotyczą <p>✓ Warsztaty:</p> <ul style="list-style-type: none">• przygotowanie zgłoszenia incydemu do PUODO (30 minut)• przygotowanie komunikatu do osób, których dotyczy naruszenie (15 minut)
--	---

