PROGRAM TRZYDNIOWEGO KURSU DLA IOD - JAK DOSTOSOWAĆ ORGANIZACJĘ DO WYMOGÓW OGÓLNEGO ROZPORZĄDZENIA O OCHRONIE DANYCH (RODO/GDPR)	
TEMAT	SZCZEGÓŁOWE ZAGADNIENIA
Część 1 – Wprowadzenie do RODO	✓ Krótkie wprowadzenie ✓ Omówienie podstawa prawnych o RODO o Ustawa o ochronie danych osobowych o Pakiet reformujący UE o Przegląd przepisów wprowadzających o Inne akty prawne mające znaczenie z punktu widzenie ochrony danych osobowych: ustawa o świadczeniu usług drogą elektroniczną, prawo telekomunikacyjne, ustawa o prawach autorskich i prawach pokrewnych ✓ Podstawowe definicje o dane osobowe: zwykłe, szczególne kategorie danych osobowych, dane dotyczące wyroków skazujących oraz czynów zabronionych o przetwarzanie danych osobowych o administratora danych osobowych o zbiór danych, czynność przetwarzania, a baza danych ✓ Powierzenie, udostępnienie, a może współadministrowanie? o studium przypadków, w których dochodzi do przekazania danych podmiotowi zewnętrznemu o obowiązki spoczywające na stronach w związku z powierzeniem przetwarzania danych osobowych o na jakich warunkach można dane udostępnić o omówienie pojęć: odbiorca danych, podmiot przetwarzający

LEX ARTIST SP. Z O.O.
UL. SZANCOWA 74/1
01-458 WARSZAWA
TELEFON: (22) 253 28 18
E-MAIL: KANCELARIA@LEX-ARTIST.PL

REGON: 366550145
NIP: 527-279-63-98
BRE BANK S.A. 62 1140 2004 0000 3602 5030 0372

	○ 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 ○ 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 umowy powierzenie przetwarzania danych osobowych (30 minut)
Część 2 – Legalność przetwarzania danych osobowych	✓ Zasady przetwarzania danych osobowych: ○ zgodność z prawem, rzetelność, przejrzystość ○ ograniczenie celu ○ minimalizacja ○ prawidłowość ○ ograniczenie przechowywania ○ integralność i poufność ○ rozliczalność ✓ Przesłanki legalności przetwarzania danych osobowe: ○ kiedy i po spełnieniu jakich warunków możemy przetwarzać

	dane osobowe: zwykłe, szczególne kategorie danych osobowych oraz dane dotyczące wyroków skazujących i czynów zabronionych o analiza przesłanki zgody - elementy ważnej zgody: dobrowolność, konkretność, świadomość, jednoznaczność ✓ Przekazywanie danych osobowych do Państwa trzecich lub organizacji międzynarodowych ✓ **Warsztat:** o Określanie podstaw prawnych przetwarzania danych osobowych na podstawie konkretnych przykładów (30 minut)
Część 3 - Świadomość	✓ Jaka jest istota świadomości? ✓ Kto oraz w jakiej formie powinien przeprowadzać szkolenia: o metody szkolenia ✓ Świadomość roli IODa w organizacji: ✓ Audyt i wdrożenie przepisów RODO: o jak przygotować plan audytu o jaki powinien być zakres audytu o jakie dokumentu oraz procedury należy przeanalizować o jak rozplanować cykliczne audyty ✓ Organ Ochrony Danych Osobowych: o status i zadania o kontrole organu – uwarunkowania prawne kontroli, rodzaje i techniki kontroli, jak w praktyce wygląda kontrola, przygotowanie organizacji i pracowników do kontroli ✓ **Warsztaty:** o Opracowywanie zakresu tematycznego szkolenie pracowników (20 minut) o Opracowanie planu audytu, zakresu tematów i dokumentów niezbędnych do jego przeprowadzenie w oparciu o przedstawiony stan faktyczny (20 minut)

Część 4 – Prawa osób, których dane dotyczą	✓ Przejrzystość o czym jest i jak ją realizować? o elementy przejrzystości ✓ Prawa osób, których dane dotyczą: o prawo dostępu do danych o prawa do sprostowania danych o prawo do usunięcia danych ("prawo do bycia zapomnianym") o prawo do ograniczenia przetwarzania o prawo do przenoszenia danych o prawo do sprzeciwu o prawo do niepodlegania decyzji opartej na zautomatyzowanym przetwarzaniu, w tym profilowaniu o wykonywanie prawa osób, których dane dotyczą ✓ Obowiązek informacyjny – kiedy i o czym informować o obowiązek informacyjny pierwotny o obowiązek informacyjny wtórny o warstwowy obowiązek informacyjny ✓ Podstawy i rodzaje odpowiedzialności ✓ Czynniki brane pod uwagę przy decyzji o nałożeniu kary oraz jej wymiarze ✓ **Warsztaty:** o Przygotowywanie klauzul realizujących obowiązek informacyjny w oparciu o przedstawiony stan faktyczny oraz przygotowywanie klauzuli zgody (45 minut) o Analiza kiedy, które prawa przysługują w oparciu o przestawione stany faktyczne (30 minut) o Przygotowywanie odpowiedzi na żądanie osoby, której dane dotyczą (20 minut)
Część 5 - Zabezpieczenia i	✓ Zabezpieczenia fizyczne – w tej części dowiesz się między innymi: o czego RODO wymaga w zakresie bezpieczeństwa fizycznego

obowiązki względem Regulatora	○ jak zabezpieczyć budynek/pomieszczenia przed skutkami zagrożeń, takich jak pożar czy zalanie ○ sposobach na stworzenie systemu kontroli dostępu ○ jak zabezpieczyć najbardziej newralgiczne miejsca np. serwerownię ✓ Zabezpieczenia techniczne – systemy informacyjne zgodne z RODO, w tym: ○ analiza ryzyka – punkt wyjścia do zapewnienia adekwatności stosowanych zabezpieczeń ○ przykłady zabezpieczeń systemów informacyjnych i infrastruktury technicznej, jakie należy stosować ○ definicje, techniki i przykłady anonimizacji oraz pseudonimizacji danych ○ jak od strony technicznej wykonać prawo do przenoszenia oraz do usunięcia danych ○ rozwiązania chmurowe zgodne z RODO ○ privacy by design i privacy be default – co należy uwzględnić projektując system informacyjny? ○ współpraca z IT przy realizacji zasady rozliczalności ○ zapewnienie zdolności do szybkiego przywrócenia integralności i poufności danych ○ RODO, a szyfrowanie danych ○ wymogi RODO w stosunku do nowych technologii – Big Data i Internet rzeczy ✓ Zabezpieczenia organizacyjne: ○ Polityka Ochrony Danych Osobowych ○ rekomendowane procedury np. procedura realizacji praw osób, których dane dotyczą ○ osoby odpowiedzialne za ochronę danych osobowych w organizacji

	○ rejestrowanie czynności przetwarzania i kategorii czynności przetwarzania ○ ocena ryzyka, w tym ocena skutków dla ochrony danych, ○ konsultowanie innowacyjnych procesów z organem nadzoru ✓ **Warsztaty**: ○ plan Polityki Ochrony Danych Osobowych – jakie są niezbędne elementy, które należy w niej uwzględnić? (15 minut) ○ przykładowy Rejestr Czynności Przetwarzania (1 godzina) ○ modelowa DPIA – ocena skutków dla ochrony danych (warsztat realizowany wspólnie z prowadzącym, 45 minut ✓ Zgłaszanie danych kontaktowych Inspektora Ochrony Danych ✓ Zgłaszanie incydentów – zdobędziesz informacje dotyczące: ○ anatomii incydentów – jakie są główne źródła wycieków oraz przykłady najbardziej znanych incydentów ○ horyzontu czasowego zarządzania incydentem – terminów przewidziane w RODO ○ analizy incydentu i kiedy incydent należy zgłosić do Regulatora ○ w jaki sposób dokonać zgłoszenia incydentu do Prezesa Urzędu Ochrony Danych Osobowych ✓ **Warsztat** – przygotowanie zgłoszenia incydentu do Regulatora (30 minut)