„Szkolenie ABI , ADO - Administrator Bezpieczeństwa Informacji, Administrator Danych Osobowych – kurs oraz warsztaty wraz z umiejętnością przeprowadzania audytów bezpieczeństwa informacji".

Moduł I – 8 godz.

1. System i przepisy prawa ochrony danych osobowych. Podstawowe pojęcia: (2h)
źródła, prawa ochrony danych osobowych w Polsce i w Unii Europejskiej- aktualne i planowane
zakres zastosowania ustawy o ochronie danych osobowych,
pojęcie danych osobowych, w tym pojęcie danych osobowych „wrażliwych"
pozostałe podstawowe pojęcia prawa ochrony danych osobowych.
Przepisy prawa w zakresie ochrony danych osobowych.
- przegląd aktów prawnych regulujących przetwarzanie danych osobowych,
ustawa z dnia 29 sierpnia 1997r. o ochronie danych osobowych,
akty wykonawcze do Ustawy o ochronie danych osobowych,
2. Charakterystyka pracy ABI w Polsce oraz w środowisku międzynarodowym: (2h)
. administrator bezpieczeństwa informacji (ABI publiczny a prywatny),
administrator danych osobowych (ADO),
Środowisko pracy ABI-ch: podatności ludzkie, metody kradzieży danych, kategorie zagrożeń omawiane na podstawie wycieków danych w Polsce,
Współpraca z GIODO, w tym omówienie zakresu uprawnień i przebiegu kontroli,
predyspozycje osobowe,
najczęstsze problemy ABI-ch,
dokumentacja dotycząca pracy ABI-ego,
wytyczne i sposoby opracowywanie obowiązkowych sprawozdań dla ADO i GIODO (przepisy obowiązujące od 30 maja 2015 r.),
wytyczne i sposoby prowadzenia przez administratora bezpieczeństwa informacji rejestru zbiorów danych (przepisy obowiązujące od 26 maja 2015 r),
ABI jako prowadzący Jawny Rejestr zbiorów danych,
rejestracja Administratora Bezpieczeństwa Informacji w GIODO.
ABI wewnętrzny, a zewnętrzny,
3. Obowiązki związane z przetwarzaniem danych osobowych: (2h)
podstawy prawne przetwarzania danych osobowych,
obowiązki szczególnej staranności przy przetwarzaniu danych osobowych,
obowiązki informacyjne związane z przetwarzaniem danych osobowych,
rejestracja zbiorów danych osobowych w tym zwolnienia z obowiązku rejestracji
przymusowe wykonywanie decyzji GIODO
4. Powierzanie danych osobowych do przetwarzania. Udostępnianie danych osobowych. Odpowiedzialność związana z przetwarzaniem danych osobowych: (1 h)
powierzenie a udostępnienie danych osobowych - podobieństwa i różnice,
zawieranie umów powierzenia danych osobowych do przetwarzania,
. osoba upoważniona do przetwarzania danych osobowych
. procesor" danych osobowych
. odpowiedzialność za naruszenie zasad ochrony danych osobowych, w tym: Kodeks Pracy, przepisy karne ustawy o ochronie danych osobowych oraz Kodeks Karny i Kodeks Cywilny.
. praktyczne przykłady
5. Ostatnie i planowane zmiany w przepisach o ochronie danych osobowych. (1 h)
. projekt Rozporządzenia UE,
wysokie kary grzywny,
obowiązek powołania inspektora ochrony danych osobowych (IODO),
obowiązek informowania GIODO o incydencie,
poszerzony obowiązek informacyjny ADO,
prawo do bycia zapomnianym,

współadministrator danych osobowych,
pytania i indywidualne konsultacje.

Moduł II 7 godz.

Bezpieczeństwo danych osobowych, teoretyczne i praktyczne rozwiązania dot. ochrony danych osobowych przetwarzanych w organizacji.

1. Wprowadzenie - Podstawowe pojęcia i zagadnienia związane z problematyką ochrony danych osobowych. (15 min)
2. Bezpieczeństwo informacji - Omówienie zasad budowania i funkcjonowania bezpiecznych systemów przetwarzania informacji. (15 min)
3. Podstawowe akty prawne oraz przepisy branżowe dot. ochrony danych osobowych. (10 min)
4. Rozporządzenie Ministra Spraw Wewnętrznych i Administracji z dnia 29 kwietnia 2004r. w sprawie dokumentacji przetwarzania danych osobowych oraz warunków technicznych i służące do przetwarzania danych osobowych - omówienie przedmiotowego aktu wykonawczego organizacyjnych, jakim powinny odpowiadać urządzenia i systemy informatyczne wraz z interpretacją. (30 min)
5.Wymagania aplikacji przetwarzających dane osobowe w zakresie odnotowywania udostępniania danych osobowych i bezpieczeństwa przetwarzania danych osobowych. (15 min)
6. Zarządzanie zbiorami danych osobowych po zmianach wprowadzonych ustawą z dnia 7 listopada 2014r.o ułatwieniu wykonywania działalności gospodarczej oraz Rozporządzeniem Ministra Administracji i Cyfryzacji z dnia 11 maja 2015 r. w sprawie sposobu prowadzenia przez administratora bezpieczeństwa informacji rejestru zbiorów danych (Dz. U. 2015 r., poz. 719). (20 min)
7. Zasady organizacji przetwarzania danych osobowych po 1 stycznia 2015 r. w związku ze zmianami wprowadzonymi ustawą z dnia 7 listopada 2014 r. o ułatwieniu wykonywania działalności gospodarczej oraz Rozporządzeniem Ministra Administracji i Cyfryzacji z dnia 11 maja 2015 r. w sprawie trybu i sposobu realizacji zadań w celu zapewniania przestrzegania przepisów o ochronie danych osobowych przez administratora bezpieczeństwa informacji (Dz. U. 2015 r., poz. 745)- Obowiązki ADO, ABI i ASI oraz osób upoważnionych wynikające z przepisów dot. ochrony danych osobowych. (40 min)
8. Zarządzanie ryzykiem w zakresie przetwarzania danych osobowych. - podatności, zagrożenia i sposoby przeciwdziałania, analiza ryzyka . (15 min)
9. Przetwarzanie danych osobowych: (20 min)

wymogi bezpieczeństwa dotyczące pomieszczeń przetwarzania danych osobowych
wymogi bezpieczeństwa dotyczące stanowisk przetwarzania danych osobowych
zabezpieczenia kryptograficzne przetwarzanych danych osobowych – omówienie narzędzi służących do szyfrowania
bezpieczne przetwarzanie danych osobowych w systemach informacyjnych i informatycznych

10. Utrata danych zapobieganie poprzez backup i szyfrowanie danych, zabezpieczenia fizyczne danych osobowych i inne. (1,5 h)

przechowywanie i archiwizowanie danych osobowych
zabezpieczenia fizyczne danych osobowych,
ochrona fizyczna,
monitoring wizyjny,
technologia biometryczna,
zabezpieczenia organizacyjne danych osobowych,
polityka kluczy,
polityka czystego biurka i czystego ekranu,
polityka haseł, procedura korzystania z komputerów przenośnych,
zabezpieczenia informatyczne danych osobowych,
tworzenie kopii zapasowych,
szyfrowanie danych,

monitoring i zabezpieczenie sieci informatycznej,
obszar przetwarzania i lokalizacje zamiejscowe,
powierzenie przetwarzania danych osobowych,
udostępnianie danych osobowych na wniosek.
praktyczne przykłady,
11. Komunikacja zewnętrzna a bezpieczeństwo danych osobowych: (15 min)
zagrożenia płynące z sieci Internet - sposoby bezpiecznego korzystania z serwisów www
poczta elektroniczna - zasady bezpiecznej korespondencji.
12. Ochrona fizyczna danych osobowych (15 min)
polskie normy a ochrona danych osobowych
zabezpieczenia fizyczne - rodzaje i zastosowanie
13.Tworzenie dokumentacji Bezpieczeństwa Informacji: (1,5 h)
praktyczne rozwiązania w zakresie opracowania i wdrożenia Polityki Bezpieczeństwa Informacji, Polityka bezpieczeństwa – przygotowanie dokumentu głównego.
Polityka bezpieczeństwa – przygotowanie załączników (narzędzi ABI).
Etapy wdrożenia – wdrożenie procedur i szkolenia pracowników.
Organizacja i przeprowadzanie szkoleń a zaznajomienie z dokumentacją.
praktyczne rozwiązania w zakresie opracowania i wdrożenia Instrukcji Zarządzania Systemem Informatycznym
praktyczne rozwiązania w zakresie opracowania i wdrożenia Instrukcji Postępowania w sytuacji naruszenia Bezpieczeństwa Danych Osobowych
Procedury Bezpieczeństwa jako część Systemu Bezpieczeństwa Informacji - zasady poprawnego tworzenia procedur, wdrażania oraz oceny funkcjonowania. Mechanizmy kontrolne jako element ciągłej poprawy jakości bezpieczeństwa informacji.

Moduł III – 8 godz.
Warsztaty „Administrator Bezpieczeństwa Informacji – dokumentacja”
1. Wdrożenie Polityki Bezpieczeństwa oraz powołanie Administratora Bezpieczeństwa Informacji: (0,5 h)
osoby odpowiedzialne za opracowanie, wdrożenie i aktualizacje dokumentacji Polityki Bezpieczeństwa,
podstawa prawna,
czy wyznaczyć ABI-ego, jeżeli tak to kogo i dlaczego?.
2. Nadawanie, modyfikacja i odbieranie upoważnienia do przetwarzania danych osobowych: (0,5 h)
podstawa prawna,
niezbędne elementy upoważnienia,
zakres upoważnienia.
3. Zbiory Danych osobowych: (1 h)
identyfikacja zbiorów i ich elementów,
legalizacja elementów zbiorów,
identyfikacja zbiorów powierzonych lub otrzymanych w powierzeniu,
rejestracja zbiorów danych.
Wdrażanie zabezpieczeń fizycznych.
Obszar przetwarzania i kontrola dostępu.
Polityka czystego ekranu, czystego biurka i druku oraz haseł
4. Procedury rozpoczęcia i zakończenia pracy z systemem informatycznym: (1 h)
podstawa prawna
procedury dostosowane do konkretnych rozwiązań informatycznych.
5. Legalne źródła danych: (1,5 h)
Między innymi: zgoda na przetwarzanie danych,
Możliwości kontroli danych przez podmiot danych
Wdrażanie zabezpieczeń fizycznych.

Wdrażanie zabezpieczeń organizacyjnych.
Metody zabezpieczania infrastruktury informatycznej.
Własne systemy informatyczne a ich outsourcing.
Zabezpieczanie sprzętu użytkowników.
Skuteczne sposoby usuwania danych osobowych.
Nadzór ABI nad ASI w praktyce – przykłady.
6. Umowy powierzenia: (1 h)
zapisy niezbędne,
zapisy inne dostosowane do operacji powierzenia danych.
7. Sprawozdanie w rozumieniu art. 36. Art. 36a. 2 pkt 1 a Ustawy o ochronie danych osobowych: (1 h)
zakres,
czynności niezbędne do sporządzenia sprawozdania,
8. Metody zabezpieczania infrastruktury informatycznej.(1,5h)
Własne systemy informatyczne a ich outsourcing.
Zabezpieczanie sprzętu użytkowników.
Skuteczne sposoby usuwania danych osobowych.
Rejestracja zbioru danych osobowych lub ABI w GIODO.
Wypełnianie formularza zgłoszenia zbioru danych osobowych.
Zgłaszanie zbiorów za pośrednictwem serwisu e-GIODO.
Określenie stosowanych zabezpieczeń w zgłoszeniu zbioru do GIODO.
Przepisy prawa w zakresie ODO – przypomnienie podstawowych pojęć.
Podstawowe pojęcia z zakresu bezpieczeństwa informacji.
GIODO – struktura, zakres działań, kontrole.
Podmioty zewnętrzne – powierzanie danych osobowych.
Przykłady właściwych i niewłaściwych wdrożeń
ĆWICZENIA:
o dodawanie zapisów o powierzeniu przetwarzania danych osobowych do umów o świadczenie usług,
o tworzenie treści klauzul zgody na przetwarzanie danych osobowych, marketing i przetwarzanie wizerunku,
o tworzenie treści obowiązku informacyjnego stacjonarnego i na potrzeby mailingu.
ĆWICZENIA:
o przygotowanie protokołu z kontroli wewnętrznej,
o przygotowanie raportu z incydentu oraz umieszczanie incydentu w rejestrze,
. o przygotowywanie protokołu zniszczenia danych
Podsumowanie materiału, przykłady incydentów ochrony danych osobowych.
Indywidualne konsultacje. Wdrożenie i nadzór nad systemem ochrony danych osobowych
Krótka rozmowa nt. warunków, w jakich będzie wdrażany system ochrony danych osobowych.
Wdrażanie zabezpieczeń informatycznych.
Ryzyko wypływu danych z systemu informatycznego.
Ocena skuteczności wdrożenia.
Incydentalne kontrole systemu ochrony danych osobowych.
Działania w trakcie incydentu oraz stosowanie środków zapobiegawczych.
Rekomendacja ABI kierowana do ADO.
Rozporządzenia z 11 maja 2015 r
Wymogi dot. planu sprawdzeń okresowych.
Wymogi dot. programu sprawdzenia.
Wymogi dot. powiadomienia ADO o sprawdzeniu.
Wymogi dot. sprawozdania ze sprawdzenia na wezwanie GIODO.
Udostępnianie informacji o przetwarzanych zbiorach danych osobowych.
ĆWICZENIA:

o przygotowanie planu sprawdzenia,
o przygotowanie programu sprawdzenia,
o przygotowanie sprawozdania ze sprawdzenia.

Moduł IV – 7 godz.
Warsztaty: „Administratora Bezpieczeństwa Informacji – realizacja ustawowych zadań"
Sporządzenie planu sprawdzeń,audyt ochrony danych osobowych, (1,5 h)
Zawartość planu sprawdzeń,
Zasady definiowania sprawdzeń w ramach planu,
Zasady wyboru kolejności realizacji sprawdzeń,
Nadzór nad realizacją planu oraz komunikacja w ramach jego realizacji.

Realizacja i dokumentacja sprawdzeń planowych i doraźnych. (1,5 h)
Planowanie realizacji sprawdzenia,
Komunikacja w ramach realizacji sprawdzenia,
Czynności w ramach sprawdzenia,
Dokumentowanie czynności w trakcie sprawdzenia,

Sprawozdanie ze sprawdzenia. (1 h)
Zawartość sprawozdania ze sprawdzenia,
Zasady określania i formułowania wniosków ze sprawdzenia,
Dystrybucja sprawozdania ze sprawdzenia.
. Raport z incydentu – z punktu widzenia użytkownika oraz z punktu widzenia ABI: (1,5 h)
elementy raportu
procedura zgłaszania incydentu
możliwości wykorzystania raportów
zarządzanie ryzykiem
Identyfikacja funkcji w badanej organizacji (1,5 h)
. AD0 - prawidłowa identyfikacja
. ABI - prawidłowa forma powołania
- ASI - właściwy zakres obowiązków
. Osoba upoważniona - właściwa identyfikacja
. Obszary przetwarzania - identyfikacja obszaru przetwarzania
. Zabezpieczenie fizyczne danych osobowych - identyfikacja
. Zabezpieczenie organizacyjne - identyfikacja
. Zabezpieczenie informatyczne - identyfikacja
Ćwiczenia zakresu dokumentacji, identyfikacja ADO w badanej organizacji.

Moduł V – 8 godz.
Warsztaty indywidualne:
. Tworzenie polityki bezpieczeństwa przetwarzania danych osobowych - tworzenie dokumentu
. Powołanie ABI - przygotowanie dokumentu
. upoważnienie i oświadczenie- tworzenie dokumentu
. ewidencja osób upoważnionych - tworzenie dokumentu
. ewidencja obszarów przetwarzania -tworzenie dokumentu
. ewidencja zbiorów danych osobowych - tworzenie dokumentu
. opis struktury zbiorów - tworzenie dokumentu
. listy kontrolne - tworzenie szablonów
. sprawozdania ze sprawozdania- tworzenie szablonów
. planowe sprawozdania stanu ochrony danych osobowych
. tworzenie planu szkolenia osób upoważnionych
. tworzenie instrukcji zarządzenia systemem informatycznym

. polityka kluczy -tworzenie procedury
. umowa o powierzeniu - tworzenie dokumentu
. powołanie ASI - tworzenie dokumentu

Ćwiczenia

wypełnienie wniosku zgłoszenia danych do GIODO
. wypełnienie wniosku zgłoszenia ABI do GIODO
. tworzenie zgód w różnych celach
. tworzenie treści obowiązku informacyjnego ADO
. dodawanie zapisów o powierzeniu danych osobowych

Podsumowanie materiału oraz incydenty
. incydenty związane z korespondencją elektroniczną
. incydenty związane z korespondencją papierową
. incydenty związane z korespondencją z elektronicznymi nośnikami

Ćwiczenia
. ocena skuteczności wdrożenia
. incydentalne kontrole systemów ochrony danych osobowych
. incydenty oraz stosowanie środków zapobiegawczych
. rekomendacja ABI kierowane do ADO
. przykładowe właściwego i niewłaściwego wdrożenia .

Ogółem: 38 godz.