Kurs dla Administratora Bezpieczeństwa Informacji

Ramowy plan szkolenia (7h)

1. Wstęp – dlaczego należy chronić dane osobowe?
2. Podstawy prawne ochrony danych osobowych.
3. Wyjaśnienie najważniejszych pojęć:
    a. Dane osobowe – imię, nazwisko, numer PESEL, e-mail, adres IP;
    b. Przetwarzanie danych osobowych – kto, kiedy i w jaki sposób przetwarza dane osobowe (identyfikacja procesów przetwarzania danych);
    c. Zbiory danych osobowych.
4. Administrator Danych Osobowych – kto jest administratorem danych i jakie ma obowiązki.
5. Administrator Bezpieczeństwa Informacji:
    a. Kto może pełnić rolę ABI;
    b. Obowiązki ABI wynikające z ustawy po nowelizacji;
    c. Rejestracja ABI w rejestrze GIODO.
6. Przetwarzanie danych osobowych:
    a. Ogólne zasady – legalności, celowości, merytorycznej poprawności, adekwatności oraz ograniczenia czasowego;
    b. Przesłanki legalności – podstawy prawne, które umożliwiają przetwarzanie danych osobowych (zgoda na przetwarzanie danych osobowych, przepis prawa, prawnie usprawiedliwiony cel, realizacja umowy, dobro publiczne)
    c. Zgoda na przetwarzanie danych osobowych – prawidłowa klauzula zgody. Kiedy zgoda jest niezbędna? – warsztat – redakcja klauzuli zgody
    d. Rejestracja zbiorów danych – które zbiory należy zarejestrować, kiedy i w jaki sposób dokonać rejestracji – warsztat – wypełnianie wniosku rejestracyjnego.
7. Obowiązek informacyjny administratora danych.
8. Dokumentacja z zakresu ochrony danych osobowych – obowiązek wdrożenia i stosowania:
    a. Polityki Bezpieczeństwa;
    b. Instrukcji Zarządzania Systemem Informatycznym
    c. Rejestr zbiorów danych osobowych
    d. Upoważnienie do przetwarzania danych osobowych

Omówienie poszczególnych elementów, które powinny składać się na dokumentację. Porady i wskazówki dotyczące tworzenia dokumentacji.

9. Zasady przekazywania danych innym podmiotom:
    a. Powierzenie a udostępnienie – komu, kiedy i na jakich zasadach można przekazywać dane osobowe;
    b. Przekazywanie danych na podstawie przepisów prawa;
    c. Przekazanie danych w ramach grupy kapitałowej;
    d. Uprawnienie do kontroli procesorów.
10. Zabezpieczenia organizacyjne i techniczne – w jaki sposób zabezpieczyć poufność, integralność i rozliczalność danych?
    a. Szkolenie pracowników jako zabezpieczenie organizacyjne (obowiązek Administratora Danych)
    b. Wdrożenie wewnętrznych procedur – Polityka czystego biurka i Polityka kluczy;
    c. Zabezpieczenia fizyczne obszaru przetwarzania danych;
    d. Zabezpieczenia systemów informatycznych.
11. Podstawy i rodzaje odpowiedzialności prawnej – odpowiedzialność Administratora Danych oraz poszczególnych osób:
    a. Odpowiedzialność administracyjna – kontrola i decyzje GIODO;
    b. Odpowiedzialność dyscyplinarna pracowników;
    c. Odpowiedzialność cywilna – ochrona dóbr osobistych (nazwisko, pseudonim);
    d. Odpowiedzialność karna.
12. Odpowiedź na pytania i wątpliwości uczestników. Konsultacje.

Szkolenie trwa 7 godzin

9.00 Rozpoczęcie szkolenia
11.00 Przerwa kawowa
13.00 Lunch
16.00 Zakończenie szkolenia

Uczestnik otrzymuje:

„Certyfikat ABI” oraz materiały szkoleniowe, wzory klauzul, szablony dokumentacji oraz 2 godzinne konsultacje z ekspertem ds. ochrony danych osobowych.