1-DNIOWY KURS DLA INSPEKTORÓW / SPECJALISTÓW OCHRONY DANYCH LUB ADMINISTRATORÓW

SZANOWNI PAŃSTWO,

Proponowane przez nas szkolenie to wyjście naprzeciw oczekiwaniom uczestników naszych dotychczasowych szkoleń oraz licznych zapytań w tej materii. Wokół RODO narosło już tyle mitów, że czas raz na zawsze się z nimi rozprawić, a że nie da się tego zrobić gremialnie i na raz, przed nami długa droga pracy organicznej. Tylko systematycznie zdobywana wiedza, dzielenie się doświadczeniami i poglądami, podnoszenie kwalifikacji zawodowych pozwala na poczucie się pewniejszym w wykonywaniu codziennych obowiązków Inspektora Ochrony Danych. Niezależnie od branży, jakie reprezentujemy, da się sprowadzić wspólny mianownik zadań Inspektorów.

My go zdefiniowaliśmy i chcemy byście dali nam Państwo szansę jego przedstawienia. Chodzi o rzetelność i ugruntowanie wiedzy, a jest ona ze skrajnie różnych dziedzin. Wbrew pozorom te różne dziedziny: prawo, informatyka, matematyka, da się ze sobą połączyć w sposób syntetyczny, by przenikając się nawzajem pomagały nam w codziennej pracy Inspektora.
Nasza propozycja to jednodniowe skondensowane szkolenie teoretyczno-praktyczne, na którym poza niezbędną teorią koncentrujemy się na praktyce we wszystkim tym, czym na co dzień powinien zajmować się Inspektor Ochrony Danych czy Administrator. Nasze główne cele to nie przedstawianie Państwu schematów teoretycznych, ale praca na żywych przykładach (kazusach) i dokumentach, wypracowania umiejętności ich tworzenia i audytowania, przygotowywania sprawdzeń, sprawozdań i raportów, analizowaniu i szacowaniu ryzyka, rozpoznawaniu zagrożeń, definiowaniu ryzyk w wybranych obszarach.

Szczegóły kursu znajdują się w planie szkolenia, jednak najogólniej ujmując podzieliliśmy go na 3 główne moduły:
1) REASUMCPCJA WIEDZY Z OCHRONY DANYCH OSOBOWYCH – obalanie mitów;
2) WARSZTATY – PRAKTYCZNE ZASTOSOWANIE WIEDZY W PROCESIE OCHRONY DANYCH OSOBOWYCH – praca na dokumentach;
3) WARSZTATY – ANALIZA I SZACOWANIE RYZYKA.

Uczestnicy Kursu otrzymają **CERTYFIKAT** uczestnictwa wraz z autoryzowanym przez nas suplementem szczegółowo opisującym jego przebieg. Dodatkowo, każdy Uczestnik otrzyma komplet dokumentacji RODO stworzonej w oparciu o System Zarządzania Bezpieczeństwem Informacji opartym o wytyczne normy ISO 27001, ISO 27005 oraz ISO 27035. Jest to w sumie ponad 300 stron gotowej dokumentacji w tym m.in.:
- Polityka Ochrony Danych Osobowych
- Polityka Zarządzania Systemem Teleinformatycznym
- Polityka Ciągłości Działania
- Plan Awaryjny
- Instrukcja Postępowania w Sytuacji Naruszenia Danych Osobowych wraz z załącznikami
- Polityka Nadawania Uprawnień
- Polityka Rekrutacji
- upoważnienia dla pracowników
- oświadczenia pracowników
- rejestr osób przetwarzających dane
- wykaz pomieszczeń tworzących obszar, w którym przetwarzane są dane osobowe
- opis zbiorów danych
- plan sprawdzeń
- sprawozdanie ze sprawdzenia
- oświadczenia o przeszkoleniu
- procedura weryfikacji tożsamości
- procedura udzielania informacji
- procedura rozpoznawania
- procedura udostępnienia danych
- Wykaz identyfikatorów
- Procedura haseł Administrator/Inspektor Ochrony Danych
- Rejestr Czynności Przetwarzania oraz
- Rejestr Kategorii Czynności.

Ponadto, Kurs objęty jest przez nas **PROGRAMEM PARTNERSKIM**, co oznacza, że w trakcie Kursu jak i po jego zakończeniu będziecie Państwo mogli korzystać z naszego wsparcia prawnego i informatycznego.

PLAN SZKOLENIA

OCHRONA DANYCH OSOBOWYCH. WPROWADZENIE

MODUŁ I – TEORETYCZNO-PRAWNE ASPEKTY PRZETWARZANIA DANYCH OSOBOWYCH

1. Prawna forma reformy dotyczącej bezpieczeństwa i ochrony danych osobowych;
2. Implementacja bezpośrednia czy przepisy wykonawcze w krajowym systemie prawnym;
3. Ogólnoświatowe i ogólnoeuropejskie tendencje w podejściu do danych osobowych. Przyczyna, przebieg, oczekiwany skutek czyli wyjaśnienie, kto i dlaczego stworzył General Data Protection Regulations – RODO (pl) wskazanie różnic pomiędzy dyrektywą, a rozporządzeniem.
4. Analiza podstawowych pojęć:

- dane osobowe
- dane wrażliwe
- przetwarzanie
- administrator
- powierzenie danych
- udostępnienie danych a powierzenie
- podmiot przetwarzający / procesor
- pseudonimizacja
- aninimizacja
- usunięcie
- prywatność
- ochrona danych a anonimizacja społeczeństwa
- zbiory danych, ich identyfikacja,

ROLA ADMINISTRATORA

5. GDPR/RODO – szczegółowa analiza rozporządzenia
6. Co wprowadza RODO – analiza najważniejszych zmian dotyczących systemu ochrony danych osobowych, ich struktury i bezpieczeństwa;

7 Zasady przetwarzania danych osobowych:

- rzetelność i przejrzystość;
- legalność;
- merytoryczna poprawność danych;
- integralność;
- celowość;
- adekwatność;
- rozliczlność;
- poufność;
- adekwatność
- ograniczenia czasowe przetwarzania;

8. Obowiązki:

- administratorów danych osobowych;
- administrujących danymi osobowymi;
- inspektorów ochrony danych – wprowadzenie;
- administratorów systemów informatycznych – wprowadzenie;
- administratorów aplikacji – wprowadzenie;

9. Obowiązki administratorów danych i nowe zasady administrowania: nowe czy stare po nowemu?
10. Zasada ochrony danych na etapie projektowania „privacy by design”;
11. Domyślna ochrona danych „privacy by default”;
12. Współadministrowanie a wspólne operacje przetwarzania danych osobowych;
13. Przekazywanie danych do państwa trzeciego i organizacji międzynarodowych;
14. Międzynarodowy transfer danych osobowych a powierzanie danych osobowych;

15. Prawa jednostki, której dane są przetwarzane:
- prawo do informacji;
- prawo do dostępu do swoich danych;
- prawo do sprostowania;
- prawo do bycia zapomnianym – prawo do usunięcia danych – kiedy?
- prawo do przenoszenia danych;
- prawo do ograniczenia przetwarzania;
- prawo do sprzeciwu wobec przetwarzania – kiedy?

MODUŁ II – WARSZTATY – PRAKTYCZNE ZASTOSOWANIE WIEDZY W PROCESIE OCHRONY DANYCH OSOBOWYCH

1. Wprowadzenie do audytowania;
2. Podstawowe definicje:
- audytor;
- dowód z audytu;
- cele audytu;
- role i zakres odpowiedzialności;
- skuteczna komunikacja;
- kontekst organizacji;
- zasoby;
- kompetencje;
- monitorowanie;
3. Analiza dokumentacji ochrony danych osobowych – warsztaty praktyczne:
- Polityka Ochrony Danych Osobowych;
- Polityka Zarządzania Systemem Teleinformatycznym;
- Polityka Ciągłości Działania;
- Plan Awaryjny;
- Instrukcja Postępowania w Sytuacji Naruszenia Danych Osobowych wraz z załącznikami;
- Polityka Nadawania/Odbierania Uprawnień;
- Procedura Rekrutacji;
- Upoważnienia dla pracowników;
- Oświadczenia pracowników;
- Rejestr osób przetwarzających dane
- Wykaz pomieszczeń tworzących obszar, w którym przetwarzane są dane osobowe
- Opis zbiorów danych
- Plan sprawdzeń
- Sprawozdanie ze sprawdzenia
- Oświadczenia o przeszkoleniu

MODUŁ III – WARSZTATY – ANALIZA I SZACOWANIE RYZYKA.

ANALIZA RYZYKA

1. Metody szacowania ryzyka:
- jakościowa,
- ilościowa,
- mieszane – szczegółowa analiza różnych metod szacowania.
2. Określenie aktywów i ich właścicieli;
3. Określenie zagrożeń i podatności oraz innych wymagań dotyczących bezpieczeństwa informacji;
4 Określenie konsekwencji, jakie utrata rozliczalności, poufności, integralności i dostępności może mieć dla aktywów informacyjnych;
5. Szacowanie skutków i prawdopodobieństwa wystąpienia ryzyka oraz estymowanie poziomów ryzyka;
6. Określenie odpowiedniego wariantu postępowania z ryzykiem;
7. Wybór celów stosowania zabezpieczeń i zabezpieczeń mających na celu obniżenie ryzyka do poziomu akceptowalnego;
8. Macierze ryzyka;
9. Postępowanie z ryzykiem