2-DNIOWE SZKOLENIE DLA INSPEKTORÓW OCHRONY DANYCH

SZANOWNI PAŃSTWO,

Proponowany przez nas Kurs na Inspektora Ochrony Danych 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 2 dniowy kurs - 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. 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 4 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 – BEZPIECZEŃSTWO INFORMATYCZNE – CYBERBEZPIECZEŃSTWO;
4) WARSZTATY – ANALIZA I SZACOWANIE RYZYKA.

Uczestnicy Kursu otrzymają CERTYFIKATY 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

Dzień 1

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
- zbiry 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;
- cykl PDCA (Plan-Do-Check-Act)
- kontekst organizacji;
- cele;
- zasoby;
- kompetencje;
- monitorowanie;

3. Audyt:

- Audyt pierwszej strony;
- Audyt drugiej strony;
- Audyt trzeciej strony;

4. Plan sprawdzeń; przykłady i analiza;
5. Listy kontrolne; przykłady i analiza;
6. Raport poaudytowy – struktura i analiza;
7. 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
- Procedura weryfikacji tożsamości
- Procedura udzielania informacji
- Procedura rozpoznawania
- Procedura udostępnienia danych
- Wykaz identyfikatorów
- Procedura haseł Administrator/Inspektor Ochrony Danych

PANEL DYSKUSYJNY

PODSUMOWANIE I ZAKOŃCZENIE DNIA DRUGIEGO

Dzień 2

MODUŁ III – WARSZTATY – BEZPIECZEŃSTWO INFORMATYCZNE

BEZPIECZEŃSTWO INFORMATYCZNE - CYBERBEZPIECZEŃSTWO

1. Inwentaryzacja zasobów:
- sprzęt informatyczny,
- systemy operacyjne i aplikacje,
- formularze internetowe i strony internetowe - jakie dane pobieramy,
- lokalizacja serwerów i ich wpływ na przetwarzanie danych,
- użytkownicy,
- obszar przetwarzania danych,

2. PZST – Polityka Zarządzania Systemem Teleinformatycznym:
- przydział identyfikatorów i kodów dostępu,
- sposób uwierzytelniania,
- polityka haseł,
- rejestrowanie i wyrejestrowywanie użytkowników – Procedura Nadawania/Odbierania Uprawnień;
- co to jest architektura systemu?
- łącza transmisji danych,
- oprogramowanie systemowe,
- wymagania systemów:

3. Polityka czystego biurka i ekranu
4. Zabezpiecznia prewencyjne
5. Zabezpiecznia doraźne
6. Elektroniczne nośniki danych osobowych
7. Bezpieczne drukowanie
8. Zasady bezpieczeństwa przy korzystaniu ze sprzętu komputerowego
9. Zasady bezpiecznej pracy w przypadku dostępu zdalnego
10 Zabezpieczanie plików

MODUŁ IV – 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. Etap I: Wstępny etap analizy ryzyka:

a) Identyfikacja aktywów
b) Wycena aktywów –oszacowanie ich wartości
c) Identyfikacja zagrożeń
d) Określenie podatności

9. Etap II –Szacowanie ryzyka :

a) Wybór metody analizy ryzyka
b) Oszacowanie wartości ryzyka

10. Etap III –Strategia postępowania z ryzykiem:

a) Określenie postępowania z ryzykiem
b) Obniżenie ryzyka do poziomu akceptowalnego, poprzez wybór stosownych zabezpieczeń;

11. Macierze ryzyka;
12. Postępowanie z ryzykiem

PANEL DYSKUSYJNY

PODSUMOWANIE I ZAKOŃCZENIE SZKOLENIA

Szkolenie prowadzi:

Łukasz Laskowski

Radca Prawny | Ekspert ds. Ochrony Danych Osobowych | Inspektor Ochrony Danych

Radca prawny, absolwent Wydziału Prawa, Administracji i Ekonomii Uniwersytetu Wrocławskie. Inspektor Ochrony Danych Osobowych w placówkach samorządowych, przedsiębiorstwach i organizacjach. Wykładowca Wyższej Szkoły Prawa we Wrocławiu, Instytutu Szkolenia Ekonomiczno-Prawnego w Opolu, Polskiego Towarzystwa Ekonomicznego Zakładu Szkolenia i Doradztwa Ekonomicznego w Opolu. Prowadzi szkolenia z zakresu ochrony danych osobowych dla przedsiębiorstw, instytucji samorządowych, instytucji państwowych, organizacji społecznych i stowarzyszeń. Doświadczenie zawodowe zdobywał jako doradca prawny w Frąckowiak Marek CPF we Wrocławiu, następnie jako asystent sędziego w Sądzie Apelacyjnym we Wrocławiu, a od 2009 r. prowadzi indywidualną praktykę zawodową jako kancelarie radcy prawnego. Specjalizuje się w sprawach z zakresu prawa pracy i ubezpieczeń społecznych, prawa sportowego, ochrony danych osobowych i sprawach gospodarczych. Współpracuje z Okręgiem Dolnośląskim Polskiego Związku Niewidomych.

Mariusz Kania

Ekspert ds. Ochrony Danych Osobowych | Inspektor Ochrony Danych

Specjalizuje się w bezpieczeństwie systemów informatycznych, w szczególności we wdrażaniu systemów bezpieczeństwa w strukturach informatycznych naszych Klientów. W oparciu o wyniki audytów przygotowuje i wdraża instrukcje zarządzania systemami informatycznymi. W tej materii prowadzi również szkolenia dla pracowników administracji publicznej, firm z sektora MiŚP spółek, placówek medycznych oraz dla kadry zarządzającej. Jako czynny Inspektor Ochrony Danych posiada doświadczenie w zakresie ochrony danych osobowych. Od ponad 15 lat zajmuje się systemami informatycznymi i ich bezpieczeństwem w szczególności bezpieczeństwem w Internecie. Jako audytor Mariusz uczestniczył w wielu projektach audytorskich i kontrolnych zarówno w spółkach typu korporacyjnego, jak i firm z sektora MSP, w których wdrażał procedury i polityki systemu bezpieczeństwa informacji i systemu zarządzania systemami informatycznymi.