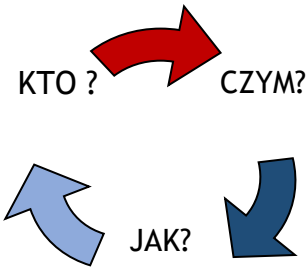
KOMPLEKSOWE ZDALNE WARSZTATY

na temat:

„ZASADY ORGANIZACJI OCHRONY INFORMACJI W ŚWIETLE PRZEPISÓW O SYSTEMIE CYBERBEZPIECZEŃSTWA - A ZADANIA IOD i ASI”

Problem wiodący: czy inspektor ochrony danych osobowych lub ASI odpowiada za cyberbezpieczeństwo[1]?



ZAPEWNIA CYBERBEZPIECZEŃSTWO W ORGANIZACJI

INSPEKTOR OCHRONY DANYCH OSOBOWYCH CONSULTING

JAROSŁAW FELIŃSKI

EDUKACJA JAKO ELEMENTARNA WARTOŚĆ BEZPIECZEŃSTWA DANYCH I INFORMACJI

[1] Ustawa z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa1),2)

Inspektor Ochrony Danych Osobowych Consulting Jarosław FELIŃSKI
75-604 Koszalin; ul. Zwycięstwa 138/4 - siedziba NIP 669 105 09 71 REGON 321364647
KONTAKT: mb - 602105852 v 508608136
jaroslaw.felinski@gazeta.pl

Jarosław Feliński - Praktyk, wykładowca wyższych uczelni; (wykładowca na studiach podyplomowych z problematyki zarządzania bezpieczeństwem informacji: **Uniwersytetu Jagiellońskiego** w Krakowie; AGH Kraków; DSW Wrocław; WSAP Szczecin; Wyższej Szkoły Informatyki Stosowanej i Zarządzania pod auspicjami Polskiej Akademii Nauk WIT Warszawa, **Twórca autorskiego programu podyplomowych studiów zarządzania bezpieczeństwem informacji dla ABI 2013 i IODO 2017** – kierownik studiów podyplomowych w roku akademickim od 2013 – 2017/2018. Autor programu studiów podyplomowych **„Inspektor Ochrony Danych Osobowych – poziom zaawansowany"** w WSISiZ PAN Warszawa - od 2017/2018. **Audytor Wiodący PN ISO/IEC 27001 [IRCA]. Prezes Zarządu Stowarzyszenia Inspektorów Ochrony Danych Osobowych w Polsce.**

Proponowany czas zajęć – 9.30 / 15.30

Cel i zakres główny szkolenia:

- określenie zasad organizacji ochrony informacji i danych osobowych w świetle RODO i przepisów prawa polskiego o cyberbezpieczeństwie;
- wykazanie możliwości wykonania zadań ochrony danych w połączeniu z ochroną informacji i cyberbezpieczeństwem;
- wykazanie zadań osób funkcyjnych, IODO / ASI i innych osób określonych w ustawie o cyberbezpieczeństwie – *„Art. 9. 1. Operator usługi kluczowej: - wyznacza osobę odpowiedzialną za utrzymywanie kontaktów z podmiotami krajowego systemu cyberbezpieczeństwa";*
- omówienie zadań pracowników, wykonawców usług i relacji z innymi podmiotami w zapewnieniu cyberbezpieczeństwa;
- omówienie reguł ochrony informacji w kontekście prawa do ochrony danych i informacji w świetle *„cyberustawy";*
- celowość dokonywania audytów bezpieczeństwa danych wg RODO;
- metody i standardy opracowania dokumentacji określonej w Rozporządzeniu[2] i zasady ich wdrożeń;
- zasady realizacji zadań wykazanych w Rozporządzeniu jako środki techniczne zabezpieczeń;
- omówienie zakresu § 1. 1. podmiot świadczący usługi z zakresu cyberbezpieczeństwa w zakresie warunków organizacyjnych jest obowiązany **dysponować personelem posiadającym umiejętności i doświadczenie** w zakresie:

  - identyfikowania zagrożeń w odniesieniu do systemów informacyjnych,
  - analizowania oprogramowania szkodliwego i określania jego wpływu na system informacyjny operatora usługi kluczowej,
  - zabezpieczania śladów kryminalistycznych na potrzeby postępowań prowadzonych przez organy ścigania.

[2] ROZPORZĄDZENIE MINISTRA CYFRYZACJI z dnia 10 września 2018 r. w sprawie warunków organizacyjnych i technicznych dla podmiotów świadczących usługi z zakresu cyberbezpieczeństwa oraz wewnętrznych struktur organizacyjnych operatorów usług kluczowych odpowiedzialnych za cyberbezpieczeństwo

AGENDA I PROGRAM ZAJĘĆ

I. Nowe obowiązki podmiotów kluczowych w świetle przepisów ustawy:

a. Pojęcia podstawowe i ich zastosowanie w organizacji
b. Struktura ochrony informacji w organizacji – schemat organizacyjny zmiany
c. Status i zakres zadań *„wyznaczonej osoby odpowiedzialnej”*;
d. Kompetencje i wiedza osoby wyznaczonej;
e. Słowniczek pojęć od **A**ktywa do **Z**agrożenia;
f. System Zarzadzania Bezpieczeństwem Informacji [SZBI] – czym jest;
g. Znaczenie i kontekst informacji w SZBI

II. Obowiązki prawne IODO po nowelizacji RODO

a. Dokumentowanie procesów zarządzania bezpieczeństwem informacji;
b. Zasady i zakres opracowania dokumentacji określonej w ustawie;
c. Kompletność SZBI z regulacjami wewnętrznymi;
d. Zadania Zarządu w procesie opracowania rozwiązania;
e. Wyjaśnienie określenia ustawowego określenia „zrozumienie zagrożeń cyberbezpieczeństwa”,
f. Warunki komunikacji z „organem właściwym do spraw cyberbezpieczeństwa”,
g. Standaryzacja dokumentacji wg PN ISO27001

III. Standard ISO PN 27001

a. Zakres i połączenie normy z przepisami ustawy;
b. Zadania i wymagania ISO jako podstawa do tworzenia SZBI;
c. Wymagania formalne SZBI, bez pomijania wymagań obowiązkowych;
d. Przesłanki legalności dostępu do dokumentacji o cyberbezpieczeństwie;
e. Określenie znaczenia pojęć i działań w przypadku naruszenia i incydentu;
f. Ewidencja osób uprawnionych dokumentacji i zasady jej ochrony;
g. Wymagania w zakresie dokumentacji;
h. Ocena zagrożeń wg PN 27001 i 27002 i 27005;

IV. Obowiązki w zakresie zabezpieczeń fizycznych

a. Zabezpieczenia fizyczne nośników;
b. Zbiorów papierowych, nośników elektronicznych;
c. Bezpieczeństwo danych w relacjach zewnętrznych;
d. Upoważnienia do przetwarzania danych – wariant;
e. Reagowanie na incydenty;
f. Zasady prowadzenia nadzoru wewnętrznego i odpowiedzialność.

Szkolenie kończy się sprawdzeniem wiedzy i uzyskaniem zaświadczenia.

KOSZTORYS ZAJĘĆ

Proponowany czas zajęć: 9.30 – 16.30

Sala wirtualna

Ograniczenie Covid 19

ROZLICZENIE FAKTURA VAT.

Cena uczestnictwa 350 zł netto

Informacja: https://www.iodoconsulting.pl/

Kontakt w sprawie zgłoszenia: iodo@iodoconsulting.pl