OCHRONA DANYCH OSOBOWYCH PO 1 STYCZNIA 2015

Oferta szkoleniowa

W dniu 1 stycznia 2015 r. weszła w życie nowelizacja ustawy z dnia 29 sierpnia 1997 r. o ochronie danych osobowych. Problemy interpretacyjne nowych przepisów oraz rozszerzony zakres odpowiedzialności wymaga od kierowników jednostek wdrożenia dodatkowych rozwiązań organizacyjnych w obszarze ochrony danych osobowych.

I. O NAS

Open-Security Audit Project (lub **Open – Audit**) jest firmą o charakterze specjalistycznym, wspierającą procesy profesjonalnego planowania, wdrażania i monitorowania mechanizmów zabezpieczeń systemów IT i danych w sektorze publicznym i prywatnym. Realizowane przez nas projekty związane są ściśle z zagrożeniami w procesach biznesowych, dla danych czy w systemach informatycznych.

Poza działalnością o charakterze technicznym, wspieramy również naszych klientów w planowaniu i realizacji zabezpieczeń danych pod kątem wymagań prawnych, zarówno na poziomie krajowym (PL) jak i międzynarodowym (UE).

Nasze projekty realizujemy zgodnie z metodyką **PRINCE2** lub inną preferowaną przez naszych klientów. Przy małych projektach dobieramy metodykę tak, aby nie budowała barier, lecz wspierała nas i klienta w optymalnej ścieżce wytworzenia zamierzonego efektu.

Nasze kompetencje skierowane są na …

OBSZAR PROCESOWEGO ZARZĄDZANIA BEZPIECZEŃSTWEM

- Analizujemy architekturę bezpieczeństwa organizacji pod kątem zgodności z TOGAF;
- Organizujemy i przeprowadzamy audyty bezpieczeństwa informacji pod kątem zgodności systemów zarządzania bezpieczeństwem informacji z normami grupy ISO/IEC 27000 (w szczególności ISO/IEC 27001: 2013 czy PN-ISO/IEC 27001:2014);
- Organizujemy i przeprowadzamy audyty bezpieczeństwa systemów informatycznych według standardów COBIT i CISA;
- Organizujemy i przeprowadzamy audyty systemów zarządzania bezpieczeństwem pod kątem zgodności z obowiązującymi regulacjami prawnymi [PL], w szczególności, zgodnie z zapisami:
  - Ustawy z dnia 17 lutego 2005 r. o informatyzacji działalności podmiotów realizujących zadania publiczne i związanego z nią rozporządzenia Rady Ministrów z dnia 12 kwietnia 2012 r. w sprawie Krajowych Ram Interoperacyjności, minimalnych wymagań dla rejestrów publicznych i wymiany informacji w postaci elektronicznej oraz minimalnych wymagań dla systemów teleinformatycznych;
  - Ustawy z dnia 29 sierpnia 1997 r. o ochronie danych osobowych.
- Projektujemy i budujemy Systemy Zarządzania Bezpieczeństwem Informacji (SZBI / ISMS)
- Wykonujemy analizy i projektujemy procesy zarządzania bezpieczeństwem w modelu usługowym opartym o:
  - Normę ISO/IEC 20000-1 i ISO/IEC 20000-2;
  - Information Technology Infrastructure Library (ITIL).
- Współpracujemy z zespołami CERT (w tym CERT.GOV.PL) w imieniu naszych klientów.

OBSZAR ZABEZPIECZEŃ TECHNICZNYCH

- Prowadzimy techniczne audyty bezpieczeństwa systemów teleinformatycznych pod kątem wykrycia podatności na ataki (wykonujemy również testy penetracyjne);
- Projektujemy i wdrażamy zabezpieczenia sieci, systemów operacyjnych oraz systemów aplikacyjnych opartych na technologiach WEB.

OBSZAR ANALITYCZNY

- Projektujemy i dokumentujemy procesy z wykorzystaniem notacji BPMN.
- Świadczymy usługi konsultacyjne (consulting), podczas:
  - Opracowywania założeń do Specyfikacji Istotnych Warunków Zamówienia. W takiej sytuacji, nasi eksperci pomagają organizacji w przygotowaniu dokumentacji przetargowej. Sami nie bierzemy wówczas udziału w postępowaniu;
  - Negocjacji z innymi dostawcami usług, gdy dochodzi do sytuacji spornych, w których trudno jest wypracować kompromis.

Open-Security Audit Project nie jest typową działalnością korporacyjną. Nasze zespoły są dedykowane dla każdego kontraktu, a klient nie ma problemu z dostępnością konsultantów. Współpracujemy również na podstawie średnio i długo terminowych kontraktów. Wizytówką naszych Kierowników Projektów w czasie spotkań biznesowych jest wiedza, doświadczenie oraz wysoki poziom kultury osobistej. Naszą misją jest popularyzacja mechanizmów zabezpieczających uniemożliwiających kradzież danych z systemów teleinformatycznych. Nie jesteśmy dostawcami technologii, ale w ramach prowadzonych projektów współpracujemy z naszymi partnerami dostarczającymi technologiczne rozwiązania bezpieczeństwa.

Posiadamy wiedzę potwierdzoną certyfikatami:

- C|EH (Certified Ethical Hacker / Etyczny Hacker);
- CompTIA Security+;
- ITILv3;
- PRINCE2;
- ISO 27001 (audytor wiodący);
- ISO 27001 (audytor wewnętrzny);
- RHCE (inżynier systemowy Red Hat Enterprise Linux).

Posiadamy wiedzę i doświadczenie związane z regulacjami prawnymi, w tym realizując zadania:

- Pełnomocników ds. Bezpieczeństwa Cyberprzestrzeni działając na rzecz podmiotu zlecającego (kontrakt);
- Architektów i wdrożeniowców wymagań Krajowych Ram Interoperacyjności;
- Administratorów Bezpieczeństwa Informacji.

Zapewniamy całkowitą zgodność naszych działań z rozporządzeniem Rady Ministrów z dnia 12 kwietnia 2012 r. w sprawie Krajowych Ram Interoperacyjności, minimalnych wymagań dla rejestrów publicznych i wymiany informacji w postaci elektronicznej oraz minimalnych wymagań dla systemów teleinformatycznych.

II. TEMATYKA SZKOLENIA

Ustawodawstwo zarówno krajowe, jaki i europejskie określa dokładne zasady ochrony danych osobowych. Na obszarze Europy, ochrona danych osobowych uregulowana jest dyrektywą „95/46/EC PARLAMENTU EUROPEJSKIEGO I RADY z dnia 24 października 1995 w sprawie ochrony osób fizycznych w zakresie przetwarzania danych osobowych oraz swobodnego przepływu tych danych". W Polsce, zasady te określa ustawa „z dnia 29 sierpnia 1997 r. o ochronie danych osobowych", której nowelizacja weszła w życie w dniu 1 stycznia 2015 r. ustanawiając nowe zasady ich ochrony.

W obecnym kształcę regulacji, nie można zostawić przypadkowi ochrony danych osobowych, a nadzór nad realizacją polityki ich ochrony w instytucjach publicznych i w firmach prywatnych został, w rozumieniu ustawy, znacząco zaostrzony.

III. SZCZEGÓŁOWA OFERTA SZKOLENIA

Szkolenie dotyczy przede wszystkim **Administratorów danych osobowych** i powołanych **Administratorów Bezpieczeństwa Informacji**, kadry kierowniczej odpowiedzialnej za system ochrony danych oraz pracowników działów kadr, obsługi klienta i innych działów przetwarzających dane osobowe. Z uwagi na nowelizację ustawy o ochronie danych osobowych, procedura powoływania ABI w organizacjach musi być przemyślaną decyzją kierownictwa, na co również zwrócimy uwagę podczas szkolenia.

Uczestnictwo w szkoleniu pozwala na oswojenie się z nowymi zadaniami, a także ułatwia wdrożenie zasad ochrony danych w jednostce przetwarzającej dane osobowe. Szkolenie ma na celu przede wszystkim zaznajomienie uczestników z zasadami ochrony danych osobowych wynikającymi z przepisów prawa (w tym również z najnowszej nowelizacji ustawy) i dobrych praktyk, a także na aspekty praktyczne pracy z danymi osobowymi i codzienne problemy przy wykonywaniu obowiązków związanych z przetwarzaniem danych.

<u>W trakcie szkolenia odpowiemy na pytania</u>

- Jak przetwarzać dane osobowe zgodnie z prawem;
- Jak stworzyć i wdrożyć system ochrony danych osobowych;
- Jak powinna wyglądać dokumentacja ochrony danych osobowych;
- Jak należy zabezpieczać dane osobowe zgodnie z wytycznymi GIODO;
- Jak i z kim zawrzeć umowy powierzenia przetwarzania danych osobowych;
- Jak przygotować klauzule zgody na przetwarzanie danych osobowych;
- Jak wyodrębnić zbiory i które zbiory podlegają rejestracji w GIODO;
- Jak bez negatywnych konsekwencji przejść kontrolę GIODO.

<u>Szkolenie przeznaczone jest dla:</u>

- Osób kierujących organizacją, sprawujących nadzór zarządczy nad ochroną informacji;
- Osób bezpośrednio nadzorujących pracę komórek, w których przetwarzane są dane osobowe;
- Osób bezpośrednio nadzorujących komórkę informatyki;
- Osób bezpośrednio przetwarzających dane (pracownicy działów wprowadzania i przetwarzania danych, administratorów systemów informatycznych oraz pracowników obsługi spraw obywatelskich).

ZAKRES MERYTORYCZNY SZKOLENIA

1. **Ustawa o ochronie danych osobowych** - przegląd wprowadzonych zmian prawnych, które weszły w życie z dniem 1 stycznia 2015 r., w szczególności:
   - Analizę zapisów dotyczących obowiązków i odpowiedzialności **Administratorów Danych Osobowych (ADO),** których zadania są obecnie realizowane przez kierowników urzędów administracji państwowej;
   - Analizę zapisów dotyczących powoływania **Administratorów Bezpieczeństwa Informacji oraz obowiązków na nich nałożonych.**
2. **Rozporządzenie Ministra Spraw Wewnętrznych i Administracji** z dnia 29 kwietnia 2004 r. w sprawie dokumentacji przetwarzania danych osobowych oraz warunków technicznych i organizacyjnych, jakim powinny odpowiadać urządzenia i systemy informatyczne służące do przetwarzania danych osobowych.
3. **Ochrona danych osobowych w orzecznictwie**.
4. **Ochrona danych osobowych w praktyce** – jak interpretować nowe zapisy ustawy pod kątem rozwiązań praktycznych.
5. **Warsztat praktyczny** pokazujący jak:
   - Prawidłowo wypełnić wniosek rejestracyjny zbioru danych osobowych;
   - Prawidłowo wytwarzać dokumentację bezpieczeństwa zbiorów danych osobowych;
   - Prawidłowo prowadzić rejestr zbiorów danych osobowych;
   - Prawidłowo przygotowywać sprawozdanie Administratora Bezpieczeństwa Informacji przekazywane do GIODO;
   - Prawidłowo zorganizować zarządzanie bezpieczeństwem danych osobowych w instytucji (np. w procesie rekrutacji);
   - Prawidłowo zaplanować udział informatyki w ochronie danych.

FORMA SZKOLENIA

1. Wykład – prezentacja.
2. Warsztat.

CZAS TRWANIA SZKOLENIA

1 dzień roboczy (ok. 8 godzin z uwzględnieniem przerw kawowych i przerwy na lunch).

IV. TECHNICZNE ASPEKTY SZKOLENIA

Kurs prowadzony jest przez specjalistę ds. bezpieczeństwa, posiadającego wieloletnie doświadczenie w ochronie danych osobowych i w wytwarzaniu wymaganej ustawą dokumentacji bezpieczeństwa. Kurs prowadzony w sposób interaktywny, w postaci prezentacji multimedialnej, umożliwiając uczestnikom zadawanie pytań związanych z prezentowanym zagadnieniem.

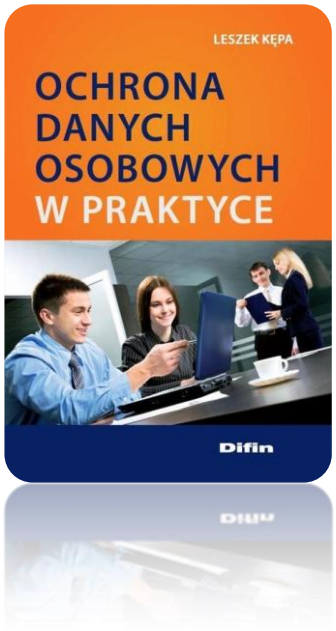
Każdy uczestnik szkolenia otrzymuje materiały dydaktyczne, zawierające:

1. Wydruk znowelizowanej ustawy o ochronie danych osobowych z zaznaczonymi zmianami, które weszły w życie z dniem 1 stycznia 2015 r.
    a. Wydruk rozporządzenia Ministra Administracji i Cyfryzacji z dnia 10 grudnia 2014 r. w sprawie wzorów zgłoszeń powołania i odwołania administratora bezpieczeństwa informacji;
    b. Wydruk rozporządzenia Ministra Spraw Wewnętrznych i Administracji z dnia 11 grudnia 2008 r. w sprawie wzoru zgłoszenia zbioru danych do rejestracji Generalnemu Inspektorowi Ochrony Danych Osobowych;
    c. Wydruk rozporządzenia Ministra Spraw Wewnętrznych i Administracji z dnia 29 kwietnia 2004 r. w sprawie dokumentacji przetwarzania danych osobowych oraz warunków technicznych i organizacyjnych, jakim powinny odpowiadać urządzenia i systemy informatyczne służące do przetwarzania danych osobowych.
2. Wydruk slajdów prezentacji szkoleniowej z miejscem na notatki ze szkolenia.
3. Przykład wypełnionego zgłoszenia zbioru danych osobowych do GIODO, opatrzony komentarzami.

Każdy uczestnik szkolenia otrzymuje certyfikat potwierdzający udział w szkoleniu.

V. WARUNKI FINANSOWE OFERTY

1. Całkowita kwota realizacji usługi wynosi **300 zł + VAT** za każdego uczestnika szkolenia.
2. Oferta jest ważna **60 dni** od dnia jej dostarczenia pocztą elektroniczną lub faksem.
3. Cena szkolenia nie obejmuje posiłków oraz ew. zakwaterowania uczestników szkolenia.
4. Cena szkolenia zakłada, że miejscem przeprowadzenia szkolenia jest siedziba Zamawiającego lub inna lokalizacja przez niego wskazana.
5. Cena szkolenia obejmuje grupy nie mniejsze niż 10 osób.
6. Cena szkolenia obejmuje drobny poczęstunek (kawa, herbata, woda, zimne przekąski).



UWAGA! Osoba, mająca pełnić funkcję **Administratora Bezpieczeństwa Informacji (ABI)** otrzyma w trakcie szkolenia książkę „Ochrona danych osobowych w praktyce", a jeżeli taka osoba nie została wyznaczona, książkę otrzyma Administrator Danych Osobowych lub osoba przez niego wyznaczona.

Z książki można dowiedzieć się m.in:

- Jak racjonalnie stosować się do wymagań ustawy;
- Co robić, gdy dane osobowe „wypłyną" poza organizację;
- W jaki sposób przygotować zgodę na przetwarzanie danych;
- Rejestracji zbioru danych krok po kroku;
- Jak zabezpieczać dane osobowe;
- Jak wygląda kontrola GIODO;
- Odpowiedzialność za nieprzestrzeganie przepisów;
- Jak przygotować się na przyszłe zmiany w prawie.

Zapraszam do współpracy
Marcin Kurpiewski