Plan szkolenia

Praktyczne aspekty wdrożenia ogólnego rozporządzenia o ochronie danych osobowych.

W dniu 27 kwietniu 2016 roku przyjęte zostało **Rozporządzenie o ochronie danych osobowych** w skrócie **RODO (ang. GDPR** - General Data Protection Regulation). Rozporządzenie **zacznie obowiązywać od dnia 25 maja 2018 roku.** Nowe przepisy zawarte w rozporządzeniu wprowadzają szereg zasad ochrony danych osobowych oraz ich przetwarzania, **określając wprost nowe obowiązki dla podmiotów** przetwarzających dane osobowe.

Nowe przepisy w przedmiocie ochrony danych osobowych wiążą się z koniecznością przeprowadzenia przez przedsiębiorców **dogłębnej analizy i weryfikacji wewnętrznych procesów dotyczących przetwarzania danych osobowych,** aby **dostosować się do wytycznych rozporządzenia pod względem prawnym, technicznym i organizacyjnym**.

Rozporządzenie zastąpi obowiązujące dotychczas ramy prawne ochrony danych osobowych, stanowiąc bezpośrednio skuteczną podstawę prawną regulującą kompleksowo prawa i obowiązki związane z przetwarzaniem danych osobowych.

Na podmioty oraz administratora danych osobowych i inspektora danych osobowych nakładane są l**iczne obowiązki** związane z **zapewnieniem środków technicznych i organizacyjnych** celem ochrony danych osobowych, aby zapewnić stopień bezpieczeństwa odpowiadający ryzyku. Oznacza to dla przedsiębiorcy **obowiązek pseudonimizacji i szyfrowania danych osobowych, zapewnienie poufności, integralności, dostępności i odporności systemów i usług przetwarzania, regularne testowanie, mierzenie i ocenianie skuteczności środków technicznych i organizacyjnych** mających zapewnić bezpieczeństwo przetwarzania.

Zapewnienie przygotowania organizacji do wejścia w życie nowej regulacji jest niezbędne.

Szkolenie pozwoli zdobyć wiedzę na temat przepisów i praktycznych rozwiązań dotyczącą stosowania unijnego rozporządzenia o ochronie danych osobowych przy wykonywaniu bieżących czynności, w tym wdrażaniu/modyfikacji systemów teleinformatycznych. Podczas szkolenia omówione zostaną nowe obowiązki administratora bezpieczeństwa informacji, zadania inspektorów ochrony danych w świetle nowych obowiązków ADO, dokumentacja przetwarzania danych osobowych oraz ich inwentaryzacja. Szkolenie pozwoli na poznanie do-

tychczasowych doświadczeń sprawdzenia zlecanego ABI przez GIODO. Na szkoleniu zaprezentowane zostanie narzędzie do zarządzania systemem ochrony danych osobowych.

Czas szkolenia: 6 godzin.

Program:

I. Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych (obowiązywanie bezpośrednio od 25 maja 2018 roku).

1. Administrator Bezpieczeństwa Informacji - zmiana statusu i zadań po wejściu do stosowania RODO
a) obowiązek wyznaczenia inspektora ochrony danych,
b) zadania w kontekście nowych obowiązków ADO,
c) rola w zarządzaniu ryzykiem,
d) niezależność inspektora ochrony danych.

2. Administrator Ochrony Danych Osobowych w RODO
a) zarządzanie uprawnieniami do przetwarzania danych osobowych,
b) rejestrowanie czynności przetwarzania danych osobowych.

4. Dokumentacja przetwarzania danych osobowych
a) prawo do ograniczenia przetwarzania,
b) powiadomienie o obowiązku sprostowania lub usunięciu danych osobowych rejestrowanie czynności przetwarzania,
c) domyślna ochrona danych osobowych (ochrona danych osobowych w fazie projektowania),
d) zgłoszenie naruszenia ochrony danych osobowych organowi nadzorczemu,
e) bezpieczeństwo przetwarzania,
f) rejestrowanie czynności przetwarzania,
g) usuwanie danych,
h) ocena skutków dla ochrony danych osobowych.

5. Zabezpieczenia stosowane w RODO
a) zdarzenia zagrażające bezpieczeństwu danych,
b) przykłady organizacyjnych środków bezpieczeństwa,
c) obowiązki pracownika,
d) zabezpieczenie systemów,

e) kontrola dostępu do systemów,
f) bezpieczeństwo funkcjonowania,
g) przesyłanie danych,
h) identyfikatory i hasła,
i) nośniki danych i niszczenie danych.

6. Analiza ryzyka w RODO
a) wymagania analizy ryzyka na etapie projektowania,
b) przeprowadzenie analizy ryzyka w celu doboru zabezpieczeń ,
c) wymagania analizy ryzyka dotyczące oceny skutków przetwarzania,
d) przeprowadzenie wcześniejszych konsultacji,
e) konsekwencje naruszenia ochrony danych osobowych (zgłoszenie naruszenia organowi nadzorczemu, zawiadomienie podmiotu danych, dokumentowanie incydentu, odpowiedzialność karna).

7. Inwentaryzacja danych osobowych
a) lokalny rejestr zbiorów,
b) rejestr czynności (dane osobowe administratora i inspektora ochrony danych, cele przetwarzania, kategorie odbiorców, terminy usunięcia poszczególnych kategorii danych, techniczne i organizacyjne środki bezpieczeństwa).

8. Sprawdzenia zlecane ABI przez GIODO
a) rodzaje sprawdzeń,
b) opracowanie planu sprawdzeń,
c) przeprowadzenie i dokumentowanie sprawdzeń,
d) prowadzenie postępowań w formie audytów ochrony danych,
e) przygotowanie sprawozdania dla ADO.

9. Odpowiedzialność na podstawie RODO z tytułu naruszenia zasad ochrony danych osobowych
a) odpowiedzialność administracyjna (uprawnienia naprawcze organu nadzorczego),
b) kary pieniężne i ich wysokość,
c) postępowanie w przypadku naruszenia ochrony danych osobowych,
d) postępowanie sprawdzające doraźne w sytuacji naruszenia danych osobowych.

II. Prezentacja narzędzia do zarządzania systemem ochrony danych osobowych.
1. Szyfrowanie wiarygodnie zabezpieczające wytwarzanie, gromadzenie i przekazywanie danych.
2. Przechowywanie danych na serwerze w postaci zaszyfrowanej.
3. Brak dostępu do danych przez administrację serwera.

Adresaci:

Zarządy banków i dyrektorzy oddziałów, pracownicy zajmujący się przetwarzaniem danych osobowych, pracownicy sporządzający dokumentację przetwarzania danych osobowych, audytu, prawnicy, pracownicy działu reklamacji, zgodności i compliance, pracownicy odpowiedzialni za ochronę danych osobowych, informatycy i pracownicy działów IT.

Korzyści :

- Zastosowanie podejścia opartego na zminimalizowaniu ryzyka potencjalnych kar i odpowiedzialności związanymi z umyślnym lub nieumyślnym niedotrzymaniu obowiązków RODO.
- Zapoznanie z zakresem zmiany statusu i zadań administratora bezpieczeństwa informacji po wejściu RODO.
- Nabycie umiejętności sporządzania dokumentacji niezbędnej do przetwarzania danych osobowych.
- Zapoznanie z lokalnym rejestrem zbiorów, rejestrem czynności i operacji.
- Zapoznanie z zadaniami Inspektora Ochrony Danych w RODO.
- Nabycie wiedzy dotyczącej organizacyjnych środków bezpieczeństwa (zabezpieczenie danych, zabezpieczenie systemów, kontrola dostępu).
- Poznanie zasad rejestracji zbiorów danych osobowych i administratorów bezpieczeństwa informacji.
- Zapoznanie z rekomendacjami GIODO.
- Zapoznanie z warunkami stosowania ustawy o ochronie danych osobowych przy budowie systemów teleinformatycznych.
- Poznanie dotychczasowych doświadczeń w sprawdzeniach zlecanych administratorowi bezpieczeństwa informacji przez GIODO.
- Prezentacja przykładowego narzędzia do zarządzania systemem ochrony danych osobowych.