## Formularz zgłoszenia na warsztaty: Realizowanie (w praktyce) zadań wynikających z przepisów o ochronie danych osobowych

Warsztaty oparte są na analizowaniu problemów z codziennej pracy przy danych osobowych i z bezpieczeństwem informacji w kontekście obowiązujących przepisów, decyzji GIODO oraz orzecznictwa. Podczas warsztatów uczestnicy będą musieli poradzić sobie:

* z konkretnymi incydentami bezpieczeństwa
* trudnym szefem, który nie rozumie ich roli w zakresie nadzorowania bezpieczeństwa informacji
* pracownikami, którzy „robią po swojemu”
* pismem z GIODO
* kontrolą z przestrzegania przepisów w praktyce
* decyzją GIODO nakazującą przywrócenie stanu zgodnego  z prawem
* analizą ryzyka i zagrożeń
* niewłaściwym zabezpieczeniem danych
* niezgłoszonymi od dawna zbiorami do GIODO
* nadawaniem i zmienianiem upoważnień do przetwarzania danych
* aktualizacją polityki bezpieczeństwa, którą zrobił ktoś inny
* współpracą z informatykiem, który współpracować nie chce

Warsztaty są skierowane do osób, które nadzorują przestrzeganie przepisów o ochronie danych osobowych w praktyce. Mają na celu wzbogacenie uczestników o praktyczne umiejętności, które będą w stanie przełożyć na codzienną pracę. Na warsztatach będą mieli okazję przekuć wiedzę w praktykę. Udział w obu dniach ma zapewnić kompleksowe przygotowanie do realizowania związanych z nadzorowaniem i audytowaniem bezpieczeństwa informacji.

**Program (każdy punkt zawiera, krótkie wprowadzenie do teorii, a następnie zajęcia praktyczne)**

**Dzień 1**

Opracowywanie oraz aktualizacja dokumentacji bezpieczeństwa (tworzenie systemu zarządzania informacją, analiza ryzyka i zagrożeń, nadzór nad procesem upoważniania do przetwarzania danych)

1. Podstawowe pojęcia: polityka bezpieczeństwa, instrukcja zarządzania systemami informatycznymi, ewidencja upoważnień, upoważnienia, oświadczenie o zachowaniu poufności, analiza ryzyka i zagrożeń, kodeksy postępowania.
2. Przeprowadzanie analizy ryzyka i zagrożeń
3. Tworzenie polityki bezpieczeństwa krok po kroku
4. Obligowanie pracowników/współpracowników do zachowania informacji w poufności
5. Nadawanie/zmienianie upoważnień
6. Prowadzenie ewidencji upoważnień
7. Tworzenie instrukcji zarządzania systemem informatycznym krok po kroku
8. Nadzór nad adekwatnością dokumentacji bezpieczeństwa do ryzyka i zagrożeń
9. Wprowadzanie systemu zarządzania bezpieczeństwem informacji

**Dzień 2**

Realizowanie zadań ABI w praktyce: przeprowadzanie sprawdzeń, pisanie sprawozdań, reagowanie na incydenty, prowadzenie rejestru zbiorów)

1. Podstawowe pojęcia: dokumentacja bezpieczeństwa, polityka reagowania na naruszenia bezpieczeństwa informacji, plan sprawdzeń, sprawdzenia zgodności przetwarzania z przepisami, kontrole, sprawozdania dla ADO i GIODO, rejestr zbiorów prowadzony przez ABI, rejestr zbiorów prowadzony przez GIODO
2. Realizowanie zadań ABI/osoby nadzorującej przestrzeganie przepisów: problemy i dylematy
3. Polityka reagowania na naruszenia bezpieczeństwa: czy warto ją wprowadzać, czy warto reagować na każdy incydent?
4. Przygotowywanie planu sprawdzeń
5. Przeprowadzanie sprawdzeń planowych, doraźnych i dla GIODO
6. Przygotowywanie sprawozdania ze sprawdzenia
7. Kontrola zewnętrzna w zakresie zgodności przetwarzania z przepisami
8. Prowadzenie rejestrów zbiorów przez ABI / zgłaszanie zbiorów do GIODO.
9. Wykreślanie zbiorów z rejestrów.

**Termin warsztatów: 23-24 marca 2017 roku (czwartek i piątek).**
Miejsce: **komfortowa, klimatyzowana sala w centrum konferencyjnym Cube Center przy ul. Pięknej 24/26 A w ścisłym centrum Warszawy.**

Podczas szkolenia przewidziany jest bufet kawowy oraz obiad. Uczestnicy otrzymają dodatkowo podczas trwania warsztatów wodę do picia oraz ciastka. Przewidziane są zarówno materiały papierowe, niezbędne do realizacji ćwiczeń, jak i elektroniczne. Każdy uczestnik otrzyma świadectwo odbycia warsztatów.

Ramy czasowe:

* 9:30-10:00 Rejestracja uczestników, bufet kawowy
* 10:00 – 12:30 Pierwsza część warsztatów
* 12:30 – 13:00 Obiad
* 13:00 – 15:30 Druga część warsztatów

**Koszt udziału dla podmiotów publicznych:**

* Dla uczestnika, który weźmie udział jedynie w jednym wybranym dniu:  250 zł + 23% VAT
* Dla uczestnika, który weźmie udział w obu dniach szkolenia 450 zł + 23 VAT
* Istnieje możliwość otrzymania faktury ze zwolnieniem z VAT, na podstawie przysłanego skanu oświadczenia o zwolnieniu podmiotowym.

**Koszt udziału do pozostałych:**

* Dla uczestnika, który weźmie udział jedynie w jednym wybranym dniu:  400 zł + 23% VAT
* Dla uczestnika, który weźmie udział w obu dniach szkolenia 700 zł + 23 VAT

## Zgłoszenie uczestnika:

Imię, nazwisko oraz e-mail uczestnika:

|  |
| --- |
|  |

Dane płatnika FV (nazwa, adres, NIP):

|  |
| --- |
|  |

Zgłoszenia na

🗖 Oba dni warsztatów (23 i 24 marca)

🗖Tylko dzień 1: Opracowywanie oraz aktualizacja dokumentacji bezpieczeństwa (tworzenie systemu zarządzania informacją, analiza ryzyka i zagrożeń, nadzór nad procesem upoważniania do przetwarzania danych)

🗖 Tylko dzień 2: Realizowanie zadań ABI w praktyce: przeprowadzanie sprawdzeń, pisanie sprawozdań, reagowanie na incydenty, prowadzenie rejestru zbiorów)

Oświadczenie o zwolnieniu z VAT

🗖 Oświadczam, że nabyta od firmy ESCEKA – Sylwia Czub-Kiełczewska usługa szkoleniowa jest finansowana ze środków publicznych w całości, zgodnie z treścią art. 43 ust. 1 pkt 29 lit c ustaw z dnia 11 marca 2004 roku o podatku od towarów i usług. Tym samym wystawiona faktura jest zwolniona z podatku VAT.

Po zarezerwowaniu miejsca na warsztatach dla uczestnika, płatnik otrzyma fakturę proforma, której opłacenie będzie stanowiło potwierdzenie i zagwarantowania miejsca na warsztatach. W przypadku uczestników z podmiotów publiczny, faktura zostanie wystawiona w dniu warsztatów i wręczona uczestnikowi, który będzie miał 14 dni na jej opłacenie.

Data i podpis osoby zgłaszającej uczestnika szkolenia

|  |
| --- |
|  |

Administratorem danych osobowych jest ESCEKA – Sylwia Czub-Kiełczewska, z siedzibą przy ul. Piłsudskiego 111/28, 05-091 Ząbki. Dane będą przetwarzane w celu realizacji usługi szkoleniowej. Uczestnikowi oraz osobie zgłaszającej przysługuje prawo do wglądu i edycji swoich danych. Administrator danych nie przewiduje dalszego udostępniania danych. Podanie danych jest dobrowolne, ale niezbędne do przyjęcia zgłoszenia.