Załącznik nr 1
do Zapytania ofertowego

Opis usługi na przeprowadzenie Audytu Bezpieczeństwa Informacji na potrzeby Powiatowego Urzędu Pracy w Łańcucie

AUDYT RODO

ETAP I – WERYFIKACJA

I. Zdefiniowanie zasad zarządzania danymi osobowymi:

1. Polityka Bezpieczeństwa.
2. Weryfikacja dokumentów pod kątem zgodności z RODO:
- marketing, klienci, kontrahenci, pracownicy, formularze, klauzule, umowy: powierzenia, z podmiotami wsparcia
3. Inwentaryzacja danych:
- zbiory danych,
- aktywa,
- dane przekazywane stronom trzecim
4. Klasyfikacja danych.
5. Zarządzanie dostawcami.
6. Legalność przetwarzania danych:
- podstawa prawna, zgody, umowy

II. Weryfikacja procesów wdrożonych w organizacji:

1. Procesy inwentaryzacji, klasyfikacji danych:
- ewidencja danych osobowych,
- rejestry klasyfikacji
2. Procesy zarządzania zmianą:
- zarządzanie projektami,
- listy wymagań
3. Procesy zarządzania ryzykiem.
4. Procesy zarządzania dostawcami:
- weryfikacja i analiza umów

III. Weryfikacja procedur wdrożonych w organizacji:

1. Spełnianie obowiązku informacyjnego.
2. Przetwarzanie danych osobowych.
3. Sprostowanie danych osobowych.
4. Usuwanie danych osobowych.
5. Ograniczenia przetwarzania danych osobowych.
6. Przeniesienie/przejęcie danych.
7. Kopiowanie danych.

8. Wnoszenie sprzeciwu wobec przetwarzania danych osobowych.
9. Przekazywanie danych do państw trzecich.
10. Obsługa incydentów.

IV. Sprawdzenie zabezpieczeń, luk w systemie IT.
V. Sprawdzenie zgodności funkcjonowania systemów mailingowych z RODO.
VI. Sprawdzenie gotowości organizacji do stosowania przepisów w zakresie:
- profilowania i stosowania domyślnej ochrony danych

ETAP II – WDROŻENIE

I. Analiza ryzyk/ocena skutków:

1. Zbadanie obszaru ryzyka.
2. Opracowanie celów przetwarzania danych osobowych.
3. Określenie zasobów informatycznych.
4. Weryfikacja obecnych technicznych i organizacyjnych środków zabezpieczeń danych osobowych i kontroli nad ich przepływem.
5. Ocena wyników szacowania ryzyka.
6. Wdrożenie procesów zarządzania ryzykiem w firmie.

II. Opracowanie dokumentacji:

1. Opracowanie oświadczeń o poufności oraz upoważnień.
2. Stworzenie klauzul informacyjnych oraz zgód dotyczących przetwarzania danych.
3. Stworzenie ewidencji osób upoważnionych.
4. Stworzenie wzorów umów powierzenia/aneksów.
5. Przygotowanie rejestru czynności przetwarzania.
6. Przygotowanie polityki prywatności.
7. Opracowanie procesu związanego z obsługą incydentu.
8. Opracowanie technicznych i organizacyjnych środków zabezpieczeń.

Dostosowanie obecnie funkcjonującego systemu do wymogów RODO.
Przedstawienie zaleceń poprawy bezpieczeństwa danych osobowych.
Wsparcie merytoryczne przy pracy zespołu powołanego w zakresie bezpieczeństwa i kontroli w organizacji.

AUDYT WEWNĘTRZNY

1. Weryfikacja aktualizacji regulacji wewnętrznych w zakresie zmieniającego się otoczenia w zakresie bezpieczeństwa informacji.
2. Weryfikacja aktualności inwentaryzacji sprzętu i oprogramowania służącego do przetwarzania informacji.
3. Weryfikacja ryzyka utraty integralności, dostępności lub poufności informacji.
4. Weryfikacja uprawnień osób realizujących działania w zakresie bezpieczeństwa informacji.
5. Weryfikacja sposobu i procedur dotyczących zmiany uprawnień w systemie.

6. Weryfikacja stopnia świadomości pracowników w zakresie zagrożeń, naruszeń i skutków dotyczących nieuprawionego wykorzystania informacji.
7. Weryfikacja zabezpieczenia sprzętu przed dostępem osób nieuprawnionych.
8. Weryfikacja procedur w zakresie pracy mobilnej i na odległość.
9. Weryfikacja zapisów dotyczących zabezpieczania informacji zapisanych na nośnikach.
10. Weryfikacja zapisów w umowach z dostawcami gwarantujących odpowiedni poziom zabezpieczeń
11. Weryfikacja zasad postępowania z informacjami, które zapewniają minimalizację wystąpienia ryzyka kradzieży informacji
12. Weryfikacja systemu teleinformatycznego pod kątem:
- dbałości o aktualizację oprogramowania,
- minimalizowania ryzyka utraty informacji w wyniku awarii,
- ochrony przed błędami , utratą, nieuprawnioną modyfikacją,
- stosowania mechanizmów kryptograficznych w sposób adekwatny do zagrożeń,
- zapewnienia bezpieczeństwa plików systemowych,
- redukcji ryzyk wynikających z wykorzystania opublikowanych podatności technicznych systemów teleinformatycznych,
- podejmowanych działań w wyniku naruszenia bezpieczeństwa informacji,
- kontroli zgodności systemów teleinformatycznych z odpowiednimi normami i politykami bezpieczeństwa,
13. Weryfikacja sposobu zgłaszania incydentów oraz szybkość podjęcia działań korygujących.
14. Weryfikacja zapisów dotyczących przeprowadzania audytu wewnętrznego w zakresie bezpieczeństwa informacji na rzadziej niż raz na rok.

SZKOLENIE PRACOWNIKÓW

CZ**ĘŚĆ** I – JAK JEST

1.Ochrona danych osobowych - zagadnienia ogólne.
2. Przetwarzanie danych osobowych:
- Praktyczne aspekty przetwarzania danych osobowych pracowników oraz interesantów;
- Rola Administratora Danych Osobowych w strukturze organizacyjnej;
- Rola Administratora Bezpieczeństwa Informacji w strukturze organizacyjnej;
- Komunikacja z pozostałymi pracownikami przetwarzającymi dane osobowe;
3. Dokumentacja wymagana przez ustawę o ochronie danych osobowych:
- Polityka Bezpieczeństwa;
- Instrukcja Zarządzania Systemem Informatycznym;
- Upoważnienia dla pracowników;
- Umowy powierzenia przetwarzania danych osobowych;
4. Zbiory danych osobowych:
- Bezpieczeństwo w systemach teleinformatycznych

CZ**ĘŚĆ** II – RODO - CO SI**Ę** ZMIENI

1. Akty prawne
2. Pojęcie danych osobowych
- dane zwykłe – dane sensytywne;
3. Nowe definicje
- identyfikatory sieciowe, dane biometryczne, genetyczne, pseudonimizacja, profilowanie
4. Obowiązki Administratorów Danych
- obowiązek informacyjny, rejestrowanie czynności, zgłaszanie naruszeń, wdrożenie; mechanizmów „privacy by design" i innych

5. Inspektor Ochrony Danych:
- przejście Administratora Bezpieczeństwa Informacji na Inspektora Ochrony Danych;
- wyznaczenie Inspektora;
- status Inspektora;
- zadania Inspektora;
6. Szacowanie ryzyka
7. Umowy powierzenia
8. Prawa przysługujące podmiotowi danych
- do bycia zapomnianym, do przenoszenia danych, do niepodlegania profilowaniu i inne;
9. Organ nadzorczy
- nowa rola, status, zadania i uprawienia;
- sankcje za nieprzestrzeganie przepisów rozporządzenia: administracyjne kary pieniężne – warunki ich nakładania i wysokość, odszkodowanie za poniesioną szkodę;
10. Projekt ustawy o ochronie danych osobowych.