ZETO LUBLIN

OFERTA

Ochrona danych osobowych
i bezpieczeństwo informacji

Spis treści

1. Wdrożenia RODO

1.1. Przejecie funkcji IOD oraz wdrożenie RODO

Zapewniamy przejęcie funkcji Inspektora Ochrony Danych Osobowych (IOD) przez specjalistę spełniającego wymogi zawarte w RODO. Powołany IOD stoi na czele zespołu ekspertów, którzy zajmują się kompleksowym wdrożeniem wymagań ogólnego europejskiego rozporządzenia o ochronie danych osobowych w Twojej organizacji. Proces wdrożenia obejmuje poniżej wymienione obszary.

Audyt bezpieczeństwa informacji w szczególności:

a) Analiza urządzeń brzegowych;

b) Analiza istniejącej na dzień przeprowadzenia audytu topologii i konfiguracji sieci lokalnej;

c) Analiza parametrów technicznych urządzeń;

d) Analiza oprogramowania wykorzystywanego przez Zamawiającego w zakresie zabezpieczenia informatycznego;

e) Audyt centralnych urządzeń gromadzenia danych (serwery, macierze);

f) Audyt właściwości umów z dostawcami usług przechowywania danych.

Audyt zgodności ochrony danych osobowych:

a) Analiza wdrożonej dokumentacji dot. przetwarzania danych osobowych oraz ocena stopnia zgodności przyjętych procedur z wymaganiami określonymi w RODO;

b) Analiza procesów pozyskiwania danych osobowych (umowy, zgody, klauzule, obowiązek informacyjny etc.);

c) Weryfikacja zadań wykonywanych przez Administratora Bezpieczeństwa Informacji (ABI) (sprawdzenia i sprawozdania, raporty, zakres prowadzonych szkoleń, upoważnienia do przetwarzania danych osobowych);

d) Badanie poziomu wiedzy i znajomości przez pracowników obowiązujących w organizacji zasad i procedur dot. prawidłowego zabezpieczenia i przetwarzania danych osobowych (badanie ankietowe).

Analiza ryzyka i rejestr czynności przetwarzania danych osobowych:

a) Inwentaryzacja procesów, w których przetwarzane są dane osobowe – stworzenie szczegółowej mapy stanowiącej wykaz wszystkich procesów / czynności przetwarzania danych osobowych w organizacji;

b) Określenie potencjalnych zagrożeń, podatności i negatywnych skutków mających wpływ na procesy przetwarzania danych osobowych;

c) Identyfikacja obszarów, w których zachodzi wysokie ryzyko naruszenia podstawowych praw i wolności osób fizycznych, których dane przetwarza organizacja;

d) Ocena ryzyka i określenie obszarów wymagających dostosowania do przepisów RODO / GDPR;

e) Zbiorcze zestawienie wyników analizy – dane wejściowe do podejmowania decyzji odnośnie postępowania z ryzykiem.

Opracowanie dokumentacji zawierającej zasady i procedury przetwarzania danych osobowych zgodne z RODO m.in.:

a) Rejestr czynności przetwarzania danych osobowych i polityk ochrony danych;

b) Upoważnienia do przetwarzania danych osobowych;

c) Procedury dot. zabezpieczeń fizycznych stosowanych w organizacji;

d) Dostosowanie organizacji do nowych obowiązków informacyjnych;

e) Dostosowanie umów powierzenia przetwarzania danych osobowych;

f) Określenie zasad usuwania i przechowywania danych osobowych z uwzględnieniem przepisów sektorowych (zasady retencji danych osobowych) zgodnych z RODO.

Szkolenie pracowników z zakresu ochrony danych osobowych z zakresu:

a) stosowania procedur opracowanych w wyniku wdrożenia RODO w organizacji;

b) warsztatu wykonywania i aktualizacji analizy ryzyka;

c) dla pracowników odpowiedzialnych w organizacji za nadzór nad przetwarzaniem danych osobowych;

d) zarządzania incydentami bezpieczeństwa informacji, w tym ochrony danych osobowych – szczegółowe omówienie procedury notyfikowania organu o naruszeniu ochrony danych osobowych.

1.2. Wdrożenie RODO oraz wsparcie IOD

Zespół naszych ekspertów zajmie się kompleksowym wdrożeniem przepisów ogólnego europejskiego rozporządzenia o ochronie danych RODO w Twojej organizacji. Wykonamy wszystkie elementy opisane w punkcie pierwszym oferty oraz dodatkowo zapewnimy aktywne wsparcie dla IOD powołanego w Twojej organizacji.

Oferta ta obejmuje zakres czynności opisany w pkt. 1.1. **z wyłączeniem objęcia funkcji IOD**.

Wsparcie IOD obejmuje dostarczenie kompletu dokumentacji i instrukcji pozwalających na skuteczne zarządzanie procesami przetwarzania danych osobowych zidentyfikowanymi podczas wykonanego przez nas wdrożenia. Inspektor otrzyma wsparcie zespołu ekspertów z zakresu ochrony danych osobowych oraz bezpieczeństwa IT w postaci szeregu godzin konsultacyjnych oraz szkoleń z elementami warsztatów m.in. z zakresu wykonywania analizy ryzyka oraz oceny skutków przetwarzania danych osobowych.

2. Audyty i przygotowanie do wdrożenia RODO

2.1. Audyt

Zadania audytowe koncentrują się na weryfikacji bieżącego poziomu zabezpieczeń, spełnienia wymogów prawnych i proceduralnych określonych w ustawie z dnia 29 sierpnia 1997 r. o ochronie danych osobowych, w świetle nowych wymagań określonych w Rozporządzeniu 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 oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych RODO / GDPR).

Zadania audytowe realizowane są w kluczowych obszarach funkcjonowania organizacji i zostały podzielone na trzy podstawowe grupy. W ramach każdej grupy weryfikowany jest stopień spełnienia przez organizację wymagań dotyczących zabezpieczeń technicznych i proceduralnych określonych w RODO/GDPR i KRI.

Audyt bezpieczeństwa informacji:

a) Analiza urządzeń brzegowych;

b) Analiza istniejącej na dzień przeprowadzenia audytu topologii i konfiguracji sieci lokalnej;

c) Analiza parametrów technicznych urządzeń;

d) Analiza oprogramowania wykorzystywanego przez Zamawiającego w zakresie zabezpieczenia informatycznego;

e) Audyt centralnych urządzeń gromadzenia danych (serwery, macierze);

f) Audyt właściwości umów z dostawcami usług przechowywania danych.

Audyt zgodności ochrony danych osobowych:

a) Analiza wdrożonej dokumentacji dot. przetwarzania danych osobowych oraz ocena stopnia zgodności przyjętych procedur z wymaganiami określonymi w RODO;

b) Analiza procesów pozyskiwania danych osobowych (umowy, zgody, klauzule, obowiązek informacyjny etc.);

c) Weryfikacja zadań wykonywanych przez Administratora Bezpieczeństwa Informacji (ABI) (sprawdzenia i sprawozdania, raporty, zakres prowadzonych szkoleń, upoważnienia do przetwarzania danych osobowych);

d) Badanie poziomu wiedzy i znajomości przez pracowników obowiązujących w organizacji zasad i procedur dot. prawidłowego zabezpieczenia i przetwarzania danych osobowych (badanie ankietowe);

Analiza pod kątem obszarów wymagających dostosowania do RODO / GDPR

Wykonujemy ocenę stopnia wdrożenia poszczególnych wymagań określonych w RODO / GDPR oraz analizę ogólnego przygotowania organizacji do stosowania nowych przepisów dot. ochrony danych osobowych:

a) Analiza wykazu procesów przetwarzania danych osobowych;

b) Weryfikacja rejestru czynności przetwarzania danych osobowych;

c) Ocena metodyki i wykonania analizy ryzyka dla danych osobowych;

d) Analiza procedur dotyczących zarządzania incydentami bezpieczeństwa informacji, w tym procedury notyfikowania organu o naruszeniach ochrony danych osobowych;

e) Analiza polityk i procedur dotyczących realizacji praw osób, których dane dotyczą (prawo do bycia zapomnianym, prawo do przenoszenia danych, prawo do sprzeciwu etc.);

f) Analiza wzorów umów dot. powierzenia przetwarzania danych osobowych;

g) Weryfikacja metodyki wykonywania analiz ryzyka;

2.2. Audyt zgodności z wymaganiami rozporządzenia o krajowych ramach interoperacyjności (KRI)

Audyt obejmuje kompleksową analizę dostosowania systemów informatycznych do działalności w zakresie zadań publicznych. Wynikiem analizy całokształtu systemu IT jest określenie uwarunkowań nałożonych przez Ustawę z dnia 17 lutego 2005 r. o informatyzacji działalności podmiotów realizujących zadania publiczne. W swoim zakresie obejmuje:

a) Sprawdzenie systemów względem spełnienia norm przez organizację wynikających z Krajowych Ram Interoperacyjności;

b) Sprawdzenie procesów udostępniania danych cyfrowych podmiotom komercyjnym i podmiotom realizujących zadania publiczne;

c) Realizacja procesów związanych z platformą ePUAP.

2.3. Audyt ochrony danych osobowych

Audyt obejmuje analizę sposobu przetwarzania danych osobowych w organizacji.

a) Analiza wdrożonej dokumentacji dot. przetwarzania danych osobowych oraz ocena stopnia zgodności przyjętych procedur z wymaganiami określonymi w RODO /GDPR;

b) Analiza obecnie prowadzonych ewidencji i rejestrów w obszarze ochrony danych osobowych;

c) Analiza procesu nadawania, modyfikacji i cofania upoważnień do przetwarzania danych osobowych oraz zarządzania uprawnieniami dostępu do systemów informatycznych, w których przetwarzane są dane osobowe;

d) Analiza procesów pozyskiwania danych osobowych (umowy, zgody, klauzule, obowiązek informacyjny etc.);

e) Weryfikacja zadań wykonywanych przez Administratora Bezpieczeństwa Informacji (ABI) (sprawdzenia i sprawozdania, raporty, zakres prowadzonych szkoleń, upoważnienia do przetwarzania danych osobowych);

f) Badanie poziomu wiedzy i znajomości przez pracowników obowiązujących w organizacji zasad i procedur dot. prawidłowego zabezpieczenia i przetwarzania danych osobowych (badanie ankietowe);

Wyniki przeprowadzonych prac zostaną przedstawione w formie raportu wskazującego uchybienia oraz obszary wymagające dostosowania do wymagań RODO.

3. Dokumentacja zgodna z RODO

Oferujemy pakiet dokumentacji zgodnej z przepisami ogólnego europejskiego rozporządzenia o ochronie danych, którą możesz sam dostosować do potrzeb swojej organizacji.

Dokumentacja zawiera wzory:

a) Rejestru czynności przetwarzania danych osobowych;

b) Rejestru kategorii przetwarzanych danych osobowych;

c) Przykładowej analizy ryzyka wraz z metodyka i instrukcją jej przeprowadzenia;

d) Polityki ochrony danych;

e) Upoważnień do przetwarzania danych osobowych;

f) Regulaminów (np. regulamin wykorzystywania monitoringu wizyjnego);

g) Szczegółowych procedur dot. zapewnienia bezpieczeństwa w organizacji (np. polityka kluczy, polityka utylizacji nośników danych itp.);

h) Klauzul informacyjnych oraz zgód dot. przetwarzania danych osobowych;

i) Umów powierzenia przetwarzania danych osobowych;

j) Innych dokumentów pomocny przy spełnieniu wymagań RODO.

4. Szkolenia z tematyki ochrony danych osobowych - RODO

4.1. Praktyczne zastosowanie wymagań RODO w organizacji

W obszarze prawnym

- Stan prawny ulegający zmianie
- Zasady i podstawy przetwarzania danych osobowych
- Podstawy przetwarzania danych osobowych
- Nowe definicje RODO
- Obowiązki Administratora danych
- Funkcje i kompetencje Inspektora danych
- Umowa powierzenia
- Obowiązek informacyjny
- Odpowiedzialność za nieprzestrzeganie przepisów

W obszarze merytorycznym i IT

- Inne spojrzenie na ochronę danych osobowych
- Czy RODO ma coś wspólnego z normami ISO?
- Zagrożenia informacji w obszarach wspomaganych cyfrowo
- Dopasowanie istniejącej dokumentacji
- Analiza ryzyka
- Możliwość pomagania aplikacją informatyczną

4.2. Przygotowanie do pełnienia funkcji Inspektora Ochrony Danych osobowych w sektorze prywatnym i publicznym

Szkolenie kierowane jest do osób pełniących funkcję ABI oraz organizacji pierwszy raz powołujących w swoich strukturach Inspektora Ochrony Danych Osobowych. Tematyka szkolenia obejmuje omówienia wszystkich obowiązków nowego IODO wraz z praktycznymi wskazówkami i elementami warsztatów w zakresie tworzenia analiz ryzyka i rejestrów czynności przetwarzania danych osobowych. Uczestnicy zostaną również zapoznani z metodyką wykonywania audytów wewnętrznych ochrony danych osobowych. Tematy omawiane na szkoleniu:

a) Obowiązki i uprawnienia inspektora;

b) Wdrożenie RODO w organizacji;

c) Inwentaryzacja procesów przetwarzania danych osobowych;

d) Dokumentacja z zakresu ochrony danych osobowych w świetle ROD;

e) Szacowanie ryzyka i podejście oparte na ryzyku - wykonywanie analizy ryzyka i oceny skutków przetwarzania danych;

f) Incydenty ochrony danych osobowych i ich raportowanie do organu nadzorczego w ciągu 72 h;

g) Audyt wewnętrzny ochrony danych osobowych.

4.3. Podejście oparte na ryzyku w RODO - warsztaty

Szkolenie z elementami warsztatów wykonywania analizy ryzyka i oceny skutków przetwarzania danych (DPIA) w związku RODO.

Teoria:

Analiza ryzyka – ogólne rozporządzenie „RODO" wymaga, aby zastosowane zabezpieczenia w procesach związanych z przetwarzaniem danych osobowych były dobrane w oparciu o wyniki identyfikacji ryzyka tj. ocenę ryzyka pod kątem źródła, charakteru, prawdopodobieństwa i wagi zagrożenia oraz o najlepsze praktyki pozwalające zminimalizować to ryzyko. (obecnie obowiązująca ustawa też już na to wskazywała w **Art. 36.** ….. Administrator danych jest obowiązany zastosować środki techniczne i organizacyjne zapewniające ochronę przetwarzanych danych osobowych odpowiednią do zagrożeń oraz kategorii danych objętych ochroną…).

Warsztaty:

a) Inwentaryzacja procesów, w których przetwarzane są dane osobowe – stworzenie przykładowej mapy stanowiącej wykaz procesów / czynności przetwarzania danych osobowych w organizacji;

b) Określenie potencjalnych zagrożeń, podatności i negatywnych skutków mających wpływ na procesy przetwarzania danych osobowych;

c) Identyfikacja obszarów, w których zachodzi wysokie ryzyko naruszenia podstawowych praw i wolności osób fizycznych, których dane przetwarza organizacja;

d) Ocena ryzyka i określenie obszarów wymagających dostosowania do przepisów RODO;

e) Zbiorcze zestawienie wyników analizy – dane wejściowe do podejmowania decyzji odnośnie postępowania z ryzykiem.

4.4 Informacja publiczna w świetle RODO

Szkolenie, na którym zostaną przedstawione podstawowe zagadnienia związane z dostępem do informacji publicznej w świetle obowiązywania RODO.

Szkolenie kierowane jest do przedstawicieli podmiotów, którzy podlegają Ustawie o dostępie do Informacji Publicznej. Zgodnie z nowymi uwarunkowaniami prawnymi wnoszonymi przez Rozporządzenie Ochrony Danych Osobowych zmienia się podejście do udzielanych informacji w trybie informacji publicznej. Niejasności i liczne przypadki nadinterpretacji przepisów mogą narazić na naruszenia podstawowych praw człowieka jakim jest ochrona jego danych osobowych. Uczestnicy tego kierunkowego szkolenia powinni poznać właściwą ścieżkę postępowania w kwestii udzielania informacji publicznej.

4.5 Zasady prowadzenia audytu wewnętrznego zgodnego z KRI i RODO w oparciu o system zarządzania bezpieczeństwem informacji (ISO 27001)

Szkolenie kierowane jest do przedstawicieli JST zwłaszcza etatowych komórek kontroli wewnętrznej, Inspektorów Ochrony Danych Osobowych, Administratorów Bezpieczeństwa Informacji. W części wstępnej szkolonym zostanie przybliżone otoczenie prawne ładu informatycznego stanowiącego podstawę Krajowych Ram Interoperacyjności. Tematyka główna szkolenia obejmie wskazanie metodyki prowadzenia audytów wewnętrznych z elementami warsztatowymi. Zajęcia kończą się uzyskaniem przez uczestników zaświadczeń o ukończeniu szkolenia.

5. ZODO – autorska aplikacja do zarządzania procesem ochrony danych osobowych pozwalająca m.in. na:

Zarządzanie dostępami pracowników do poszczególnych aktywów.

Porządkuję i ułatwia zarządzanie dostępem użytkowników do poszczególnych aktywów organizacji. Formalny i udokumentowany proces nadawania lub odbierania praw dostępu do aktywów przez okres współpracy.

Dokumentacja związana z procesem przetwarzania danych osobowych.

Usprawnia, w stosunku do tradycyjnej formy, w dużym stopniu proces zarządzania, aktualizacją i wdrażaniem zmian w obowiązujących politykach i zasadach oraz ich publikację dla szerszego grona użytkowników. Proces szkolenia w oparciu o aktualne wersje obowiązujących zasad w organizacji.

Ewidencje i rejestry.

Generowanie wymaganych ewidencji: upoważnień, aktywów, zbiorów, obszarów przetwarzania, udostępnień, umów powierzenia, czynności i kategorii przetwarzania danych i innych.

Analiza ryzyka.

Dla zidentyfikowanych aktywów sporządzana i utrzymywana jest ewidencja, dzięki której w łatwy i co ważne powtarzalny sposób można poddawać je cyklicznej analizie ryzyka.

Zdarzenia i incydenty

System zapewnia zgłaszanie, rejestrację, dokumentowanie podejmowanych działań eliminujących zdarzenia lub incydenty, dane wejściowe np.: do analizy ryzyka.

Audyt wewnętrzny (sprawdzenie)

Moduł ten został przygotowany, aby wesprzeć staranne planowanie i uzgodnienie aktualnych wymagań audytu oraz działania obejmujące weryfikację zgodności przetwarzanych zbiorów.

Szkolenia i ocena poziomu wiedzy

Istotnym jest, aby dopuścić do przetwarzania danych osoby, które są to tego odpowiednio przygotowane (szkolenie, upoważnienie, oświadczenie).

Klienci decydujący się na wdrożenie otrzymują terminową licencję na aplikację – gratis!

Kontakt:

zeto.lublin.pl
rodo@zeto.lublin.pl

81 718 42 00
Diamentowa 2, 20-447 Lublin