



OFERTA

**Usług audytowych i doradczych
w zakresie
ochrony danych osobowych**

dla

jednostek administracji publicznej

1. Cel i zakres dokumentu

Projekt

Zgodnie z wymaganiami prawnymi oraz dobrymi praktykami w zakresie ochrony informacji, ochrona danych osobowych wymaga budowy systemu bezpieczeństwa informacji.

Celem proponowanych usług jest zapewnienie zgodności z obecnymi wymaganiami prawnymi oraz przygotowanie i płynne przeprowadzenie podmiotu przez okres zmian prawnych w zakresie ochrony danych osobowych wynikających z wejścia w życie od 25 maja 2018 Rozporządzenia Parlamentu Europejskiego 2016/679 w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych.

Obecnie obowiązującymi aktami prawnymi w zakresie ochrony danych osobowych są między innymi ustawa z dnia 29 sierpnia 1997 roku o ochronie danych osobowych oraz rozporządzenie Ministra Spraw Wewnętrznych i Administracji z dnia 29 kwietnia 2004 roku w sprawie dokumentacji przetwarzania danych osobowych oraz warunków technicznych i organizacyjnych, jakim powinny odpowiadać urządzenia i systemy informatyczne służące do przetwarzania danych osobowych.

Powyższe regulacje prawne w obecnym kształcie utracą moc w dniu 25 maja 2018 roku.

Zgodnie z szacunkami Ministerstwa Cyfryzacji które wprowadza RODO na grunt Polski zmianom ulegnie ponad 130 ustaw, co spowoduje konieczność ponownych analiz poprawności przetwarzania danych w przedsiębiorstwach i podmiotach publicznych.

Naszym celem będzie pomoc Państwu w okresie zmian prawnych i po ich wprowadzeniu a przede wszystkim zapewnienie bezpieczeństwa w prowadzeniu działalności oświatowej a aspekcie wymagań RODO i prawdopodobnych zmian w ustawie o oświacie.

Klient

Gmina/Miasto/Starostwo/samorządowe organizacyjne

jednostki

Osoba odpowiedzialna

Dostawcy usługi

TBD MAZOWSZE Sp. z o.o.

ul. Aślanowicza 18

08-110 SIEDLCE

NIP 8212264268 REGON 712363817 KRS 0000053292

Sąd Rejonowy dla m.st. Warszawy XIV Wydział Gospodarczy KRS

Wysokość kapitału zakładowego 90 000 zł

Audytel S.A.

ks. I. Skorupki 5, 00-546 Warszawa

NIP 779-21-69-697 REGON 634288697 KRS 0000309391

Sąd Rejonowy dla m.st. Warszawy XII Wydział Gospodarczy KRS

Wysokość kapitału zakładowego 500 112 zł (w całości opłacony)

Osoba odpowiedzialna

Stefan Książek

Telefon: (25) 631 14 00, 509 817 817

e-mail: stefan.ksiazek@tbdsiedlce.pl

Data

28 lipca 2017 r.

2. Opis usługi

Usługi doradcze
związane z
wdrożeniem
systemu ochrony
danych osobowych

W ramach usług doradczych podczas wdrażania systemu ochrony danych osobowych proponujemy następujący schemat pracy:

1. Przegląd zbiorów danych osobowych oraz systemów służących do ich przetwarzania

Przegląd zbiorów polega na zidentyfikowaniu wszystkich zbiorów danych osobowych występujących w urzędzie oraz analizie podstaw prawnych przetwarzania. Audytorzy oceniają spełnienie przez Klienta obowiązków (m.in.: informacyjnego, rejestracyjnego) nałożonych na niego przez prawo. Aplikacje i systemy informatyczne służące do przetwarzania danych osobowych podlegają ocenie pod kątem zgodności z wymaganiami prawnymi.

2. Szacowanie ryzyka dla danych osobowych

Metodyka analizy ryzyka jest oparta na normie PN-ISO/IEC 27005. Wybór tej normy wynika z wymagań Rozporządzenia o Krajowych Ramach Interoperacyjności (Rozdział IV, § 20. 1 ust. 3).

- 1) Określenie rejestru aktywów (listy składników aktywów informacyjnych – np. procesy, infrastruktura, systemy, zbiory danych, budynki, usługi zewnętrzne),
- 2) Określenie katalogu zagrożeń, które mogą wystąpić dla poszczególnych składników aktywów,
- 3) Przybliżona ocena wpływu danego zagrożenia na dany składnik aktywów,
- 4) Przybliżona ocena prawdopodobieństwa wystąpienia danego zagrożenia,
- 5) Ustalenie indeksu ryzyka jako wypadkowej wpływu i prawdopodobieństwa (punkty 3 i 4),
- 6) Rekomendacje co do zastosowania zabezpieczeń zmniejszających poziom ryzyka
- 7) Przedstawienie ryzyk szacunkowych do akceptacji przez Kierownictwo,

3. Wsparcie przy opracowaniu lub aktualizacji dokumentacji

Realizacja prac wdrożeniowych polega na:

- 1) opracowaniu Polityki Bezpieczeństwa Danych Osobowych,
- 2) opracowaniu Instrukcji zarządzania systemem informatycznym służącym do przetwarzania danych osobowych,
- 3) opracowaniu instrukcji postępowania w przypadku naruszenia ochrony danych osobowych,

- 4) opracowaniu (w oparciu o informacje przekazane przez Klienta) wymaganych przepisami prawa:
 - a) wykazu zbiorów danych osobowych oraz systemów służących do ich przetwarzania,
 - b) opisu struktury zbiorów danych osobowych,
 - c) wykazu pomieszczeń przetwarzania danych osobowych,
 - d) opisu przepływu danych między systemami,
- 5) opracowaniu ewidencji osób upoważnionych do przetwarzania danych osobowych oraz przygotowaniu upoważnień do przetwarzania danych osobowych dla pracowników.

3. Rejestracja zbiorów w rejestrze GIODO

Przygotowanie wniosków zgłoszeniowych i wniosków aktualizacyjnych do rejestru Generalnego Inspektora Ochrony Danych Osobowych lub do rejestru prowadzonego przez ABI dla zbiorów danych osobowych objętych obowiązkiem rejestracyjnym oraz reprezentowanie klienta w kontaktach z Departamentem Rejestracji Biura Generalnego Inspektora Ochrony Danych Osobowych.

4. Szkolenie pracowników

Szkolenia dla pracowników przetwarzających danych osobowych odbędą się w siedzibie Klienta w trakcie 1-2 sesji szkoleniowych. Tematyka szkolenie obejmuje podstawową wiedzę w zakresie danych osobowych, omówienie uwarunkowań prawnych oraz wskazanie obowiązków pracowników wynikających z przyjmowanej Polityki bezpieczeństwa danych osobowych.

Outsourcing funkcji Administradora Bezpieczeństwa Informacji

Usługa polega na przejęciu obowiązków ABI, jest to m.in.:

- 1) sprawowanie nadzoru nad przestrzeganiem obowiązujących zasad bezpieczeństwa przetwarzania danych osobowych,
- 2) prowadzenie dokumentacji systemu ochrony danych osobowych (modyfikacje, aktualizacje, uzupełnienia),
- 3) koordynacja procesów związanych z funkcjonowaniem systemu bezpieczeństwa przetwarzania danych osobowych,
- 4) przeprowadzanie czynności przewidzianych dla ABI w procedurach zgodnie z Polityką Bezpieczeństwa i Instrukcją Zarządzania Systemem Informatycznym,
- 5) wydawanie zaleceń dotyczących zabezpieczania danych,
- 6) sprawowanie nadzoru nad administrowaniem uprawnieniami do przetwarzania danych osobowych, stosowaniem procedury

- przetwarzania zbiorów danych oraz przechowywaniem i aktualizacją dokumentacji ochrony danych osobowych,
- 7) nadzór nad wykonywaniem nakazów zawartych w decyzjach GIODO kierowanych do Zamawiającego,
 - 8) reprezentowanie Zamawiającego jako administratora danych osobowych, również przed GIODO, w zakresie spraw bezpośrednio związanych z ochroną danych osobowych,
 - 9) wsparcie przy opracowywaniu klauzul, na podstawie których realizowany jest obowiązek informacyjny oraz zbierana jest zgoda na przetwarzanie danych osobowych,
 - 10) opiniowanie umów Zamawiającego związanych z dostępem do danych osobowych, w tym umów o powierzeniu przetwarzania danych osobowych,
 - 11) opiniowanie wniosków o udostępnienie danych osobowych,
 - 12) koordynacja działań i współpraca z właściwymi komórkami organizacyjnymi Zamawiającego w sytuacjach podejrzenia naruszeniu bezpieczeństwa przetwarzania danych osobowych,
 - 13) kontrola bezpieczeństwa danych oraz przestrzegania procedur, zgodnie z zatwierdzonym przez Zamawiającego planem kontroli,
 - 14) przeprowadzanie rocznych przeglądów bezpieczeństwa oraz corocznych szkoleń dla pracowników,
 - 15) szkolenie nowo zatrudnionych pracowników za pośrednictwem internetowego narzędzia szkoleniowego oraz doszkolenie przy najbliższej wizycie kontrolnej,
 - 16) prowadzenie dodatkowych szkoleń pracowników Zamawiającego w przypadku istotnych zmian przepisów z zakresu ochrony danych osobowych,
 - 17) opracowywanie planu audytu i przekazywanie go do akceptacji Zamawiającego,
 - 18) sporządzanie sprawozdań dla Zamawiającego, będącego Administratorem Danych,
 - 19) przeprowadzanie kontroli na zlecenie GIODO,
 - 20) prowadzenie rejestru zbiorów danych osobowych, za wyjątkiem zbiorów danych wrażliwych,
 - 21) przygotowywanie wniosków zgłoszeniowych i wniosków aktualizacyjnych zbiorów danych wrażliwych do rejestru GIODO.

Umowa na usługę outsourcingu funkcji Administratora Bezpieczeństwa Informacji zawierana jest na okres minimum 1 roku.

Z dniem 25 maja 2018 r. gwarantujemy przejęcie przez Administratora Bezpieczeństwa Informacji funkcji Inspektora Ochrony Danych, wykonującego zadania zgodnie z art. 39 RODO

3. Warunki handlowe

Ceny

Uzależnione od specyfiki Klienta oraz indywidualnych ustaleń
