Formularz ofertowy/wstępnego audytu

Poniższe zapytanie ofertowe służy wstępnemu rozpoznaniu Państwa działalności. Informacje w nim zawarte traktowane są jako poufne (vide zastrzeżenie poufności na końcu dokumentu) i wykorzystane zostaną przez make-SOFT Marcin Kazimierczak tylko i wyłącznie w celu do tego przeznaczonym, czyli przygotowania oferty oraz podczas ewentualnego procesu audytu i wdrożenia. Sporządzenie oferty na podstawie niniejszego zapytania jest bezpłatne i nie zobowiązuje Państwa do skorzystania z naszych usług.

Prosimy o przesłanie wypełnionego zapytania ofertowego na adres [biuro@make-soft.pl](mailto:biuro@make-soft.pl)

1. OGÓLNE DANE PRZEDSIĘBIORCY

|  |  |
| --- | --- |
| Pełna nazwa organizacji:  Forma prawna:  Klasyfikacja PKD: | Osoba kontaktowa:  Telefon: Stacjonarny:  e-mail: |
| Ulica, kod, miasto:  Województwo: | Pełnomocnik:  Telefon: Stacjonarny:  e-mail: |
| NIP: | www: |

B. OFERTA POWINNA OBEJMOWAĆ:  
 *(prosimy o zaznaczenie odpowiednich opcji)*

|  |  |
| --- | --- |
| B.1 Audyt bezpieczeństwa informacji | |
| 1. Przedwdrożeniowy, w związku z procesem zapewnienia zgodności z RODO/GPDR, |  |
| 1. Powdrożeniowy, w związku z testem funkcjonowania wdrożonych procedur zgodności z RODO/GPDR |  |
| 1. Okresowy audyt zewnętrzny, |  |
| B.2 Testy bezpieczeństwa systemu informatycznego:  (przynajmniej jeden z testów powinien być wykonany w przypadku firm > 20 stanowisk) | |
| 1. Testy zabezpieczeń firmowych serwisów www (oraz aplikacji webowych), |  |
| 1. Testy zabezpieczeń sieci LAN/WAN, |  |
| 1. Testy zabezpieczeń sieci WIFI, |  |
| B.4 Zapewnienie zgodności działania firmy z RODO/GPDR:  (kwoty przybliżone, oszacowane według informacji zawartych w ankiecie. Szczegółowa oferta możliwa jest do przedstawienia po wykonaniu audytu przedwdrożeniowego). | |
| 1. Opracowanie oceny ryzyka oraz programu dostosowania do zgodności z RODO |  |
| 1. Opracowanie (spersonalizowanego) Systemu Zarządzania Bezpieczeństwem Informacji, określającego ochronę danych w firmie, zaprojektowanego według zasady „Privacy by Design” |  |
| 1. Outsourcing funkcji Inspektora Ochrony Danych (powdrożeniowy nadzór nad procesami ochrony danych w firmie w przypadku powołania wymaganego przez prawo) |  |
| 1. Outsourcing funkcji Specjalisty Ochrony Danych (powdrożeniowy nadzór nad procesami ochrony danych w firmie w przypadku dobrowolnego powołania + aktualizacja dokumentacji systemu zarządzania) |  |
| 1. Outsourcing funkcji Incident Response Manager (nadzór nad obsługą incydentów naruszenia ochrony danych w firmie) |  |

C. Prosimy o odpowiedzi na poniższe pytania:  
*(w razie wątpliwości prosimy o kontakt z biurem)*

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| C.1 Całkowita liczba lokalizacji: | Lokalizacja I Centrala | Lokalizacja II | Lokalizacja III | Lokalizacja IV | Suma |
| C.2 Organizacja lub nazwa / zakładu /oddziału | JW. |  |  |  |  |
| C.3 Adres (ulica, kod, miasto) |  |  |  |  |  |
| C.4 Rodzaj prowadzonej działalności (opis) |  |  |  |  |  |
| C.5 Całkowita liczba pracowników w obszarze objętym planowanymi usługami – audytem, wdrożeniem itp.  w przeliczeniu na pełne etaty, łącznie z pracownikami tymczasowymi oraz sezonowymi (podwykonawcy jeśli zostali ujęci w zakresie). |  |  |  |  |  |
| C.6 Ilość pracowników przetwarzających dane osobowe w systemach teleinformatycznych |  |  |  |  |  |

D. Ankieta systemu zarządzania

*(w razie wątpliwości prosimy o kontakt z biurem)*

|  |  |
| --- | --- |
| D.1 Polityka Bezpieczeństwa Informacji | |
| D.1.1 Czy podmiot posiada ustanowioną (i działającą) Politykę Bezpieczeństwa Informacji/Politykę Ochrony Danych Osobowych? |  |
| D.2 Organizacja bezpieczeństwa informacji | |
| D.2.1 Incydenty bezpieczeństwa | |
| D.2.1.1 Czy w podmiocie ustanowione zostały formalne procedury reagowania na incydenty związane z bezpieczeństwem informacji? |  |
| D.2.1.1 Ilość incydentów w ciągu ostatnich 6 miesięcy? |  |
| D.2.2 Zarządzanie aktywami | |
| D.2.2.1 Czy podmiot posiada zinwentaryzowane aktywa organizacji? |  |
| D.2.2.2 Czy wszystkie aktywa posiadają przypisanych właścicieli? |  |
| D.2.2.3 Czy podmiot posiada ustanowione zasady klasyfikacji informacji? |  |
| D.2.3 Bezpieczeństwo fizyczne | |
| D.2.3.1 Czy podmiot korzysta z outsourcingu usług ochrony? |  |
| D.3.3.2 Czy podmiot wykorzystuje monitoring wizyjny (CCTV)? |  |
| D.2.4 Bezpieczeństwo informatyczne | |
| D.2.4.1 Czy w podmiocie stosowana jest sieć WiFi? |  |
| D.2.4.2 Czy w podmiocie dopuszczalna jest telepraca (VPN, RDP, VNC, itp.)? Podać rodzaje. |  |
| D.2.4.3 Czy podmiot posiada ustanowione zasady zarządzania nośnikami? |  |
| D.2.4.4 Czy w podmiocie wprowadzone są zasady zarządzania dostępem użytkowników do aplikacji (nadawania, odbieranie, zmiana uprawnień, okresowy przegląd)? |  |
| D.2.4.5 Czy w podmiocie stosowane jest oprogramowanie wykrywające, zapobiegające przed szkodliwym oprogramowaniem (antywirusy, antyspam)? |  |
| D.2.4.6 Czy podmiot korzysta w outsourcingu usług IT? |  |
| D.2.4.7 Ilość osób zatrudnionych w podmiocie w obszarze IT? |  |
| D.2.4.8 Czy w podmiocie wykonywane są regularnie zapasowe kopie informacji? |  |
| D.2.4.9 Czy w podmiocie rejestrowane są działania administratorów i użytkowników? |  |
| D.2.4.10 Czy w podmiocie nałożone są ograniczenia w instalowaniu oprogramowania przez użytkowników? |  |
| D.2.4.11 Czy w podmiocie przeprowadzany był audyt systemów informatycznych? |  |
| D.2.4.12 Czy podmiot wykorzystuje technologie „cloud” (dane w chmurze) do wymiany informacji? |  |
| D.2.4.13 Czy podmiot wykorzystuje technologie backupu w chmurze BaaS? |  |
| D.2.4.14 Czy podmiot wykorzystuje usługi IaaS (Infrastrukture as a Service)? |  |
| D.2.4.15 Czy w podmiocie oprócz środowisk produkcyjnych systemów wykorzystywane są środowiska testowe? |  |
| D.2.4.16 Czy w podmiocie oprócz środowisk produkcyjnych systemów wykorzystywane są środowiska rozwojowe? |  |
| D.3 Zarządzanie i organizacja | |
| D.3.1 Zarządzanie zasobami ludzkimi | |
| D.3.1.1 Ilość osób zatrudnionych w podmiocie na etaty? |  |
| D.3.1.2 Ilość osób zatrudnionych B2B (pracownicy z własną działalnością)? |  |
| D.3.1.3 Ilość osób zatrudnionych na podstawie umowy o dzieło? |  |
| D.3.1.4 Czy podmiot zatrudnia obcokrajowców (pracownicy spoza EU)? |  |
| D.3.1.5 Czy podmiot w związku z przetwarza dane szczególne (pochodzenie rasowe/etniczne, poglądy polityczne, przekonania religijne, światopoglądowe, przynależność do związków zawodowych, dane genetyczne, dane biometryczne, dotyczące zdrowia, dotyczące seksualności, dotyczące orientacji seksualnej, dotyczące wyroków skazujących)? |  |
| D.3.1.6 Czy podmiot posiada podpisane umowy przetwarzania danych ze swoimi klientami? Podać orientacyjną ilość. |  |
| D.3.1.7 Czy podmiot korzysta z outsourcingu obsługi kadrowej? |  |
| D.3.1.8 Czy podmiot korzysta z outsourcingu usług rekrutacji? |  |
| D.3.1.9 Czy dane osobowe przetwarzane są u usługodawcy, czy tylko w siedzibie firmy (obsługa na miejscu)? |  |
| D.3.1.10 Czy podmiot korzysta z programów sprzedażowych, finansowo-księgowych, kadrowych, ERP, CRM zainstalowanych lokalnie? Wymienić lub opisać jakie. |  |
| D.3.2 Bezpieczeństwo i higiena pracy | |
| D.3.2.1 Czy podmiot korzysta z outsourcingu obsługi zagadnień BHP? |  |
| D.3.2.2 Czy dane osobowe przetwarzane są u usługodawcy, czy tylko w siedzibie firmy(obsługa na miejscu)? |  |
| D.3.3 Obsługa prawna | |
| D.3.3.1 Czy podmiot korzysta z outsourcingu obsługi prawnej? |  |
| D.3.3.2 Czy dane osobowe przetwarzane są u usługodawcy, czy tylko w siedzibie firmy(obsługa na miejscu)? |  |
| D.3.4 Dochodzenie należności | |
| D.3.4.1 Czy podmiot korzysta z outsourcingu działań windykacyjnych? |  |
| D.3.5 Marketing usług | |
| D.3.5.1 Czy podmiot korzysta z hostingu zewnętrznego poczty email? Podać nazwę podmiotu. |  |
| D.3.5.2 Czy podmiot korzysta z hostingu zewnętrznego stron WWW? Podać nazwę podmiotu. |  |
| D.3.5.3 Czy ze strony www wysyłany jest newsletter? Podać ilość serwisów www, w których jest newsletter. |  |
| D.3.5.4 Czy podmiot korzysta z usług outsourcingu podczas wysyłki newslettera? |  |
| D.3.5.5 Czy na stronie jest formularz kontaktu? Podać ilość serwisów www, w których jest formularz kontaktu. |  |
| D.3.5.6 Czy w podmiocie stosowane jest rozwiązane CRM? |  |
| D.3.5.7 Czy w podmiocie stosowane jest rozwiązane Email Marketing Automation? |  |
| D.3.5.8 Czy w podmiocie dane osobowe przetwarzane są w celu marketingu produktów lub usług innych podmiotów? |  |
| D.3.5.9 Czy podmiot pozyskuje/pozyskiwał dane kontrahentów od innych podmiotów? |  |
| D.4 Świadczenie usług | |
| D.4.1 Czy podmiot świadczy usługi drogą elektroniczną (e-sklep, portal internetowy)? |  |
| D.4.2 Czy usługa sprzężona jest z innymi usługami (interfejsy wymiany danych, importu/eksportu itp.) |  |
| D.4.3 Czy podmiot realizuje obsługę reklamacji produktów/usług? |  |
| D.4.4 Czy usługi są świadczone dla osób prywatnych (B2C)? |  |
| D.4.5 Czy usługi są świadczone dla firm (B2B)? |  |
| D.4.6 Czy następuje profilowanie danych (segmentacja tj. ze względu na podane przez użytkownika dane dokonuje się personalizacji oferty)? |  |

E. Ankieta obszaru IT   
*(tylko stanowiska na których przetwarzane są dane osobowe)*

|  |  |
| --- | --- |
|  | |
| E.1 Komputery stacjonarne  E.1.1 Ilość: E.1.2 Systemy operacyjne (ilości): E.1.2.1 Win10 …..  E.1.2.2 Win 8 …..  E.1.2.3 Win 7 …..  E.1.2.4 Win starsze ….  E.1.2.5 Linux ….  E.1.2.6 osx…. | E.2 Komputery przenośne  E.2.1 Ilość: E.2.2 Systemy operacyjne (ilości): E.2.2.1 Win10 …..  E.2.2.2 Win 8 …..  E.2.2.3 Win 7 …..  E.2.2.4 Win starsze ….  E.2.2.5 Linux ….  E.2.2.6 osx….  E.2.3 Czy do przetwarzania dopuszczone są komputery prywatne pracowników (na zasadzie Bring Your Own Device)? |
| E.3 Serwery lokalne  E.3.1 Czy występują Serwery lokalne: (tak/nie)  jeśli tak: E.3.2 Systemy operacyjne: E.3.2.1 Windows (wpisz ilość oraz typ)………………………………………… E.3.2.2 Linux (wpisz ilość oraz typ)………………………………………………. E.3.2.3 Inne (np. nas, san, wirtualizacja itp.) …………………………………………………………….  E.3.3 Wirtualizacja (typ, ilość hostów)  ......................................................................  E.3.4 Uwierzytelnienie użytkowników w sieci? (domena Active Directory/konta lokalne)  E.3.5 Wydzielony serwer bazy danych? (TAK/NIE)  E.3.6 Sposób archiwizacji danych? (brak/serwer NAS/nośnik zewnętrzny/chmura/inne)  E.3.7 Orientacyjny wiek sprzętu serwerowego:  < 2lata …. od 2 do 5lat …. >7Lat i więcej …..  E.3.8 Czy zabezpieczone zasilanie awaryjne UPS? …. | E.4 Sprzęt sieciowy  E.4.1 Router brzegowy (model)………………………………. E.4.2 Switche (model, ilość)……………………………………..  E.4.3 Drukarki sieciowe (ilość) ……………………………………………… E.4.4 Dyski sieciowe NAS (ilość) ……………………………………………. E.4.5 pozostałe urządzenia sieciowe: ...................................................................... E.4.6 Zaawansowane urządzenia bezpieczeństwa(jakie)? (UTM/IPS/PROXY/brak) |
|  |

F. Uwagi

|  |
| --- |
|  |

ZASTRZEŻENIE POUFNOŚCI

Na podstawie art. 721 Kodeksu cywilnego zastrzegam poufność wszelkich informacji udostępnionych podmiotowi „make-SOFT Marcin Kazimierczak” z siedzibą w Gorzowie Wlkp. podczas negocjacji w celu przygotowania oferty.

Jednocześnie oświadczam, że make-SOFT Marcin Kazimierczak ma prawo do ujawnienia informacji poufnych podmiotom, którym ujawnienie informacji jest niezbędne dla przygotowania oferty, w szczególności powiązanych osobowo lub kapitałowo, jak również pracownikom, a także osobom świadczącym na jego rzecz usługi na podstawie stosunku cywilnoprawnego.

Podpis osoby upoważnionej: …………………………………………..

Data i miejsce: ……………………………………………………………….

Dziękujemy za zainteresowanie naszą ofertą!