*Załącznik nr 1 do umowy powierzenia przetwarzania danych osobowych*

ANKIETA BEZPIECZEŃSTWA DANYCH OSOBOWYCH

do umowy powierzenia danych osobowych nr:………………. z dnia:…………………….

*Poniższa ankieta ma na celu ustalenie czy podmiot zewnętrzny zapewnia wystarczające gwarancje wdrożenia odpowiednich środków technicznych i organizacyjnych, by przetwarzanie odbywało się zgodnie z RODO i chroniło prawa osób, których dane dotyczą. W tym celu należy odpowiedzieć na poniższe pytania.*

|  |  |
| --- | --- |
| **Podmiot przetwarzający:** |  |
| **Imię i Nazwisko osoby wypełniającej** |  |
| **Stanowisko** |  |
| **Adres e-mail i nr telefonu** |  |

|  |  |  |  |
| --- | --- | --- | --- |
| **L.p.** | **Pytanie** | **Odpowiedź** | **Uwagi/Wyjaśnienia** |
| **TAK** | **NIE** | **NIE DOTYCZY** |
|  | Proszę podać ilość lokalizacji i kraje, w których będą przetwarzane powierzone dane osobowe? |  |  |  |  |
|  | Czy powierzone dane osobowe będą przekazywane poza EOG? Np. ze względu na lokalizację systemu IT, będą przetwarzane przez osoby zlokalizowane poza EOG lub osoby te będą miały możliwość dostępu do tych danych? |  |  |  |  |
|  | Jeśli tak to w jakim kraju? |  |  |  |  |
|  | Czy w Państwa organizacji przeprowadzane są okresowe audyty zgodności z przepisami ochrony danych osobowych? |  |  |  |  |
|  | Czy Państwa organizacja posiada doświadczenie w świadczeniu usług polegających na zarządzaniu zbiorami danych osobowych w imieniu innego podmiotu (pełnił rolę podmiotu przetwarzającego)? |  |  |  |  |
|  | Czy Państwa organizacja wyznaczyła w strukturach wewnętrznych Inspektora Ochrony Danych lub osobę/komórkę odpowiedzialną za nadzór nad ochroną danych osobowych? Czy Państwa organizacja jest zobowiązana do wyznaczenie IODO ? |  |  |  |  |
|  | Czy w Państwa organizacji została opracowana i wdrożona metodyka oraz procedury zarządzania ryzykiem związanym z bezpieczeństwem informacji? |  |  |  |  |
|  | Czy Państwa organizacja prowadzi rejestr czynności przetwarzania spełniający wymogi przepisu art. 30 ust. 1 RODO? |  |  |  |  |
|  | Czy Państwa organizacja prowadzi rejestr kategorii czynności przetwarzania spełniający wymogi przepisu art. 30 ust. 2 RODO? |  |  |  |  |
|  | Czy Państwa organizacja przeprowadza regularne (co najmniej raz w roku) testowanie, mierzenie i ocenianie skuteczności środków technicznych i organizacyjnych mających zapewnić bezpieczeństwo przetwarzania? |  |  |  |  |
|  | Czy Państwa organizacja gwarantuje realizację praw osób, których dane dotyczą, określonych w art. 15-22 RODO? W jaki sposób ? |  |  |  |  |
|  | Czy Państwa organizacja zapewnia, aby każdy nowozatrudniony pracownik przed rozpoczęciem czynności związanych z przetwarzaniem danych osobowych został odpowiednio przeszkolony w tym zakresie i zapoznany z powszechnie obowiązującymi przepisami o ochronie danych osobowych, także z wewnętrznymi obowiązującymi w Państwa organizacji ? |  |  |  |  |
|  | Czy Państwa organizacja prowadzi cykliczne szkolenia doskonalące dla swojego personelu lub podejmuje inne działania mające na celu podnoszenie świadomości pracowników i uaktualnianie wiedzy z zakresu ochrony danych osobowych? Z jaką częstotliwością przeprowadzane są okresowe szkolenia ? |  |  |  |  |
|  | Czy osoby wykonujące operacje na danych osobowych otrzymały stosowne upoważnienia do przetwarzania danych, spełniające wymogi przepisu art. 29 RODO? |  |  |  |  |
|  | Czy Państwa organizacja wdrożyła i stosuje sformalizowane procedury nadawania uprawnień do systemów informatycznych w ramach których przetwarzane są dane osobowe? |  |  |  |  |
|  | Czy Państwa organizacja prowadzi cykliczne przeglądy nadanych uprawnień? |  |  |  |  |
|  | Czy Państwa organizacja stosuje środki kontroli dostępu fizycznego do budynku/budynków ograniczające dostęp tylko dla autoryzowanego personelu? |  |  |  |  |
|  | Czy Państwa organizacja posiada odpowiednio wyposażone i zabezpieczone pomieszczenia umożliwiające bezpieczne przetwarzanie danych osobowych? |  |  |  |  |
|  | Czy każdy pracownik otrzymuje unikalny identyfikator do systemów informatycznych? |  |  |  |  |
|  | Czy w systemach informatycznych Państwa organizacji zapewniono wymuszanie na użytkownikach stosowania haseł o odpowiedniej sile (kombinacja liter, cyfr i znaków specjalnych, min. 8 znakowe), także ich okresowej zmiany oraz zmian w razie zaistniałej potrzeby? |  |  |  |  |
|  | Czy Państwa organizacja wdrożyła i stosuje w organizacji zasadę „czystego ekranu” polegającą na automatycznym wygaszaniu ekranu i blokowaniu systemu, po okresie bezczynności, gdzie powrót do normalnej pracy wymaga podania hasła? |  |  |  |  |
|  | Czy Państwa organizacja wdrożyła i stosuje w organizacji zasadę „czystego biurka” polegającą na obowiązku chowania dokumentów zawierających dane osobowe do zamykanych szaf na koniec dnia pracy? |  |  |  |  |
|  | Czy w systemach informatycznych Państwa organizacji są wdrożone zabezpieczenia wykrywające lub zapobiegające użyciu nieautoryzowanego oprogramowania? |  |  |  |  |
|  | Czy urządzenia mobilne (laptopy, tablety, telefony komórkowe, itp.) wykorzystywane do przetwarzania danych osobowych, którymi Państwa organizacja dysponuje, są szyfrowane? |  |  |  |  |
|  | Czy Państwa organizacja posiada wdrożone procedury bezpiecznego zbywania sprzętu, uwzględniające całkowite usuwanie danych z nośników informacji? |  |  |  |  |
|  | Czy Państwa organizacja posiada wdrożony i sformalizowany proces zarządzania incydentami związanymi z bezpieczeństwem informacji? |  |  |  |  |
|  | Czy Państwa organizacja posiada wdrożony i sformalizowany proces zarządzania ciągłością działania? |  |  |  |  |
|  | Czy korzystają Państwo z usług podwykonawców i podpowierzają lub planują podpowierzyć im przetwarzanie danych przekazanych przez administratora danych? |  |  |  |  |
|  | Jeśli tak, to czy z podwykonawcami zawarto pisemne umowy powierzenia danych odpowiadające wymogom określonym w art. 28 RODO? |  |  |  |  |
|  | Czy w związku z podpisaniem umów powierzenia ww. Państwa organizacja weryfikuje podwykonawców ? |  |  |  |  |
|  | W jaki sposób Państwa organizacja weryfikuje ww. podmioty ? |  |  |  |  |
|  | Czy Państwo wyrażają zgodę na ewentualną weryfikację w siedzibie Państwa, opisanych powyżej zasad ochrony danych osobowych? |  |  |  |  |

……………………………………………………………………………………….

 (data i podpis osoby wypełniającej)