*Załącznik B*

**ANKIETA WERYFIKACYJNA**

**DLA PODMIOTU PRZETWARZAJĄCEGO DANE OSOBOWE**

*Poniższa ankieta ma na celu weryfikację czy podmiot przetwarzający zapewnia wystarczające gwarancje stosowanie odpowiednich środków technicznych i organizacyjnych, by przetwarzanie danych osobowych odbywało się zgodnie z RODO i chroniło prawa osób, których dane dotyczą.*

**Ankieta weryfikacyjna stanowi załącznik do umowy powierzenia danych osobowych nr**:………………. **z dnia:**…………………….

**Dane podmiotu przetwarzającego**

|  |  |
| --- | --- |
| **Nazwa firmy** |  |
| **NIP** |  |
| **Adres** |  |
| **Telefon** |  |

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **L.p.** | **Pytanie** | **Odpowiedź** | | | **Uwagi** |
| **Tak** | **Nie** | **Nie dotyczy** |
| **IOD** | | | | | |
|  | Czy podmiot przetwarzający powołał inspektora ochrony danych osobowych w zgodzie z art. 37 RODO **(jeśli konieczne)** ? |  |  |  |  |
| 1. \ | Czy funkcję IOD pełni osoba której zajmowane stanowisko nie powoduje konfliktu interesów w wewnętrznej strukturze podmiotu przetwarzającego ? |  |  |  |  |
| **Dokumentacja** | | | | | |
|  | Czy polityki bezpieczeństwa danych osobowych w formie pisemnej podlegają regularnej aktualizacji ? |  |  |  |  |
|  | Czy rejestr czynności przetwarzania spełniający wymogi przepisu art. 30 ust. 1 RODO podlega regularnej aktualizacji ? |  |  |  |  |
|  | Czy rejestr kategorii czynności przetwarzania spełniający wymogi przepisu art. 30 ust. 2 RODO podlega regularnej aktualizacji ? |  |  |  |  |
|  | Czy procedura zgłaszania naruszeń do organu nadzorczego jest aktualna oraz sformułowana w zgodzie i w oparciu o art. 33 i 34 RODO ? |  |  |  |  |
|  | Czy rejestr naruszeń ochrony danych o którym mówi art. 33 RODO podlega regularnej aktualizacji ? |  |  |  |  |
|  | Czy podmiot przetwarzający gwarantuje realizacje praw osób których dane dotyczą określonych w artykule 15 – 22 RODO? |  |  |  |  |
|  | Czy w podmiocie przetwarzającym zewidencjonowano wykaz budynków i pomieszczeń stanowiących obszar przetwarzania danychosobowych ? |  |  |  |  |
|  | Czy w podmiocie przeprowadzana jest ocena skutków dla ochrony danych o których mówi art. 35 RODO osobowych w stosownych przypadkach i czy jest udokumentowana **(jeśli konieczne)** ? |  |  |  |  |
|  | Czy dokumentacja związana z zarządzaniem systemami informatycznymi podlega regularnej aktualizacji ? |  |  |  |  |
|  | Czy podmiot przetwarzający prowadzi cykliczny przegląd nadanych uprawnień do przetwarzania danych osobowych ? |  |  |  |  |
| **Środki technicznej oraz organizacyjnej ochrony pomieszczeń** | | | | | |
|  | Czy budynki, części budynków oraz pomieszczenia w których przechowywane są dane osobowe są zabezpieczone w sposób fizyczny uniemożliwiający dostęp dla osób nieupoważnionych ? |  |  |  |  |
|  | Czy jeżeli podmiot przetwarzający posiada system alarmowy, system monitoringu przemysłowego obejmujący miejsca gdzie znajdują się dane osobowe jest on sprawny i podlega regularnym przeglądom ? |  |  |  |  |
| 1. C | Czy podmiot przetwarzający zapewnia odpowiedni nadzór nad osobami niebędącymi jego pracownikami, a przebywającymi w jego siedzibie oraz mającymi dostęp do pomieszczeń w których przetwarzane są dane osobowe po godzinach pracy ? |  |  |  |  |
|  | Czy podmiot przetwarzający zapewnia organizacyjną kontrolę dostępu do pomieszczeń w których przetwarzane są dane osobowe wyłącznie dla osób upoważnionych ? |  |  |  |  |
| **Systemy teleinformatyczne** | | | | | |
|  | Czy podmiot przetwarzający zapewnia aby serwery, na których przechowywane są bazy danych są zabezpieczone w sposób uniemożliwiający dostęp dla osób nieupoważnionych ? |  |  |  |  |
|  | Czy podmiot przetwarzający posiada wdrożone procedury bezpiecznego zbywania sprzętu uwzględniające całkowite usuwanie danych z dysków twardych, nośników ? |  |  |  |  |
|  | Czy podmiot przetwarzający ewidencjonuje urządzenia systemu informatycznego (sprzęt komputerowy oraz urządzenia mobilne) służące do przetwarzania danych osobowych ? |  |  |  |  |
|  | Czy wszystkie urządzenia systemu informatycznego podmiotu przetwarzającego są zabezpieczone aktualnymi systemami antywirusowymi ? |  |  |  |  |
|  | Czy podmiot przetwarzający prowadzi monitorowanie nieudanych prób zalogowania się do systemu oraz blokowanie konta po określonej nieudanej ilości prób zalogowania ? |  |  |  |  |
|  | Czy pracownicy podmiotu przetwarzającego posiadają indywidualne konta dostępowe do systemu informatycznego ? |  |  |  |  |
|  | Czy podmiot przetwarzający wprowadził i stosuje mechanizm regularnych kopii zapasowych ? |  |  |  |  |
|  | Czy podmiot przetwarzający zapewnia okresowe testowanie mechanizmu tworzenia kopii zapasowych ? |  |  |  |  |
|  | Czy podmiot przetwarzający stosuje techniczne środki szyfrowania danych osobowych pozwalające na zachowanie ich poufności ? |  |  |  |  |
|  | Czy w systemach informatycznych podmiotu przetwarzającego zapewniono wymuszenie na użytkownikach stosowania haseł o odpowiedniej sile oraz częstotliwość ich zmiany ? |  |  |  |  |
|  | Czy podmiot przetwarzający stosuje wygaszacze ekranu, blokadę systemu po okresie bezczynności, gdzie powrót do normalnej pracy wymaga podania hasła ? |  |  |  |  |
|  | Czy podmiot przetwarzający wdrożył i stosuje zasadę czystego ekranu oraz zasadę czystego biurka ? |  |  |  |  |
| **Szkolenia** | | | | | |
|  | Czy podmiot przetwarzający w ostatnim roku kalendarzowym przeprowadził szkolenia dla swojego personelu z zakresu ochrony danych osobowych ? |  |  |  |  |
|  | Czy wszyscy nowi pracownicy podmiotu przetwarzającego zostali przeszkoleni z zakresu zasad ochrony danych osobowych ? |  |  |  |  |
| **Kontrola i weryfikacja** | | | | | |
|  | Czy podmiot przetwarzający w ostatnim roku kalendarzowym przeprowadził audyty zgodności z przepisami ochrony danych osobowych? |  |  |  |  |
|  | Czy podmiot przetwarzający testował w ostatnim roku kalendarzowym środki ochrony technicznej oraz organizacyjnej ? |  |  |  |  |
| **Podpowierzenie** | | | | | |
|  | Czy podmioty którym podmiot przetwarzający podpowierza dane osobowe zostały zweryfikowane pod kątem spełniania wymogów RODO? |  |  |  |  |

………………………………………………………………………………. (data i pieczęć firmy)