**Ankieta dla podmiotu przetwarzającego ……………………………………………………………………………………………………………….**

*Nazwa wykonawcy*

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Lp.** | **Pytanie** | **Odpowiedź** | **Poziom zgodności**  *(wypełnia Zamawiający)* | **Uwagi (dodatkowe informacje)** |
| 1. | Czy podmiot posiada doświadczenie w świadczeniu usług związanych z powierzeniem przetwarzania danych? | TAK  NIE | Zgodność  Częściowa zgodność  Niezgodność |  |
| 2. | Czy podmiot świadczył już, podobne usługi jak zamówieniu? | TAK  NIE | Zgodność  Częściowa zgodność  Niezgodność |  |
| 3. | O jak dawna podmiot służy usługi związane z powierzeniem danych osobowych do przetwarzania? |  | Zgodność  Częściowa zgodność  Niezgodność |  |
| 4. | Czy podmiot posiada opracowaną i zatwierdzoną politykę ochrony danych osobowych? | TAK  NIE | Zgodność  Częściowa zgodność  Niezgodność |  |
| 5. | Czy wdrożona polityka bezpieczeństwa została opracowana w zgodności z normami ISO 27001/27002? | TAK  NIE | Zgodność  Częściowa zgodność  Niezgodność |  |
| 6. | Czy podmiot prowadzi regularnie audyty dotyczące zasad bezpieczeństwa informacji, w tym danych osobowych, w celu weryfikacji spełniania wymogów polityki ochrony danych lub innej wewnętrznej procedury, w tym ocena skuteczności środków technicznych i organizacyjnych mających zapewnić bezpieczeństwo przetwarzania? | TAK  NIE | Zgodność  Częściowa zgodność  Niezgodność |  |
| 7. | Czy w ciągu dwóch ostatnich lat podmiot poddawał zewnętrznej kontroli niezależnych audytorów funkcjonujący w jego organizacji system ochrony danych osobowych? | TAK  NIE | Zgodność  Częściowa zgodność  Niezgodność |  |
| 8. | Czy audyt uzyskał ocenę pozytywną? | TAK  NIE | Zgodność  Częściowa zgodność  Niezgodność |  |
| 9. | Czy w ciągu dwóch ostatnich lat w podmiocie został wykonywał test penetracyjny? | TAK  NIE | Zgodność  Częściowa zgodność  Niezgodność |  |
| 10. | Czy podmiot jest przygotowany do poddania się audytowi przeprowadzonemu przez administratora danych lub audytora upoważnionego przez administratora danych? | TAK  NIE | Zgodność  Częściowa zgodność  Niezgodność |  |
| 11. | Czy podmiot powołał inspektora ochrony danych?  Jeśli tak, to proszę podać dane kontaktowe inspektora ochrony danych. | TAK  NIE | Zgodność  Częściowa zgodność  Niezgodność |  |
| 12. | Czy podmiot posiada procedury odtwarzania systemu po awarii oraz procedury ich testowania, oraz stosuje je w praktyce? | TAK  NIE | Zgodność  Częściowa zgodność  Niezgodność |  |
| 13. | Czy podmiot zapewnia szybkie przywrócenie dostępności danych osobowych i dostępu do nich w razie incydentu? | TAK  NIE | Zgodność  Częściowa zgodność  Niezgodność |  |
| 14. | Jaki jest czas przywrócenia danych osobowych po wystąpieniu incydentu? |  | Zgodność  Częściowa zgodność  Niezgodność |  |
| 15. | Czy podmiot regularnie wykonuje kopie zapasowe i wdrożył środki efektywnego przywracania danych? | TAK  NIE | Zgodność  Częściowa zgodność  Niezgodność |  |
| 16. | Czy stosowana jest zasada 3-2-1 do tworzenia kopii zapasowych danych. | TAK  NIE | Zgodność  Częściowa zgodność  Niezgodność |  |
| 17. | Czy podmiot dokonuje transferu powierzonych danych osobowych do państw trzecich lub organizacji międzynarodowych poza obszar EOG? | TAK  NIE | Zgodność  Częściowa zgodność  Niezgodność |  |
| 18. | Czy podmiot będzie podpowierzał przekazane dane osobowe innym podmiotom przetwarzającym?  Jeśli tak, proszę załączyć wykaz podmiotów, którym dane zostaną podpowierzone. | TAK  NIE | Zgodność  Częściowa zgodność  Niezgodność |  |

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| 19. | Czy przed dalszym powierzeniem danych osobowych do przetwarzania, podmiot sprawdza te podmioty pod kątem zapewnienia odpowiedniego poziomu ochrony danych osobowych? | TAK  NIE | Zgodność  Częściowa zgodność  Niezgodność |  |
| 20. | Czy podmiot prowadzi ocenę skutków dla ochrony danych? | TAK  NIE | Zgodność  Częściowa zgodność  Niezgodność |  |
| 21. | Czy podmiot dobrał zabezpieczenia zapewniające bezpieczeństwo przetwarzanych danych osobowych w odniesieniu do oceny skutków ich przetwarzania dla praw i wolności osób, których dane dotyczą? | TAK  NIE | Zgodność  Częściowa zgodność  Niezgodność |  |
| 22. | Czy podmiot przeprowadzi analizę ryzyka w zakresie świadczenia usług, związanych z przyjęciem do przetwarzania danych osobowych? | TAK  NIE | Zgodność  Częściowa zgodność  Niezgodność |  |
| 23. | Czy podmiot wdrożył procedurę postępowania w sytuacji naruszenia bezpieczeństwa informacji stanowiących naruszenie ochrony danych osobowych? | TAK  NIE | Zgodność  Częściowa zgodność  Niezgodność |  |
| 24. | Czy podmiot wdrożył procedury umożliwiające szybki kontakt z Zespołem CSIRT. | TAK  NIE | Zgodność  Częściowa zgodność  Niezgodność |  |
| 25. | Czy w stosunku do pomiotu były zgłaszane naruszenia danych osobowych lub też, czy w ciągu ostatnich dwóch lat, podmiot sam zgłaszał naruszenia do PUODO? | TAK  NIE | Zgodność  Częściowa zgodność  Niezgodność |  |
| 26. | Czy podmiot przetwarzający gwarantuje pomoc Administratorowi w wywiązaniu się z obowiązków określonych w art. 32–36 RODO? | TAK  NIE | Zgodność  Częściowa zgodność  Niezgodność |  |
| 27. | Czy podmiot przetwarzający wdrożył i stosuje środki technicznych i organizacyjne, o których mowa w art. 24 i 32 RODO, zapewniających stopień bezpieczeństwa odpowiadający ryzyku związanemu z przetwarzaniem danych osobowych? | TAK  NIE | Zgodność  Częściowa zgodność  Niezgodność |  |
| 28. | Czy zgodnie z art. 29 RODO osoby wykonujące operacje na danych osobowych otrzymały od podmiotu przetwarzającego stosowne upoważnienia do przetwarzania danych osobowy, w tym danych osobowych powierzonych do przetwarzania? | TAK  NIE | Zgodność  Częściowa zgodność  Niezgodność |  |
| 29. | Czy pracownicy podmiotu, którzy uczestniczą w operacjach przetwarzania danych osobowych zostali zobowiązani do zachowania ich w tajemnicy? | TAK  NIE | Zgodność  Częściowa zgodność  Niezgodność |  |
| 30. | Czy podmiot ewidencjonuje dostęp do systemów informatycznych w których przetwarzane będą dane osobowe powierzone przez Zamawiającego? | TAK  NIE | Zgodność  Częściowa zgodność  Niezgodność |  |
| 31. | Czy wprowadzono politykę uniemożliwiającą uwierzytelnianie za pomocą słabego hasła? | TAK  NIE | Zgodność  Częściowa zgodność  Niezgodność |  |
| 32. | Czy podmiot prowadzi monitoring zdarzeń na styku sieć lokalna – internet i przechowuje logi z tych zdarzeń? | TAK  NIE | Zgodność  Częściowa zgodność  Niezgodność |  |
| 33. | Czy podmiot posiada zapasowe centrum przetwarzania danych? | TAK  NIE | Zgodność  Częściowa zgodność  Niezgodność |  |
| 34. | Czy w centrach przetwarzania i przechowywania danych prowadzona jest kontrola dostępu osób? | TAK  NIE | Zgodność  Częściowa zgodność  Niezgodność |  |
| 35. | Czy urządzenia na których będą przetwarzane dane osobowe Zamawiającego mają szyfrowane dyski lokalne? | TAK  NIE | Zgodność  Częściowa zgodność  Niezgodność |  |
| 36. | Czy podmiot stosuje ochronę przed działaniem szkodliwego oprogramowania? | TAK  NIE | Zgodność  Częściowa zgodność  Niezgodność |  |
| 37. | Czy podmiot zapewnia oprogramowanie antywirusowe na wszystkich stacjach komputerowych? | TAK  NIE | Zgodność  Częściowa zgodność  Niezgodność |  |
| 38. | Czy podmiot wdraża nowe rozwiązania zgodnie z zasadą „privacy by design”? | TAK  NIE | Zgodność  Częściowa zgodność  Niezgodność |  |
| 39. | Czy podmiot przetwarzający prowadzi rejestr kategorii czynności przetwarzania zawierający wszystkie informacje wskazane w art. 30 ust. 2 RODO? | TAK  NIE | Zgodność  Częściowa zgodność  Niezgodność |  |
| 40. | Czy organizacja gwarantuje realizację praw osób, których dane dotyczą tj. m.in. prawo do przenoszenia danych, prawo do ograniczenia przetwarzania, prawo do bycia zapomnianym? | TAK  NIE | Zgodność  Częściowa zgodność  Niezgodność |  |
| 41. | Czy podmiot przetwarzający wdrożył odpowiednie środki zapewniające skuteczne usunięcie powierzonych danych osobowych na polecenie Administratora? | TAK  NIE | Zgodność  Częściowa zgodność  Niezgodność |  |

Data: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ Podpis: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

**Uwagi administratora danych:**