Załącznik nr 5.2 do SWZ

IGKM.271.10.2024

**LISTA KONTROLNA (WERYFIKACYJNA) PODMIOTU PRZETWARZAJĄCEGO**

Lista kontrolna służy jako pomocne narzędzie przy przeprowadzaniu audytów, w tym inspekcji przez administratora, w ramach wykonywania swoich uprawnień określonych w art. 28 ust. 3 lit. h RODO

|  |  |  |  |
| --- | --- | --- | --- |
| **Lp.** | **OBSZAR** | **PYTANIE** | **ODPOWIEDŹ** |
| 1. | **WERYFIKACJA OGÓLNA** | Czy PP wyznaczył inspektora ochrony danych? Czy PP monitoruje obowiązek wyznaczenia IOD w organizacji? |  |
| 2. | **WERYFIKACJA OGÓLNA** | Kto wykonuje **zadania dotyczące zapewniania przestrzegania przepisów o ochronie danych osobowych w organizacji** (w sytuacji braku powołania inspektora ochrony danych)? |  |
| 3. | **WERYFIKACJA OGÓLNA** | Czy PP miał kontrolę, postępowanie wyjaśniające lub inne działania prowadzone przez Prezesa UODO lub inny organ nadzorczy w związku z PP?  **Jeśli tak, prosimy o wskazanie co było przedmiotem działań prowadzonych przez Prezesa UODO i jakie są wyniki przeprowadzonych działań?** |  |
| 4. | **WERYFIKACJA OGÓLNA** | Czy PP stosuje się do przyjętych przez organ nadzorczy kodeksów postępowania? Oczywiście o ile taki kodeks występuje w danej branży. Brak stosowania kodeksu nie wpływa samoistnie na negatywną ocenę w PP. |  |
| 5. | **WERYFIKACJA OGÓLNA** | Czy PP objęty jest monitorowaniem przestrzegania kodeksu postępowania przez akredytowany podmiot monitorujący? Oczywiście o ile taki kodeks występuje w danej branży. Brak stosowania kodeksu nie wpływa samoistnie na negatywną ocenę PP. |  |
| 6. | **WERYFIKACJA OGÓLNA** | Czy PP otrzymał **certyfikat zgodności z RODO?** Brak posiadania certyfikatu nie wpływa samoistnie na negatywną ocenę PP. |  |
| 7. | **ZASOBY/ZARZĄDZANIE PERSONELEM** | Czy osoby wyznaczone do wykonywania zadań z zakresu PP **posiadają odpowiednią wiedzę i przygotowanie praktyczne do wykonywania swoich obowiązków z zakresu przetwarzania powierzonych danych?**  Prosimy uzasadnić odpowiedź np. fakt odbycia szkolenia. |  |
| 8. | **ZASOBY/ZARZĄDZANIE PERSONELEM** | Czy osoby delegowane do obsługi danych powierzonych przez administratora posiadają nadane upoważnienia do przetwarzania danych? |  |
| 9. | **ZASOBY/ZARZĄDZANIE PERSONELEM** | Czy osoby upoważnione do przetwarzania danych osobowych zostały zobowiązane do zachowania danych osobowych w tajemnicy?  **Prosimy o przedstawienie wzoru upoważnienia do przetwarzania danych osobowych wraz z obowiązkiem zachowania tajemnicy co do przetwarzanych danych lub wskazaniem w jakim dokumencie osoby upoważnione do przetwarzania danych zostały zobowiązane do zachowania tajemnicy.** |  |
| 10. | **WERYFIKACJA PROCEDUR** | Jak wygląda procedura realizacji praw osób, których dane dotyczą uwzględnienia wspierania administratora w realizacji tych praw?  **Prosimy o wskazanie odpowiedniego wyciągu z procedury.** |  |
| 11. | **ZARZĄDZANIEM DOSTĘPEM** | Czy PP zarządza dostępem do systemów oraz programów komputerowych, w którym są przetwarzane dane osobowe, poprzez proces nadawania, przeglądu i odbierania uprawnień oraz stosuje bezpieczne mechanizmy uwierzytelniania?  **Prosimy o wskazanie odpowiedniej procedury nadawania dostępu.** |  |
| 12. | **ZARZĄDZANIEM DOSTĘPEM** | Czy PP wdrożył i stosuje zasady **udzielania dostępu tylko do informacji niezbędnych do zakresu wykonywanych obowiązków** oraz zasady najmniejszego uprzywilejowania? W myśl zasady najmniejszego uprzywilejowania użytkownik ma mieć dostęp tylko do tych informacji i zasobów, które są mu niezbędne do wykonywania swojej pracy. |  |
| 13. | **ANALIZA RYZYKA** | Czy PP dobrał odpowiednie środki techniczne i organizacyjne zapewniające bezpieczeństwo przetwarzanych danych osobowych zgodnie z aktualnie przeprowadzoną analizą ryzyka naruszenia praw lub wolności osób fizycznych?  **Prosimy o przekazanie aktualnie stosowanych środków bezpieczeństwa.** |  |
| 14. | **ŚRODKI BEZPIECZEŃSTWA** | jakie środki bezpieczeństwa stosuje PP w celu zapewnienia ochrony danych osobowych w czasie ich przechowywania?  Prosimy o wskazanie stosowanych środków. |  |
| 15. | **KOPIA BEZPIECZEŃSTWA** | Czy PP przechowuje kopie bezpieczeństwa w bezpiecznej lokalizacji oraz zabezpiecza kopie przed ich nieuprawnionym dostępem? |  |
| 16. | **ZEWNĘTRZNE AUDYTY PP** | Czy PP 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?  **Prosimy o przekazanie z jaką regularnością takie audyty się odbywają oraz o wskazanie raportu/odpowiednich wniosków z raportu audytowego.** |  |
| 17. | **BEZPIECZEŃSTWO FIZYCZNE** | Czy PP zapewnia nadzór – wykluczający dostęp do danych osobowych – przed osobami niebędącymi pracownikami PP, a przebywającymi w jego siedzibie? |  |
| 18. | **ZARZĄDZANIE INCYDENTAMI** | Jak wygląda procedura postępowania w sytuacji naruszenia ochrony danych osobowych przetwarzanych w imieniu administratora?  Prosimy o wskazanie odpowiedniej procedury/fragmentów procedury. |  |
| 19. | **ZARZĄDZANIE INCYDENTAMI** | Proszę wskazać kto u PP jest odpowiedzialny za kontakt i wykonywanie procedury postępowania w sytuacji naruszenia ochrony danych?  **Prosimy o wskazanie odpowiedniego wyciągu z procedury.** |  |
| 20. | **ZARZĄDZANIE INCYDENTAMI** | Czy PP prowadzi i aktualizuje ewidencję naruszeń ochrony danych osobowych? |  |

………………………………………..

(data i czytelny podpis PP)