**Załącznik nr 6 do Ogłoszenia o zamówieniu**

**Formularz audytowy podmiotu przetwarzającego**

**Podmiot Przetwarzający:** ………………………………….

**Administrator danych:** Ośrodek Przetwarzania Informacji – Państwowy Instytut Badawczy z siedzibą w Warszawie przy al. Niepodległości 188B, Warszawa

W związku z koniecznością potwierdzenia czy Podmiot Przetwarzający zapewnia wystarczające gwarancje wdrożenia odpowiednich środków technicznych i organizacyjnych, by przetwarzanie danych osobowych spełniało wymogi RODO i chroniło prawa osób, których dane dotyczą, uprzejmie proszę o udzielenie odpowiedzi na poniższe pytania:

| **L.p.** | **Pytania w zakresie stosowanych środków technicznych lub organizacyjnych** | **Tak** | **Nie/**  **Nie dotyczy** | **Uwagi** |
| --- | --- | --- | --- | --- |
| 1. | Czy powołano Inspektora Ochrony Danych lub wyznaczono pracownika do pełnienia zadań związanych z ochroną danych osobowych |  |  |  |
| 2. | Czy osoby biorące udział w przetwarzaniu danych osobowych posiadają stosowne upoważnienia i zostały zobowiązane do zachowania tych danych w tajemnicy. |  |  |  |
| 3. | Czy podmiot przetwarzający dokumentuje fakt nadania upoważnienia do przetwarzania danych osobowych lub zobowiązania do zachowania tajemnicy? |  |  |  |
| 4. | Czy Podmiot przetwarzający prowadzi ewidencję osób upoważnionych do przetwarzania danych osobowych? |  |  |  |
| 5. | Czy Podmiot przetwarzający prowadzi Rejestr Kategorii Czynności Przetwarzania? |  |  |  |
| 6. | Czy Podmiot przetwarzający prowadzi Rejestr Czynności Przetwarzania? |  |  |  |
| 7. | Czy w Podmiocie przetwarzającym ustanowiono i wdrożono Politykę bezpieczeństwa danych osobowych? |  |  |  |
| 8. | Czy osoby dopuszczone przez Podmiot przetwarzający do przetwarzania danych osobowych zostały przeszkolone w zakresie przepisów o ochronie danych osobowych, zasad bezpieczeństwa informacji i bezpiecznego korzystania z systemu informatycznego ? |  |  |  |
| 9. | Czy Podmiot przetwarzający dokumentuje przeprowadzenie szkoleń w zakresie przepisów o ochronie danych osobowych, zasad bezpieczeństwa informacji i bezpiecznego korzystania z systemu informatycznego ? |  |  |  |
| 10. | Czy Podmiot przetwarzający w związku z realizacją usług zleconych przez Administratora korzysta lub zamierza korzystać z podwykonawców którym zostaną powierzone dane osobowe przekazane przez Administratora? |  |  |  |
| 11. | Czy Podmiot przetwarzający zamierza przekazać powierzone dane osobowe dalszym podmiot przetwarzającym poza Europejski Obszar Gospodarczy? |  |  |  |
| 12. | Czy podmiot przetwarzający posiada procedurę/ instrukcję/ mechanizm zwrotu powierzonych danych Administratorowi zgodnie z art. 28 RODO? |  |  |  |
| 13. | Czy Podmiot przetwarzający w związku z dalszym powierzeniem danych osobowych posiada odpowiednio zawarte umowy powierzenia zgodne z art. 28 RODO? |  |  |  |
| 14. | Czy Podmiot przetwarzający wykonał audyt w zakresie bezpieczeństwa informacji w okresie ostatnich 2 lat mający na celu ocenę skuteczności stosowanych środków bezpieczeństwa? |  |  |  |
| 15. | Czy podmiot przetwarzający wykonał testy penetracyjne systemów informatycznych wykorzystywanych w swojej organizacji w okresie ostatnich 3 lat? |  |  |  |
| 16. | Czy Podmiot przetwarzający wykonał w swojej organizacji testy socjotechniczne w zakresie bezpieczeństwa informacji w okresie ostatnich 3 lat? |  |  |  |
| 17. | Czy Podmiot przetwarzający posiada procedurę postępowania w przypadku naruszenia ochrony danych osobowych? |  |  |  |
| 18. | Czy Podmiot przetwarzający ma wdrożony SZBI w oparciu o normę ISO 27001? |  |  |  |
| 19. | Czy Podmiot przetwarzający posiada wdrożony proces szacowania ryzyka w zakresie zagrożeń:  a) przypadkowego lub niezgodnego z prawem zniszczenia danych osobowych,  b) utraty, modyfikacji, nieuprawnionego ujawnienia danych osobowych,  c) nieuprawnionego dostępu do danych osobowych przesyłanych, przechowywanych lub w inny sposób przetwarzanych? |  |  |  |
| 20. | Czy w oparciu o przeprowadzoną analizę ryzyka naruszenia praw i wolności osób fizycznych dla czynności, w ramach których doszło do przetwarzania danych osobowych powierzonych mu przez Administratora, Podmiot przetwarzający oświadcza, że ryzyko jest niskie? |  |  |  |
| 21. | Czy Podmiot przetwarzający zobowiązuje się poinformować Administratora w przypadku zmiany poziomu stwierdzonego ryzyka naruszenia praw i wolności osób fizycznych? |  |  |  |
| 22. | Czy Podmiot przetwarzający zapewnia:  b) zdolność do ciągłego zapewnienia poufności, integralności, dostępności i odporności systemów i usług przetwarzania,  c) zdolność do szybkiego przywracania dostępności danych osobowych i dostępu do nich w razie incydentu fizycznego lub technicznego, |  |  |  |
| 23. | Czy Podmiot przetwarzający zapewnia fizyczne zabezpieczenia pomieszczeń/obszarów przetwarzania danych osobowych przed dostępem osób nieuprawnionych w przypadku powierzonych przez Administratora danych osobowych? |  |  |  |
| 24. | Czy Podmiot przetwarzający zapewnia zabezpieczenie dostępu do sprzętu w ramach którego przetwarzane są powierzone przez Administratora dane osobowe? |  |  |  |
| 25. | Czy Podmiot przetwarzający zapewnia zabezpieczenie dostępu do serwerowni w ramach której przetwarzane są powierzone przez Administratora dane osobowe? |  |  |  |
| 26. | Czy Podmiot przetwarzający posiada systemy alarmowe/ antywłamaniowe? |  |  |  |
| 27. | Czy Podmiot przetwarzający stosuje monitoring wizyjny w ramach środków bezpieczeństwa fizycznego? |  |  |  |
| 28. | Czy Podmiot przetwarzający posiada klimatyzację w serwerowni w której przetwarza powierzone przez Administratora dane osobowe? |  |  |  |
| 29. | Czy Podmiot przetwarzający posiada oprogramowanie antywirusowe na wszystkich stacjach roboczych i na bieżąco je aktualizuje? |  |  |  |
| 30. | Czy Podmiot przetwarzający stosuje serwery proxy i bramki filtrujące? |  |  |  |
| 31. | Czy Podmiot przetwarzający posiada ochronę fizyczną obiektów w ramach swojej organizacji? |  |  |  |
| 32. | Czy Podmiot przetwarzający posiada wdrożone procedury zarządzania pojemnością systemów informatycznych? |  |  |  |
| 33. | Czy Podmiot przetwarzający wykonuje kopie bezpieczeństwa i posiada odpowiednie procedury w tym zakresie? |  |  |  |
| 34. | Czy Podmiot przetwarzający posiada wdrożoną procedurę kontroli dostępu i zarządzania przywilejami w systemach teleinformatycznych? |  |  |  |
| 35. | Czy Podmiot przetwarzający zapewnia lokalizację infrastruktury informatycznej w ramach której przetwarza powierzone przez Administratora dane osobowe w lokalizacjach bezpiecznych? |  |  |  |
| 36. | Czy w organizacji podmiotu przetwarzającego jest stosowana polityka czystego biurka? |  |  |  |
| 36. | Czy Podmiot przetwarzający posiada Zapasowe Centrum Danych? |  |  |  |
| 37. | Czy podmiot przetwarzający stosuje szyfrowanie dysków komputerów przenośnych? |  |  |  |
| 38. | Czy podmiot przetwarzający posiada procedury odtwarzania systemu po awarii oraz ich testowania? |  |  |  |
| 39. | Czy Podmiot przetwarzający stosuje podwójne zabezpieczenia dostępu do systemów informatycznych (2FA)? |  |  |  |

Data wypełnienia formularza: Osoba wypełniająca formularz:

…………………………………….... …………………………………………….

(imię, nazwisko, podpis)

Ocena, stopień zgodności i rekomendacje (wypełnia ADO):