**Załącznik nr 5 do Zaproszenia**

**Formularz weryfikacyjny kontrahenta,**

**jako podmiotu przetwarzającego w rozumieniu RODO[[1]](#footnote-1)**

Nazwa kontrahenta:

Adres siedziby:

Strona www:

|  |  |  |  |
| --- | --- | --- | --- |
| **Lp.** | **Pytanie** | **Tak/Nie/****Nie dotyczy** | **Wskazówki/wyjaśnienia** |
| 1. | Czy kontrahent wyznaczył IOD?  |  |  |
| 2. | Jeśli kontrahentnie ma obowiązku wyznaczenia inspektora ochrony danych, czy mimo wszystko wyznaczył inną osobę/zespół odpowiedzialny za nadzór nad ochroną danych osobowych w organizacji? |  |  |
| 3. | Czy kontrahent posiada opracowaną i zatwierdzoną politykę ochrony danych osobowych? |  |  |
| 4. | Czy kontrahent wdrożył procedurę postępowania w przypadku wystąpienia naruszenia ochrony danych osobowych? |  |  |
| 5. | Czy kontrahent wdrożył jakieś inne dokumenty regulujące bezpieczeństwo przetwarzania danych osobowych? |  |  |
| 6. | Czy kontrahentposiada doświadczenie w świadczeniu usług związanych z powierzeniem przetwarzania danych? Jeśli tak, jak długie? |  |  |
| 7. | Czy kontrahent, jako podmiot przetwarzający, prowadzi rejestr kategorii czynności przetwarzania? |  |  |
| 8. | Czy kontrahent zapewnia realizację praw osób, których dane dotyczą, w szczególności prawo dostępu do danych, prawo do sprostowania danych, prawo do usunięcia danych? |  |  |
| 9. | Czy kontrahent dobrał zabezpieczenia zapewniające bezpieczeństwo przetwarzanych danych osobowych w odniesieniu do oceny skutków ich przetwarzania dla praw i wolności osób, których dane dotyczą? |  |  |
| 10. | Czy kontrahent okresowo dokonuje przeglądu ryzyk związanych z przetwarzaniem danych osobowych? |  |  |
| 11. | Czy osoby przetwarzające dane osobowe przeszły szkolenie z zakresu ochrony danych osobowych? |  |  |
| 12. | Czy kontrahent zapewnia, aby nowozatrudniony pracownik przed podjęciem czynności związanych z przetwarzaniem danych osobowych został odpowiednio przeszkolony w tym zakresie i zapoznany z obowiązującymi przepisami prawa? |  |  |
| 13. | Czy osoby wykonujące operacje na danych osobowych zostały upoważnione przez kontrahenta do ich przetwarzania? |  |  |
| 14. | Czy osoby, które uczestniczą w operacjach przetwarzania danych osobowych zostały zobowiązane do zachowania ich w tajemnicy?  |  |  |
| 15. | Czy kontrahent wdrożył odpowiednie środki techniczne i organizacyjne, aby zapewnić stopień bezpieczeństwa odpowiadający ryzyku związanemu z przetwarzaniem danych osobowych, w tym: |  |  |
| * pseudonimizację i szyfrowanie danych,
 |  |  |
| * zdolność do ciągłego zapewnienia poufności, integralności, dostępności i odporności systemów i usług przetwarzania,
 |  |  |
| * zdolność do szybkiego przywrócenia dostępności danych osobowych i dostępu do nich w razie incydentu fizycznego lub technicznego?
 |  |  |
| 16. | Czy kontrahent przeprowadza audyty/kontrole/przeglądy/sprawdzenia dotyczące przestrzegania w organizacji przepisów związanych z ochroną danych osobowych? |  |  |
| 17. | Czy kontrahent korzysta z usług podwykonawców przy przetwarzaniu powierzonych danych osobowych? Jeśli tak, prosimy wskazać w kolumnie „Wskazówki/wyjaśnienia” dane podwykonawców (nazwa oraz adres siedziby). |  |  |
| 18. | Czy podwykonawcy zostali/zostaną poddani weryfikacji pod kątem wdrożenia środków ochrony danych osobowych?  |  |  |
| 19. | Czy z podwykonawcami została/zostanie zawarta umowa powierzenia przetwarzania danych osobowych? |  |  |
| 20. | Czy powierzone dane osobowe będą przetwarzane poza granicami Unii Europejskiej (dokumenty papierowe, urządzenia elektroniczne, serwery z danymi, usługi chmurowe, itp.)? Jeśli tak, prosimy wskazać szczegóły w kolumnie „Wskazówki/wyjaśnienia”. |  |  |
| 21. | Czy każdy komputer, na którym przetwarzane są dane osobowe, jest chroniony programem antywirusowym? |  |  |
| 22. | Czy kontrahent tworzy kopie zapasowe przetwarzanych danych osobowych? |  |  |
| 23. | Czy kontrahent stosuje szyfrowanie dysków komputerów przenośnych? |  |  |
| 24. | Czy w przypadku przekazywania danych osobowych środkami telekomunikacyjnymi lub na nośnikach zewnętrznych, przekazywane dane są szyfrowane? |  |  |
| 25. | Czy dostęp do wykorzystywanych przez kontrahentasystemów informatycznych wymaga uwierzytelniania użytkownika tj. podania indywidualnego identyfikatora i hasła? |  |  |
| 26. | Jeśli tak, to czy zastosowano systemowe mechanizmy wymuszające okresowe zmiany haseł użytkowników? |  |  |
| 27. | Czy systemy informatyczne przetwarzające dane osobowe wykorzystywane przez kontrahenta pozwalają przypisać określone działanie w systemie do osoby lub procesu oraz umiejscowić je w czasie (zapewniają rozliczalność operacji wykonywanych na danych)? |  |  |
| 28. | Czy pracownicy zostali zobowiązani do zabezpieczania nieużywanych w danym momencie systemów poprzez blokadę ekranu lub w inny równoważny sposób? |  |  |
| 29. | Czy kontrahent stosuje fizyczne środki służące ochronie danych przed nieuprawnionym dostępem? Jeśli tak, prosimy je wymienić w kolumnie „Wskazówki/wyjaśnienia” (np. system kontroli dostępu, system alarmowy, ochrona fizyczna, monitoring wizyjny). |  |  |

 ***………………………………………………………………………………***

(data, pieczątka, podpis osoby wypełniającej ankietę)

1. Rozporządzenie Paramentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych). [↑](#footnote-ref-1)