#### Załącznik nr 10 do SIWZ

**OŚWIADCZENIE DOTYCZĄCE BEZPIECZEŃSTWA PRZETWARZANIA DANYCH OSOBOWYCH U PODMIOTU PRZETWARZAJĄCEGO**

|  |  |  |
| --- | --- | --- |
| **L.p.** | **Pytanie** | **Odpowiedź** |
| **1** | Czy zgodnie z art. 29 RODO osoby wykonujące operacje na danych osobowych otrzymały od podmiotu przetwarzającego upoważnienia do przetwarzania danych, w których został określony w szczególności zakres przetwarzanych przez te osoby danych? |  |
| **2** | Czy podmiot przetwarzający prowadzi rejestr kategorii czynności przetwarzania zawierający wszystkie informacje wskazane w art. 30 ust. 2 RODO? |  |
| **3** | Czy podmiot przetwarzający posiada opracowaną i zatwierdzoną politykę ochrony danych osobowych? |  |
| **4** | Czy podmiot przetwarzający jest w stanie wykazać przestrzeganie danych osobowych m. in. poprzez przedstawienie obowiązujących w jego organizacji procedur i dokumentacji ochrony danych osobowych? |  |
| **5** | Czy podmiot przetwarzający zapewnia, aby nowozatrudniony pracownik przed podjęciem czynności związanych z przetwarzaniem danych osobowych został odpowiednio przeszkolony w tym zakresie i zapoznany z obowiązującymi przepisami prawa? |  |
| **6** | Czy podmiot przetwarzający dba o bieżące doskonalenie wiedzy swoich pracowników poprzez cykliczne szkolenia oraz inne działania mające na celu uświadamianie pracowników w zakresie zagadnień dotyczących ochrony danych osobowych? |  |
| **7** | Czy pracownicy podmiotu przetwarzającego, którzy uczestniczą w operacjach przetwarzania danych osobowych zostali zobowiązani do zachowania ich w tajemnicy? |  |
| **8** | Czy w ciągu dwóch ostatnich lat podmiot przetwarzający poddawał zewnętrznej kontroli niezależnych audytorów funkcjonujący w jego organizacji system ochrony danych osobowych? |  |
| **9** | Czy podmiot przetwarzający korzysta z usług tylko takich podmiotów zewnętrznych/ podwykonawców, którzy zostali wcześniej przez niego sprawdzeni pod kątem zapewnienia odpowiedniego poziomu ochrony danych osobowych? |  |
| **10** | Czy zastosowano środki kontroli dostępu fizycznego do budynku/budynków tylko dla autoryzowanego personelu? |  |
| **11** | Czy zapewniono fizyczne oddzielenie środków przetwarzania informacji zarządzanych przez organizację od tych, które należą do innych organizacji? |  |
| **12** | Czy dostęp do pomieszczeń pozostających w dyspozycji podmiotu przetwarzającego po godzinach pracy nie jest możliwy dla osób trzecich (firma sprzątająca, ochrona), bądź dostęp ten jest szczegółowo nadzorowany? |  |
| **13** | Czy każdy pracownik otrzymuje imienny identyfikator do systemów informatycznych? |  |
| **14** | Czy systemy informatyczne zapewniają wymuszanie na użytkownikach okresowe zmiany haseł oraz zmian w razie zaistniałej potrzeby? |  |
| **15** | Czy pracownicy zostali zobowiązani do zabezpieczania nieużywanych w danym momencie systemów poprzez blokadę ekranu lub w inny równoważny sposób? |  |
| **16** | Czy pracownicy zostali zobowiązani do niezwłocznego odbierania z drukarek wydruków zawierających dane osobowe lub inne poufne informacje? Czy wskazana zasada jest przestrzegana przez pracowników? |  |
| **17** | Czy w organizacji jest stosowana polityka tzw. „czystego biurka”? |  |
| **18** | Czy dane osobowe gromadzone w formie papierowej, po godzinach pracy organizacji, przechowywane są w zamykanych szafach/szafkach/szufladach bez możliwości dostępu do nich osób nieupoważnionych? |  |
| **19** | Czy zapewniono oprogramowanie antywirusowe na wszystkich stacjach? |  |
| **20** | Czy oprogramowanie posiada licencję i jest na bieżąco aktualizowane? |  |
| **21** | Czy urządzenia mobilne posiadają skonfigurowaną kontrolę dostępu? |  |
| **22** | Czy wobec urządzeń mobilnych stosuje się techniki kryptograficzne? |  |
| **23** | Czy na urządzeniach mobilnych zainstalowano oprogramowania antywirusowe? |  |
| **24** | Czy zapewniono zdolności do szybkiego przywrócenia dostępności danych osobowych i dostępu do nich w razie incydentu fizycznego lub technicznego? |  |
| **25** | Jaki przyjęto zakres oraz częstotliwość tworzenia kopii zapasowych? |  |
| **26** | Czy organizacja posiada procedury odtwarzania systemu po awarii oraz ich testowania? |  |
| **27** | Czy organizacja wdraża nowe rozwiązania zgodnie z zasadą "privacy by design"? |  |
| **28** | Czy organizacja działa zgodnie z zasadą "privacy by default"? |  |
| **29** | Czy organizacja prowadzi ocenę skutków dla ochrony danych? |  |
| **30** | Czy organizacja gwarantuje realizację praw osób, których dane dotyczą tj. m.in. prawo do przenoszenia danych, prawo do ograniczenia przetwarzania, prawo do bycia zapomnianym? |  |

Składając ofertę w postępowaniu, **oświadczam (-y) ,**  iż stosuję (-my) środki bezpieczeństwa spełniające wymogi Rozporządzenia RODO\* oraz z innych przepisów prawa powszechnie obowiązującego, które chronią prawa osób, których dane dotyczą.

**----------------------------------- --------------------------------------------**

**[miejscowość, data] [podpis (-y)]**

*\* Rozporządzenie Parlamentu 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.*