*Załącznik nr 2*

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
|  |  |  |  |  |  |
|  |  |
| **Ankieta podmiotu przetwarzającego Ocena podmiotu przetwarzającego dane w zakresie wdrożenia odpowiednich środków technicznych i organizacyjnych gwarantujących zgodność z RODO** |  |
|  | **KONTRAHENT - podmiot przetwarzający (nazwa):** |  |  |
|  | **CZEGO DOTYCZY UMOWA:** |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
| **LP**  | **PYTANIA** | **TAK/NIE** | **ODPOWIEDŹ / DODATKOWY OPIS** |  |
|  |  |  |  |  |  |
| **WIEDZA FACHOWA / WIARYGODNOŚĆ** |  |
| **1.** | Czy podmiot przetwarzający wyznaczył / zamierza wyznaczyć inspektora ochrony danych (IOD)? |   |   |  |
| **2.** | Czy podmiot przetwarzający posiada udokumentowane procedury określające zasady postępowania podczas przetwarzania danych osobowych? |   |   |  |
| **3.** | 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 i regulacjami wewnętrznymi?  |   |   |  |
| **4.** | 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?  |   |   |  |
| **5.** | Czy pracownicy podmiotu przetwarzającego, którzy uczestniczą w operacjach przetwarzania danych osobowych zostali zobowiązani do zachowania ich w tajemnicy? |   |   |  |
| **6.** | 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? |   |   |  |
| **7.** | Czy osoby zatrudnione przez podmiot przetwarzający przy przetwarzaniu danych osobowych zostały przeszkolone w zakresie obsługi, w tym bezpiecznego korzystania z systemów informatycznych wykorzystywanych przez podmiot przetwarzający? |   |   |  |
| **ZASOBY / ZABEZPIECZENIA** |  |
| **8.** | 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?  |   |   |  |
| **9.** | Czy podmiot przetwarzający prowadzi rejestr kategorii czynności przetwarzania zawierający wszystkie informacje wskazane w art. 30 ust. 2 RODO? |   |   |  |
| **10.** | Czy podmiot przetwarzający opracował i wdrożył udokumentowane instrukcje/procedury postępowania w sytuacji naruszenia ochrony danych osobowych? |   |   |  |
| **11.** | Czy podmiot przetwarzający prowadzi w sposób udokumentowany ewidencję naruszeń przepisów o ochronie danych osobowych, w tym naruszeń bezpieczeństwa danych? |   |   |  |
| **12.** | Czy zastosowano środki kontroli dostępu fizycznego do budynku/budynków umożliwiające wstęp tylko dla autoryzowanego personelu? |   |   |  |
| **13.** | 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? |   |   |  |
| **14.** | Czy każdy pracownik otrzymuje indywidualny, imienny identyfikator do systemów informatycznych? |   |   |  |
| **15.** | 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? |   |   |  |
| **16.** | Czy zapewniono oprogramowanie antywirusowe na wszystkich stacjach?  |   |   |  |
| **17.** | Czy użyto system Firewall do ochrony dostępu do sieci komputerowej? Czy firewall tworzy logi? |   |   |  |
| **18.** | Czy zostały opracowane i wdrożone udokumentowane procedury w zakresie zabezpieczenia podczas przechowywania i transportu, przenośnego służbowego sprzętu komputerowego? |   |   |  |
| **19.** | Czy stosuje się szyfrowanie dysków komputerów przenośnych? |   |   |  |
| **20.** | Czy została opracowana i wdrożona procedura wycofywania i utylizacji dysków twardych komputerów i urządzeń serwerowych, po zakończeniu ich eksploatacji? |   |   |  |
| **21.** | Czy urządzenia mobilne posiadają skonfigurowaną kontrolę dostępu? |   |   |  |
| **22.** | Czy zapewniono zdolności do szybkiego przywrócenia dostępności danych osobowych i dostępu do nich w razie incydentu fizycznego lub technicznego? |   |   |  |
| **23.** | Jaki przyjęto zakres oraz częstotliwość tworzenia kopii zapasowych? |   |   |  |
| **24.** | Gdzie są przechowywane kopie zapasowe (w jaki sposób)? |   |   |  |
| **25.** | Czy podmiot przetwarzający posiada procedury odtwarzania systemu po awarii oraz realizuje testy takich procedur? |   |   |  |
| **26.** | Czy podmiot przetwarzający wdraża nowe rozwiązania zgodnie z zasadą "privacy by design" oraz "privacy by default"? |   |   |  |
| **27.** | Czy podmiot przetwarzający gwarantuje realizację praw osób, których dane dotyczą tj. m.in. prawo do przenoszenia danych, prawo do ograniczenia przetwarzania, prawo do bycia zapomnianym? |   |   |  |
| **28.** | Czy podmiot przetwarzający zastosował środki techniczne i organizacyjne zapewniające ochronę przetwarzanych danych osobowych odpowiednią do zagrożeń oraz kategorii danych objętych ochroną, a w szczególności czy zabezpieczył dane przed ich udostępnieniem osobom nieupoważnionym, zabraniem przez osobę nieuprawnioną, przetwarzaniem z naruszeniem ustawy oraz zmianą, utratą, uszkodzeniem lub zniszczeniem w sposób adekwatny do zidentyfikowanych zagrożeń (podejście oparte na ryzyku)? Jakie ewentualnie dodatkowe środki zostały wdrożone w związku dokonaniem analizy ryzyka?  |   |   |  |
| **29.** | Czy podmiot przetwarzający prowadzi regularnie audyty dotyczące zasad bezpieczeństwa informacji, w tym danych osobowych? Czy wnioski z audytów zostały udokumentowane, np. w raporcie audytowym? |   |   |  |
| **30.** | Czy prowadzona jest ocena skuteczności i monitorowanie środków technicznych i organizacyjnych mających zapewnić bezpieczeństwo przetwarzania? Czy działania te są dokumentowane? |   |   |  |
|  |  |  |  |  |  |
|  |   |  |  |  |  |
|  | Data i podpis osoby wypełniającej ankietę |  | Data i podpis osoby zatwierdzającej ankietę |  |