**LISTA KONTROLNA (WERYFIKACYJNA) PRZETWARZAJĄCEGO**

**przed zawarciem umowy powierzenia przetwarzania danych osobowych**

| **Lp.** | **PYTANIE** | **ODPOWIEDŹ** |
| --- | --- | --- |
| **1.** | **2.** | **3.** |
|  | **WYMAGANIA INFORMACYJNE.** |  |
|  | Czy Przetwarzający wyznaczył inspektora ochrony danych?  *ODP: TAK / NIE*  Jeśli TAK, proszę o wskazanie danych IOD.  *ODP: IMIĘ, NAZWISKO, KONTAKT: NR TELEFONU, E-MAIL* |  |
|  | Kto wykonuje zadania dotyczące zapewniania przestrzegania przepisów o ochronie danych osobowych w organizacji (w sytuacji braku powołania inspektora ochrony danych)? Proszę o wskazanie.  *ODP: NIE DOTYCZY (gdy jest powołany IOD i jego dane wskazano w punkcie 1.1) / IMIĘ, NAZWISKO, KONTAKT: NR TELEFONU, E-MAIL* |  |
|  | Czy Przetwarzający stosuje się do przyjętych przez organ nadzorczy kodeksów podstępowania? Oczywiście o ile taki kodeks występuje w danej branży.  *ODP: TAK / NIE / NIE DOTYCZY (gdy nie ma takiego kodeksu)* |  |
|  | Czy Przetwarzający objęty jest monitorowaniem przestrzegania kodeksu postępowania przez akredytowany podmiot monitorujący? Oczywiście o ile taki kodeks występuje w danej branży.  *ODP: TAK / NIE / NIE DOTYCZY (gdy nie ma takiego kodeksu)* |  |
|  | Czy Przetwarzający otrzymał certyfikat zgodności z RODO?  *ODP: TAK / NIE / NIE DOTYCZY (gdy nie ma procedury takiej certyfikacji)* |  |
|  | **WYMAGANIA FAKULTATYWNE.** |  |
|  | Czy Przetwarzający stosuje pseudonimizację lub/i szyfrowanie danych osobowych?  *ODP: TAK / NIE* |  |
|  | Czy osoby wyznaczone do wykonywania zadań z zakresu Przetwarzającego posiadają odpowiednią wiedzę i przygotowanie praktyczne do wykonywania swoich obowiązków z zakresu przetwarzania powierzonych danych?  *ODP: TAK / NIE* |  |
|  | Czy Przetwarzający prowadzi i jak często 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?  *ODP: TAK, CO ....... MIESIĘCY (DNI, LAT) / NIE* |  |
|  | Czy Przetwarzający zapewnia nadzór – wykluczający dostęp do danych osobowych – przed osobami niebędącymi pracownikami, a przebywającymi w jego siedzibie?  *ODP: TAK / NIE* |  |
|  | Czy u Przetwarzającego jest wyznaczona osoba odpowiedzialna za kontakt i wykonywanie procedury postępowania w sytuacji naruszenia ochrony danych?  *ODP: TAK / NIE*  Jeśli TAK, proszę o wskazanie danych kontaktowych tej osoby.  *ODP: IMIĘ, NAZWISKO, KONTAKT: NR TELEFONU, E-MAIL* |  |
|  | Czy 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?  *ODP: TAK / NIE* |  |
|  | Czy Przetwarzający korzysta z usług tylko takich podmiotów zewnętrznych/podwykonawców, którzy zostali wcześniej przez niego sprawdzeni pod kątem zapewnienia odpowiedniego poziomu ochrony danych osobowych?  *ODP: TAK / NIE* |  |
|  | Czy Przetwarzający 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.  *ODP: TAK / NIE* |  |
|  | Czy Przetwarzający tworzy i przechowuje kopie bezpieczeństwa w bezpiecznej lokalizacji oraz zabezpiecza kopie przed ich nieuprawnionym dostępem?  *ODP: TAK / NIE* |  |
|  | Czy Przetwarzający prowadzi i aktualizuje ewidencję naruszeń ochrony danych osobowych?  *ODP: TAK / NIE* |  |
|  | Czy Przetwarzający przekazuje dane do państwa trzeciego lub organizacji międzynarodowej?  *ODP: TAK / NIE*  Jeśli TAK, proszę o wskazanie do jakiego państwa trzeciego lub organizacji międzynarodowej są przekazywane dane osobowe.  *ODP: KRAJ, NAZWA ORGANIZACJI* |  |
|  | Czy Przetwarzający miał kontrolę, postępowanie wyjaśniające lub inne działania prowadzone przez Prezesa UODO lub inny organ nadzorczy, zakończone wydaniem zaleceń pokontrolnych lub decyzji?  *ODP: TAK / NIE*  Jeżeli TAK, proszę o wskazanie przedmiotu postępowania prowadzonego przez Prezesa UODO lub innych organ kontrolny i jakie są wyniki przeprowadzonych działań?  ODP: PRZEDMIOT POSTĘPOWANIA, SYGNATURA SPRAWY, ORGAN PROWADZĄCY, WYNIK POSTĘPOWANIA, WYDANE DECYZJE LUB ZALECENIA |  |
|  | **WYMAGANIA OBLIGATORYJNE.** |  |
|  | Czy osoby delegowane do obsługi danych powierzonych przez administratora posiadają nadane upoważnienia do przetwarzania danych?  *ODP: TAK / NIE* |  |
|  | Czy osoby upoważnione do przetwarzania danych osobowych zostały zobowiązane do zachowania danych osobowych w tajemnicy?  *ODP: TAK / NIE*  DODATKOWO: Można przedstawić wzór upoważnienia do przetwarzania danych osobowych wraz z obowiązkiem zachowania tajemnicy co do przetwarzanych danych lub wskazać w jakim dokumencie osoby upoważnione do przetwarzania danych zostały zobowiązane do zachowania tajemnicy. |  |
|  | Czy Przetwarzający posiada opracowaną procedurę realizacji praw osób, których dane dotyczą, uwzględniającą wspieranie administratora w realizacji tych praw?  *ODP: TAK / NIE* |  |
|  | Czy Przetwarzający 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?  *ODP: TAK / NIE* |  |
|  | Czy Przetwarzający dobrał odpowiednie środki techniczne i organizacyjne zapewniające bezpieczeństwo przetwarzanych danych osobowych?  *ODP: TAK / NIE* |  |
|  | Czy Przetwarzający przeprowadza analizę ryzyka naruszenia praw lub wolności osób fizycznych dla organizacji?  *ODP: TAK / NIE* |  |
|  | Czy Przetwarzający opracował procedurę postępowania w sytuacji naruszenia ochrony danych osobowych przetwarzanych w imieniu administratora?  *ODP: TAK / NIE* |  |
|  | Czy Przetwarzający prowadzi rejestr kategorii czynności przetwarzania zawierający wszystkie informacje wskazane w art. 30 ust. 2 RODO?  *ODP: TAK / NIE* |  |
|  | Czy Przetwarzający posiada opracowaną i zatwierdzoną politykę ochrony danych osobowych oraz instrukcję zarządzania systemami informatycznymi?  *ODP: TAK / NIE* |  |
|  | Czy oprogramowanie stosowane przez Przetwarzającego posiada licencję i jest na bieżąco aktualizowane?  *ODP: TAK / NIE* |  |
|  | Czy zapewniono zdolności do szybkiego przywrócenia dostępności danych osobowych i dostępu do nich w razie incydentu fizycznego lub technicznego?  *ODP: TAK / NIE* |  |
|  | Czy Przetwarzający wdraża nowe rozwiązania zgodnie z zasadą „privacy by design”?  *ODP: TAK / NIE* |  |
|  | Czy Przetwarzający działa zgodnie z zasadą „privacy by default”?  *ODP: TAK / NIE* |  |
|  | Czy Przetwarzający prowadzi ocenę skutków dla ochrony danych?  *ODP: TAK / NIE* |  |

**POUCZENIE:**

1. Lista kontrolna podzielona została na 3 części:
   1. Część pierwsza zawierająca wymagania informacyjne – zawiera ona pytania dotyczące ogólnego funkcjonowania podmiotu przetwarzającego, dane IOD (jeśli został wyznaczony) oraz dane kontaktowe,
   2. Część druga zawierająca wymagania fakultatywne – zawiera ona pytania, na które udzielenie negatywnej odpowiedzi (lub w przypadku pytań nr 2.11 i 2.12 pozytywnej odpowiedzi) nie powoduje automatycznie stwierdzenia niespełniania przesłanek do zawarcia umowy powierzenia przetwarzania danych osobowych. Po jednym punkcie otrzymuje się za udzielenie odpowiedzi TAK do pytań nr 2.1-2.10 oraz odpowiedzi NIE do pytań nr 2.11-2.12. Pozytywny wynik z tej części otrzymuje się, gdy zostanie zgromadzone co najmniej 9 punktów,
   3. Część trzecia zawierająca wymagania obligatoryjne – zawiera ona pytania, na które udzielenie negatywnej odpowiedzi do któregokolwiek z pytań, spowoduje stwierdzenie niespełniania przesłanek do zawarcia umowy powierzenia przetwarzania danych osobowych.
2. Pod każdym z pytań zawarto podpowiedź w jakiej formie należy udzielić odpowiedzi (np. TAK / NIE / NIE DOTYCZY / lub wskazanie konkretnych danych żądanych w tym pytaniu).
3. Lista kontrolna jest jednym z elementów wypełnienia obowiązków prawnych ciążących na Białostockim Centrum Onkologii im. Marii Skłodowskiej-Curie w Białymstoku, jako Administratorze Danych Osobowych. Zgodnie z art. 28 ust. 1 Rozporządzenia 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 (ogólne rozporządzenie o ochronie danych) (RODO) – „Jeżeli przetwarzanie ma być dokonywane w imieniu administratora, korzysta on wyłącznie z usług takich podmiotów przetwarzających, które zapewniają wystarczające gwarancje wdrożenia odpowiednich środków technicznych i organizacyjnych, by przetwarzanie spełniało wymogi niniejszego rozporządzenia i chroniło prawa osób, których dane dotyczą”. Kontrola Administratora Danych Osobowych nad spełnieniem wymagań z ww. przepisu następuje przed podpisaniem umowy powierzenia przetwarzania danych osobowych z podmiotem przetwarzającym.