

Załącznik nr 1 do Umowy powierzenia przetwarzania danych osobowych (wzór)

[•] Jedynie wybrany Wykonawca zobowiązany będzie do przedłożeniaZamawiającemu wypełnionej Ankiety przed zawarciem umowy powierzenia przetwarzania danych osobowych[•]**Ankieta – spełnianie wymagań bezpiecznego przetwarzania danych osobowych**

Celem wypełnienia ankiety<sup>1</sup> jest wykazanie, że Podmiot przetwarzający spełnia wymóg wdrożenia odpowiednich środków technicznych i organizacyjnych, wymaganych przez 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, dalej: „rozporządzenie”) i chroni prawa osób, których dane dotyczą, jak również potwierdzenie że Administrator, zgodnie z przepisem art. 28 ust. 1 rozporządzenia, korzysta wyłącznie z usług podmiotów, które wdrożyły odpowiednie środki techniczne i organizacyjne, zapewniających że przetwarzanie spełnia wymogi rozporządzenia i chroni prawa osób, których dane dotyczą.

Nazwa Podmiotu [•] .....

| Lp. | Pytanie                                                                                                                                                                                                                                       | Poziom zgodności <sup>2</sup><br>Zgodność/częściowa<br>zgodność/brak<br>zgodności | Odpowiedź<br><br>(przedstawić opisowo sposób realizacji/wdrożone<br>środki) |
|-----|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------|-----------------------------------------------------------------------------|
| 1.  | Jakie środki techniczne i organizacyjne, o których mowa w art. 32 rozporządzenia wdrożył Podmiot przetwarzający?<br><br>Należy krótko opisać środki techniczne i organizacyjne stosowane w celu zapewnienia bezpieczeństwa danych obejmujące: |                                                                                   |                                                                             |

<sup>1</sup> Zamiast ankiety, Podmiot przetwarzający może przedstawić ogólny opis środków technicznych i organizacyjnych stosowanych przez ten Podmiot przetwarzający (z uwzględnieniem zagadnień wskazanych w ankiecie), by wykazać, że zapewnia wystarczające gwarancje by przetwarzanie spełniało wymogi rozporządzenia i chroniło prawa osób, których dane dotyczą.

<sup>2</sup> Wybrać właściwe.

|    |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       |  |  |
|----|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--|--|
|    | <ol style="list-style-type: none"> <li>1) zarządzanie ryzykiem w obszarze danych osobowych,</li> <li>2) zarządzanie incydentami, w tym zasady zgłaszania Administratorowi danych osobowych naruszenia przetwarzania danych osobowych,</li> <li>3) środki umożliwiające pseudonimizację i szyfrowanie danych osobowych,</li> <li>4) środki zapewniające zdolność do ciągłego zapewnienia poufność, integralność, dostępność i odporność systemów i usług przetwarzania,</li> <li>5) środki zapewniające zdolność do szybkiego przywrócenia dostępności danych osobowych i dostępu do nich po awariach i innych sytuacjach kryzysowych,</li> <li>6) procesy umożliwiające regularne testowanie, mierzenie i ocenianie skuteczności środków technicznych i organizacyjnych mających zapewnić bezpieczeństwo przetwarzania danych osobowych,</li> <li>7) środki umożliwiające identyfikację i autoryzację użytkowników,</li> <li>8) środki zapewniające ochronę danych w czasie ich przechowywania oraz przekazywania, z uwzględnieniem zasad korzystania z nośników informacji,</li> <li>9) środki umożliwiające rejestrowanie zdarzeń,</li> <li>10) środki służące do konfiguracji systemu, w tym konfiguracji domyślnej,</li> <li>11) środki zapewniające retencję danych,</li> <li>12) środki zapewniające rozliczalność,</li> <li>13) środki umożliwiające przenoszenie danych i zapewnienie ich usuwania</li> </ol> |  |  |
| 2. | Czy podmiot przetwarzający posiada opracowaną i zatwierdzoną politykę ochrony danych osobowych?                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       |  |  |

|     |                                                                                                                                                                                                                                                   |  |  |
|-----|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--|--|
| 3.  | Czy podmiot przetwarzający zapewnia, że pracownik przed podjęciem czynności związanych z przetwarzaniem danych osobowych został przeszkolony i zapoznany z obowiązującymi przepisami prawa dotyczącymi danych osobowych?                          |  |  |
| 4.  | 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 danych osobowych?          |  |  |
| 5.  | Czy jest prowadzony rejestr wszystkich kategorii czynności przetwarzania, zgodnie art. 30 ust. 2 RODO?                                                                                                                                            |  |  |
| 6.  | Czy Podmiot Przetwarzający posiada opracowaną i wdrożoną procedurę/zasady zapewniającą, że dalsze powierzenie przetwarzania danych odbywa się zawsze za uprzednią zgodą administratora danych?                                                    |  |  |
| 7.  | Czy Podmiot przetwarzający posiada opracowaną i wdrożoną procedurę/zasady zapewniającą, że na dalszy podmiot przetwarzający zostają nałożone - w drodze umowy - te same obowiązki ochrony danych, jak w umowie zawartej z administratorem danych? |  |  |
| 8.  | Czy zastosowano środki kontroli dostępu fizycznego do budynku/budynków tylko dla autoryzowanego personelu?                                                                                                                                        |  |  |
| 9.  | Czy systemy informatyczne zapewniają wymuszanie na użytkownikach okresowe zmiany haseł oraz zmian w razie zaistnienia potrzeby?                                                                                                                   |  |  |
| 10. | Czy pracownicy stosują ochronę przetwarzanych danych osobowych podczas pracy na komputerze, laptopie np. poprzez blokadę ekranu                                                                                                                   |  |  |

|     |                                                                                                                                                                                                                                                 |  |  |
|-----|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--|--|
|     | lub w inny sposób (np. w razie konieczności chwilowego opuszczenia stanowiska pracy)?                                                                                                                                                           |  |  |
| 11. | Czy dane osobowe gromadzone w formie papierowej, po godzinach pracy, przechowywane są w zamykanych szafach/szafkach/szufladach bez możliwości dostępu do nich osób nieupoważnionych?                                                            |  |  |
| 12. | Czy zapewniono oprogramowanie antywirusowe na wszystkich komputerach, w tym komputerach przenośnych?                                                                                                                                            |  |  |
| 13. | Czy oprogramowanie komputerów posiada stosowne licencje i czy jest na bieżąco aktualizowane?                                                                                                                                                    |  |  |
| 14. | Czy stosuje się szyfrowanie dysków komputerów przenośnych?                                                                                                                                                                                      |  |  |
| 15. | Czy Podmiot przetwarzający stosuje zatwierdzony kodeks postępowania, o którym mowa w art. 40 rozporządzenia?                                                                                                                                    |  |  |
| 16. | Czy Podmiot przetwarzający uzyskał certyfikację, o której mowa w art. 42 rozporządzenia?                                                                                                                                                        |  |  |
| 17. | Czy Podmiot przetwarzający posiada certyfikat zgodności z normą ISO / IEC 27001?                                                                                                                                                                |  |  |
| 18. | Czy były/są prowadzone wobec Podmiotu przetwarzającego postępowania sądowe/administracyjne związane z naruszeniem przetwarzania danych osobowych? Jeżeli były/są to należy wskazać ile było/jest takich postępowań oraz jak zostały zakończone. |  |  |

.....  
(data, czytelny podpis osoby upoważnionej do reprezentacji)