*Załącznik nr 11 do SIWZ – ankieta RODO*

**FORMULARZ AUDYTOWY PODMIOTU PRZETWARZAJĄCEGO POWIERZONE DANE OSOBOWE**

**Podmiot Przetwarzający:** *................................................................................. (nazwa i adres)*

**Klient:** KATOWICKA INFRASTRUKTURA WODOCIĄGOWO-KANALIZACYJNA Sp. z o.o., ul. Wandy 6, 40-322 Katowice

W związku z koniecznością ustalenia, czy Podmiot Przetwarzający zapewnia wystarczające gwarancje wdrożenia odpowiednich środków technicznych i organizacyjnych, by przetwarzanie danych osobowych spełniało wymogi RODO[[1]](#footnote-1) i chroniło prawa osób, których dane dotyczą, uprzejmie prosimy o udzielenie odpowiedzi na poniższe pytania.

|  |  |
| --- | --- |
|  | **Powołanie Inspektora Ochrony Danych lub osoby o podobnych kompetencjach i zadaniach** |
| **Lp.** | **TREŚĆ PYTANIA** | **TAK/NIE** | **UWAGI** |
| 1. | Czy Podmiot Przetwarzający dokonał prawnej analizy istnienia obowiązku wyznaczenia Inspektora Ochrony Danych (IOD)? |  |  |
| 2. | Czy na Podmiocie Przetwarzającym spoczywa obowiązek wyznaczenia IOD? |  |  |
| 3. | Czy Podmiot Przetwarzający wyznaczył IOD? |  | *Proszę podać dane kontaktowe IOD (imię, nazwisko, nr telefonu/ adres e-mail)* |
| 4. | Jeżeli IOD nie został wyznaczony, to czy zadania dotyczące zapewniania zgodności z przepisami o ochronie danych osobowych w ramach organizacji wykonuje inna wyznaczona osoba?  |  | *Proszę podać dane kontaktowe osoby wyznaczonej do zapewniania zgodności z przepisami o ochronie danych osobowych (imię, nazwisko, nr telefonu/ adres e-mail)* |

|  |
| --- |
| **Bezpieczeństwo zasobów ludzkich** |
| **Lp.** | **TREŚĆ PYTANIA** | **TAK/NIE** | **UWAGI** |
| 1. | Czy osoby dopuszczone przez Podmiot Przetwarzający do przetwarzania danych osobowych zostały przeszkolone w zakresie przepisów o ochronie danych osobowych, zasad bezpieczeństwa informacji i bezpiecznego korzystania z systemu informatycznego? |  |  |
| 2. | Czy Podmiot Przetwarzający dokumentuje przeprowadzanie szkoleń w zakresie przepisów o ochronie danych osobowych, zasad bezpieczeństwa informacji i bezpiecznego korzystania z systemu informatycznego ? |  |  |
| 3. | Czy osoby dopuszczone przez Podmiot Przetwarzający do przetwarzania danych osobowych są upoważnione do ich przetwarzania? |  | *Proszę opisać sposób dokumentowania upoważnień* |
| 4. | Czy Podmiot Przetwarzający dokumentuje nadawanie upoważnień do przetwarzania danych osobowych? |  |  |
| 5. | Czy osoby upoważnione do przetwarzania danych osobowych zobowiązały się do zachowania tajemnicy lub podlegają odpowiedniemu ustawowemu obowiązkowi zachowania tajemnicy? |  |  |
| 6. | Czy Podmiot Przetwarzający dokumentuje fakt zobowiązania się do zachowania tajemnicy przez upoważnione do przetwarzania danych? |  | *Proszę opisać sposób dokumentowania faktu zobowiązania osób upoważnionych* |
| 7. | Czy Podmiot Przetwarzający prowadzi ewidencję nadanych upoważnień? |  |  |

|  |
| --- |
| **Naruszenia ochrony danych osobowych oraz realizacja praw osób, których dane dotyczą** |
| **Lp.** | **TREŚĆ PYTANIA** | **TAK/NIE** | **UWAGI** |
| 1. | Czy Podmiot Przetwarzający jest w stanie zapewnić Klientowi pomoc w wywiązaniu się z obowiązku zgłaszania naruszeń ochrony danych osobowych organowi nadzorczemu oraz zawiadamiania osób fizycznych o naruszeniach, w odniesieniu do powierzanych danych osobowych? |  |  |
| 2. | Czy Podmiot Przetwarzający wdrożył procedurę lub inną dokumentację dotyczącą postępowania w przypadku naruszenia ochrony danych? |  | *Proszę opisać rodzaj wdrożonej dokumentacji* |
| 3. | Czy Podmiot Przetwarzający jest w stanie zapewnić Klientowi pomoc w wywiązaniu się z obowiązku odpowiadania na żądania osoby fizycznej w zakresie wykonywania jej praw przyznanych na mocy RODO – w odniesieniu do powierzanych danych osobowych? |  |  |

|  |
| --- |
| **Dalsze powierzanie przetwarzania powierzonych danych osobowych** |
| **Lp.** | **TREŚĆ PYTANIA** | **TAK/NIE** | **UWAGI** |
| 1. | Czy w ramach realizacji usług zleconych przez Klienta Podmiot Przetwarzający zamierza korzystać z usług podwykonawców, którym zostaną dalej powierzone dane osobowe przekazane przez Klienta (tzw. Podpowierzenie)? |  | *Proszę podać zakres podpowierzanych danych oraz informacje o rodzaju usług, jakie będą świadczone przez podwykonawców* |
| 2. | Czy Podmiot Przetwarzający zamierza podpowierzyć dane osobowe podwykonawcom zgodnie z wymogami przewidzianymi przez RODO? |  |  |
| 3. | Czy Podmiot Przetwarzający zobowiązał podwykonawców do zapewnienia takich samych środków bezpieczeństwa, co Podmiot Przetwarzający? |  |  |
| 4. | Czy Podmiot Przetwarzający zamierza przekazywać powierzone mu dane osobowe dalszym podmiotom przetwarzającym poza Europejski Obszar Gospodarczy? |  | *Do jakich krajów spoza Europejskiego Obszaru Gospodarczego podmiot zamierza przekazywać dane osobowe i na jakiej podstawie prawnej, ewentualnie z zastosowaniem jakich zabezpieczeń?* |

|  |
| --- |
| **Bezpieczeństwo przetwarzania danych** |
| **Lp.** | **TREŚĆ PYTANIA** | **TAK/NIE** | **UWAGI** |
| 1. | Czy Podmiot Przetwarzający posiada wdrożony proces szacowania ryzyka naruszenia praw i wolności osób fizycznych (identyfikacja, analiza i ocena ryzyka)? |  |  |
| 2. | Czy Podmiot Przetwarzający przeprowadził analizę ryzyka naruszenia praw i wolności osób fizycznych dla czynności, w ramach których dojdzie do przetwarzania danych osobowych powierzonych mu przez Klienta? |  |  |
| 3. | Czy w oparciu o przeprowadzoną analizę ryzyka naruszenia praw i wolności osób fizycznych dla czynności, w ramach których dojdzie do przetwarzania danych osobowych powierzonych mu przez Klienta, Podmiot Przetwarzający oświadcza, że ryzyko jest niższe niż wysokie? |  |  |
| 4. | Czy Podmiot Przetwarzający zobowiązuje się informować Klienta w przypadku zmiany poziomu stwierdzonego ryzyka naruszenia praw i wolności osób fizycznych? |  |  |
| 5. | Czy Podmiot Przetwarzający zapewnia adekwatny do ryzyka naruszenia praw i wolności osób fizycznych poziom bezpieczeństwa powierzonych danych w szczególności zabezpieczający przed przypadkowym zniszczeniem, utratą, modyfikacją, nieuprawnionym ujawnieniem?  |  | *Proszę opisać* |
| 6. | Czy Podmiot Przetwarzający wdrożył adekwatne do ryzyka naruszenia praw i wolności osób fizycznych środki ochrony na wypadek awarii, takie jak plany awaryjne, środowiska zapasowe, kopie zapasowe, lub inne? |  | *Proszę opisać* |
| 7. | Czy Podmiot Przetwarzający przechodzi regularne audyty z zakresu bezpieczeństwa danych mające na celu ocenę skuteczności zastosowanych środków technicznych i organizacyjnych? |  | *Proszę wskazać częstotliwość* |

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

*(data wypełnienia formularza) (podpis osoby wypełniającej formularz)*

1. 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; dalej **RODO** [↑](#footnote-ref-1)