**Ankieta dotycząca informacji o technicznych i organizacyjnych zabezpieczeniach stosowanych przez Podmiot przetwarzający w celu zapewnienia odpowiedniego stopnia ochrony powierzanych przez Administratora danych osobowych.**

**Data wypełnienia ankiety:** …………………………………………………

**Cel ankiety:** Ankieta ma na celu sprawdzenie czy Wykonawca jako przyszły Podmiot przetwarzający gwarantuje zapewnienie odpowiednich środków technicznych i organizacyjnych aby przetwarzanie spełniało wymogi Ogólnego rozporządzenia o ochronie danych osobowych dalej jako „RODO” i chroniło prawa osób, których dane dotyczą.

**Dane Administratora:** Pomorska Kolej Metropolitalna S.A., ul. Budowlanych 77, 80-298 Gdańsk

**Dane Podmiotu przetwarzającego:** ………………………………………………………………………………………………………………………………………………………………………………………...

**Cel powierzenia przetwarzania danych osobowych:** ………………………………………….…………………………………………………………………………………………………………………..

| **Lp.** | **Pytanie** | **Odpowiedź (tak/nie/nie dotyczy)** | **Uwagi (dodatkowe informacje)** |  |
| --- | --- | --- | --- | --- |
|  | Czy zgodnie z art. 29 RODO osoby wykonujące operacje na danych osobowych otrzymały od podmiotu przetwarzającego upoważnienia do przetwarzania danych (w formie udokumentowanej), w których został określony w szczególności zakres przetwarzanych przez te osoby danych? |  |  |  |
|  | Czy podmiot przetwarzający prowadzi rejestr kategorii czynności przetwarzania zawierający wszystkie informacje wskazane w art. 30 ust. 2 RODO? |  |  |  |
|  | Czy podmiot przetwarzający posiada opracowaną i zatwierdzoną politykę ochrony danych osobowych lub inny dokument opisujący zasady i procedury ochrony danych osobowych obowiązujące w podmiocie?  **Jeśli TAK**, proszę załączyć skan 1 strony dokumentu i spisu treści. |  |  |  |
|  | Czy podmiot przetwarzający jest w stanie wykazać przestrzeganie przepisów o ochronie danych osobowych (m.in. RODO) m. in. poprzez przedstawienie obowiązujących w jego organizacji procedur i dokumentacji związanej z systemem ochrony danych osobowych (zasada rozliczalności)? |  |  |  |
|  | 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? |  |  |  |
|  | 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?  Kiedy przeprowadzono ostatnie okresowe szkolenie obejmujące ochronę danych osobowych? |  |  |  |
|  | Czy pracownicy podmiotu przetwarzającego, którzy uczestniczą w operacjach przetwarzania danych osobowych zostali zobowiązani do zachowania ich w tajemnicy? |  |  |  |
|  | Czy w ciągu dwóch ostatnich lat podmiot przetwarzający poddawał zewnętrznej kontroli niezależnych audytorów funkcjonujący w jego organizacji system ochrony danych osobowych?  **Jeśli Tak**, proszę podać datę ostatniego zewnętrznego audytu. |  |  |  |
|  | Czy zastosowano środki kontroli dostępu fizycznego do budynku/budynków tylko dla autoryzowanego personelu? |  |  |  |
|  | Czy zapewniono fizyczne oddzielenie środków przetwarzania informacji zarządzanych przez organizację od tych, które należą do innych organizacji? |  |  |  |
|  | Czy dostęp do pomieszczeń pozostających w dyspozycji podmiotu przetwarzającego po godzinach pracy nie jest możliwy dla osób trzecich (np. firma sprzątająca, ochrona), bądź dostęp ten jest szczegółowo nadzorowany, chroniony? |  |  |  |
|  | Czy pracownicy zostali zobowiązani do zabezpieczania nieużywanych w danym momencie systemów poprzez blokadę ekranu lub w inny równoważny sposób? |  |  |  |
|  | Czy zapewniono oprogramowanie antywirusowe na wszystkich stacjach komputerowych? |  |  |  |
|  | Czy stosowane oprogramowanie posiada licencję i jest na bieżąco aktualizowane? |  |  |  |
|  | Czy stosuje się szyfrowanie dysków komputerów przenośnych i innych przenośnych nośników danych? |  |  |  |
|  | Czy urządzenia mobilne posiadają skonfigurowaną kontrolę dostępu? |  |  |  |
|  | Czy wobec urządzeń mobilnych stosuje się techniki kryptograficzne? |  |  |  |
|  | Czy na urządzeniach mobilnych zainstalowano oprogramowania antywirusowe? |  |  |  |
|  | Czy zapewniono zdolności do szybkiego przywrócenia dostępności danych osobowych i dostępu do nich w razie incydentu fizycznego lub technicznego? |  |  |  |
|  | Jaki przyjęto zakres oraz częstotliwość tworzenia kopii zapasowych? |  |  |  |
|  | Gdzie są przechowywane kopie zapasowe? |  |  |  |
|  | Czy kopie zapasowe powierzonych danych osobowych są regularnie testowane w celu określenia skuteczności ich odzyskiwania?  **Jeśli Tak**, kiedy przeprowadzono ostatnie testy. |  |  |  |
|  | Czy organizacja posiada procedury odtwarzania systemu po awarii oraz ich testowania? |  |  |  |
|  | Czy zapewniono zdolności do szybkiego przywrócenia dostępności danych osobowych i dostępu do nich w razie incydentu fizycznego lub technicznego? |  |  |  |
|  | Czy podmiot przetwarzający wdraża nowe rozwiązania zgodnie z zasadą „privacy by design”? |  |  |  |
|  | Czy podmiot przetwarzający działa zgodnie z zasadą "privacy by default"? |  |  |  |
|  | Czy podmiot przetwarzający przeprowadził analizę ryzyka w zakresie świadczenia usług związanych z przyjęciem do przetwarzania powierzonych danych osobowych?  **Jeśli Tak**, proszę o podanie daty dokonania ostatniego przeglądu. |  |  |  |
|  | Czy podmiot przetwarzający przeprowadził ocenę skutków dla ochrony danych w związku z wykorzystywaniem systemu informatycznego do przetwarzania danych osobowych? |  |  |  |
|  | 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? |  |  |  |
|  | Czy podmiot przetwarzający świadczył już, co najmniej raz, podobne usługi jak w zamówieniu? I jeśli tak, to od jak dawna działa na rynku? |  |  |  |
|  | Czy podmiot przetwarzający regularnie dokonuje przeglądu stosowanych środków organizacyjnych i technicznych? **Jeśli Tak,** to kiedy ostatnio był dokonany taki przegląd? |  |  |  |
|  | Czy przeprowadzane są przeglądy uprawnień użytkowników do systemów informatycznych, w których znajdują się powierzone dane osobowe, a jeżeli tak, to jak często? |  |  |  |
|  | Czy podmiot przetwarzający powołał inspektora ochrony danych?  **Jeśli Tak,** to proszę o podanie danych kontaktowych (imię i nazwisko oraz nr telefonu lub adres e-mail) |  |  |  |
|  | Czy w ramach dostarczenia omawianej usługi podmiot przetwarzający będzie korzystał z usług innych podmiotów podprzetwarzających?  **Jeśli Tak**, to jakich i w jakim zakresie (proszę wskazać nazwę oraz dane kontaktowe podmiotu podprzetwarzającego)? |  |  |  |
|  | 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? |  |  |  |
|  | Jakie inne, niewymienione wcześniej techniczne i organizacyjne zabezpieczenia stosuje podmiot przetwarzający w celu odpowiedniego zabezpieczenia powierzonych danych osobowych?  Uwaga! Można załączyć wykaz stosowanych zabezpieczeń jako odrębny dokument. |  |  |  |
|  | Czy podmiot przetwarzający ma opracowane i wdrożone procedury i kanały komunikacyjne umożliwiające niezwłoczne zgłaszanie incydentów i naruszeń bezpieczeństwa dotyczących powierzonych danych osobowych? |  |  |  |
|  | Czy podmiot przetwarzający przekazuje dane poza obszar Europejskiego Obszaru Gospodarczego?  **Jeśli Tak**, czy podmiot przestrzega wymagania związane z przekazywaniem danych osobowych do krajów trzecich i organizacji międzynarodowych, o których mowa w rozdziale V RODO?. |  |  |  |
|  | Czy podmiot posiada wdrożone i certyfikowane normy ISO?  **Jeśli Tak**, proszę wskazać jakie. |  |  |  |
|  | Czy w ciągu ostatnich 2 lat miały zidentyfikowano w podmiocie przetwarzającym naruszenia ochrony danych osobowych?  Jeśli Tak, krótki opis czego dotyczyły, czy podlegały zgłoszeniu do Prezesa Urzędu Ochrony Danych Osobowych (UODO)? |  |  |  |
|  | Czy w ciągu ostatnich 2 lat były przeprowadzane kontrole, postępowania przez UODO?  **Jeśli Tak**, to czego dotyczyły? |  |  |  |

**Oświadczam, że podane w powyższej ankiecie informacje są zgodne z prawdą**

**UWAGA!!!**

**WYPEŁNIONY DOKUMENT NALEŻY PODPISAĆ KWALIFIKOWANYM PODPISEM ELEKTRONICZNYM, PODPISEM ZAUFANYM LUB PODPISEM OSOBISTYM (e-dowód)**

Podpis osoby reprezentującej Podmiot przetwarzający