**Załącznik nr 3a do SWZ**

**BZP.200.3.2023**

**Ankieta badania zgodności podmiotu z RODO**

**Informacja o zapewnieniu przez podmiot przetwarzający odpowiednich środków ochrony (technicznych i organizacyjnych), umożliwiających należyte zabezpieczenie danych osobowych, wymaganych art. 24 ust. 1 i 2 oraz art. 32 RODO**

|  |  |
| --- | --- |
| **Procesor:** |  |
| **Imię i nazwisko osoby wypełniającej ankietę** |  |
| **stanowisko** |  |
| **Adres e-mail i numer telefonu** |  |

|  | **Pytanie** | **Odpowiedzi:**  **TAK/NIE/ND** | **UWAGI** |
| --- | --- | --- | --- |
|  | Czy procesor wyznaczył osobę bądź osoby odpowiedzialne za zapewnienie przestrzegania przepisów dotyczących ochrony danych osobowych, np. inspektora ochrony danych zgodnie z art. 37 ust. 1 RODO? |  |  |
|  | Czy organ nadzorczy w zakresie przetwarzania danych osobowych prowadził wobec procesora postępowanie związane z podejrzeniem naruszenia przepisów o ochronie danych osobowych? |  |  |
|  | Czy pocesor podpowierza lub zamierza podpowierzać dane osobowe przetwarzane z polecenia administratora? Jeżeli tak, to w jakim zakresie? |  |  |
|  | Czy procesor planuje przetwarzać powierzone mu dane osobowe poza EOG? Jeżeli tak, to w których państwach i jakie mechanizmy legalizujące transfer są stosowane? |  |  |
|  | Czy dalsze podmioty przetwarzające, którym procesor planuje podpowierzyć dane, będą je przetwarzać poza EOG? Jeżeli tak, to w których państwach i jakie mechanizmy legalizujące transfer są stosowane? |  |  |
|  | Czy procesor wdrożył procedury obsługi incydentów, w tym związanych z ochroną danych osobowych? |  |  |
|  | Czy proces wyboru zabezpieczeń technicznych i organizacyjnych u Procesora oparty jest na wynikach szacowania ryzyka? |  |  |
|  | Czy procesor zapewnia możliwość realizacji wszystkich praw podmiotów danych przewidzianych w RODO? |  |  |
|  | Czy procesor stosuje się do norm, standardów lub wytycznych określających zasady bezpieczeństwa informacji, zarządzania usługami etc.? |  |  |
|  | Czy procesor prowadzi rejestr kategorii czynności przetwarzania zawierający wszystkie informacje wskazane w art. 30 ust. 2 RODO? |  |  |
|  | Czy procesor opracował i wdrożył dokumentację regulującą przetwarzanie danych osobowych? |  |  |
|  | Czy nowozatrudniony pracownik procesora przechodzi odpowiednie szkolenie w zakresie ochrony danych osobowych? |  |  |
|  | Czy procesor prowadzi bieżące szkolenia swoich pracowników dotyczące ochrony danych osobowych? |  |  |
|  | Czy osoby wykonujące operacje na danych osobowych otrzymały od procesora upoważnienia do przetwarzania tych danych? |  |  |
|  | Czy pracownicy procesora, którzy uczestniczą w operacjach przetwarzania danych osobowych zostali zobowiązani do zachowania ich w tajemnicy? |  |  |
|  | Jak często procesor poddaje audytowi funkcjonujący w jego organizacji system ochrony danych osobowych? |  |  |
|  | Czy procesor korzysta z usług tylko takich podmiotów zewnętrznych/podwykonawców, którzy zostali wcześniej przez niego sprawdzeni pod kątem zapewnienia odpowiedniego poziomu ochrony danych osobowych? |  |  |
|  | Czy w organizacji jest stosowana polityka tzw. „czystego biurka”? |  |  |
|  | Czy procesor stosuje zabezpieczenia kryptograficzne, pseudonimizację lub anonimizację przetwarzanych danych osobowych? |  |  |
|  | Czy procesor wykorzystuje oprogramowanie do ochrony stacji roboczych i serwerów przed złośliwym oprogramowaniem i innymi zagrożeniami? |  |  |
|  | Czy są stosowane polityki haseł? |  |  |
|  | Czy pracownicy zostali zobowiązani do zabezpieczania nieużywanych w danym momencie systemów poprzez blokadę ekranu lub w inny równoważny sposób? |  |  |
|  | Czy zastosowano środki kontroli dostępu fizycznego do budynku/budynków tylko dla autoryzowanego personelu? |  |  |
|  | Czy dostęp do pomieszczeń procesora po godzinach pracy nie jest możliwy dla osób trzecich (firma sprzątająca, ochrona), bądź dostęp ten jest szczegółowo nadzorowany? |  |  |
|  | Czy procesor stosuje system monitoringu wizyjnego? |  |  |
|  | Czy procesor posiada zapasowe centrum przetwarzania danych? |  |  |
|  | Czy procesor posiada plan utrzymania ciągłości działania? |  |  |
|  | Czy procesor posiada plany awaryjne i odtworzeniowe komponentów/systemów IT? |  |  |
|  | Czy procesor przeprowadza regularne testy ciągłości działania? |  |  |
|  | Czy procesor wyznaczył osobę odpowiedzialną za obszar ciągłości działania? |  |  |
|  | Jak często procesor przeprowadza testy bezpieczeństwa infrastruktury teleinformatycznej (testy penetracyjne i testy podatności)? |  |  |
|  | Czy procesor wykorzystuje system IPS/IDS? |  |  |
|  | Czy procesor wykorzystuje system DLP (Data Leakage Prevention)? |  |  |
|  | Czy procesor wykorzystuje system służący do centralnego gromadzenia, analizowania i korelowania danych o zdarzeniach, podatnościach i incydentach klasy SIEM (np. QRadar Q1 Labs, NetIQ Security Manager, Check Point Eventia, TriGeo SIM, eIQ Networks SecureVue)? |  |  |

...........................................................................

(podpis podmiotu przetwarzającego)