Załącznik nr 7

OŚWIADCZENIE

o wdrożeniu minimalnych środków technicznych i organizacyjnych w przypadku powierzenia do przetwarzania danych osobowych

Nazwa Postępowania:	
Dostawa, montaż i uruchomienie Systemu Kontroli Dostępu	
Nr Postępowania:	**022/EW23/2025**

1. Uwzględniając charakter, zakres, kontekst i cele przetwarzania oraz ryzyko naruszenia praw lub wolności osób fizycznych o różnym prawdopodobieństwie i wadze zagrożenia Podmiot Przetwarzający zobowiązany jest do:
   - ✓ zapewnienia przetwarzania danych na zasadach określonych w art. 5 RODO;
   - ✓ zapewnia legalności przetwarzana danych zgodnie z art. 6–11 RODO;
   - ✓ zapewnia, przestrzegania danych osób których dane dotyczą zgodnie z art. 12-23 RODO;
   - ✓ zapewnia wypełniania obowiązków w zakresie przetwarzania danych ciążących na podstawie art. 24-31 RODO;
   - ✓ zapewnia bezpieczeństwa przetwarzania danych zgodnie z art. 32-36 RODO;
   - ✓ spełnienia wymagań w zakresie przekazywania danych do państw trzecich i instytucji międzynarodowych zgodnie z art. 44–49 RODO, jeśli taka potrzeba zaistnieje.
2. Podmiot Przetwarzający zobligowany jest do wdrążenia odpowiednich środków technicznych i organizacyjnych w szczególności do:
   - ✓ przeszkolenia wszystkich osób zatrudnionych przy przetwarzaniu danych, w tym zabezpieczeń systemów informatycznych;
   - ✓ nadania upoważnienia pracownikom dopuszczonym do przetwarzania danych osobowych;
   - ✓ zobligowaniu pracowników do zachowania w tajemnicy przetwarzanych danych osobowych oraz sposobu ich zabezpieczenia;
   - ✓ określeniu obszaru, w którym dane osobowe są przetwarzane i doboru odpowiednich zabezpieczeń uniemożliwiających dostęp osób nieupoważnionym.
   - ✓ zapewnienie spełnienia wymogów zasady „Czystego ekranu” i „Zasady czystego biurka” przed dostępem osób nieupoważnionych;
   - ✓ określenia zasad bezpieczeństwa dla dokumentów tradycyjnych i przetwarzanych na urządzeniach mobilnych (w tym szyfrowanie dysków) przetwarzających dane osobowe poza siedzibą Podmiotu Przetwarzającego;
   - ✓ wprowadzenie indywidualnych mechanizmów uwierzytelniania wszystkim pracownikom przetwarzających dane osobowe w systemach informatycznych i ich systematycznego zmieniania oraz nikomu ich nieudostępniania;

- ✓ wszystkie dokumenty zawierające dane osobowe przesyłane drogą elektroniczną powinny być zaszyfrowane. Hasło do dokumentu powinno być przekazane innym kanałem niż przekazany został dokument (np. smsem);
- ✓ stosować ochronę firewall w sytuacji, kiedy system informatyczny połączony jest z siecią publiczną;
- ✓ zainstalowania oprogramowania antywirusowego i systematyczne jego aktualizowanie;
- ✓ wykonywanie systematyczne kopi zapasowych systemów informatycznych. Zabronione jest przechowywanie kopi zapasowych w tym samym miejscu, gdzie znajdują się dane źródłowe. Po zrealizowaniu celu lub okresu przechowywania danych kopie zapasowe powinny być trwale usuwane;
- ✓ używanie wyłącznie firmowych komputerów oraz korzystanie tylko z firmowych skrzynek emaliowych odpowiednio zabezpieczonych przy przetwarzaniu danych osobowych;
- ✓ stosowania animizacji danych osobowych – polegający na takim przekształceniu danych osobowych, po którym nie można (w rozsądnym wymiarze czasowym) już przyporządkować poszczególnych informacji osobistych lub rzeczowych do zidentyfikowania osoby fizycznej. Proces anonimizacji musi być trwały i nieodwracalny.

Oświadczenie:

Oświadczam, że jako ubiegający się o udzielenie zamówienia wdrożyłem odpowiednie środki techniczne i organizacyjne zapewniające bezpieczne przetwarzanie powierzonych danych w przypadku wystąpienia potrzeby powierzenia danych osobowych przez Zamawiającego zgodnie z art. 28 ust. 3. 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,

miejscowość i data	Pieczęć imienna i podpis przedstawiciela(i) Wykonawcy