**Załącznik nr 9 do zapytania ofertowego**

**WYMAGANIA DLA PODMIOTÓW PRZETWARZAJĄCYCH –**

**ANKIETA DLA MUZEUM ZAMKOWEGO W MALBORKU**

**……………………………………………………………………………………………………………………….………….**

**Dane podmiotu przetwarzającego (procesora)**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Lp.** | **Wymóg dla podmiotu przetwarzającego**  **PODMIOT PRZETWARZAJĄCY (POTENCJALNY WYKONAWCA/KONTRAHENT):** | **TAK** | **NIE** | **UWAGI** |
| 1 | Posiada wdrożoną *Politykę ochrony danych osobowych* lub inne akty wewnętrzne określające zasady ochrony danych osobowych, informowania Administratora  o naruszeniach ochrony danych osobowych, realizacji praw podmiotów danych |  |  |  |
| 2 | Osoby upoważnione do przetwarzania danych zobowiązane są do zachowania tajemnicy lub podlegają odpowiedniemu ustawowemu obowiązkowi zachowania tajemnicy |  |  |  |
| 3 | Zapewnienia bezpieczeństwo danych poprzez wdrożone adekwatne środki techniczne i organizacyjne, np.: szyfrowanie, regularne testowanie, mierzenie i ocenianie skuteczności środków technicznych i organizacyjnych mających zapewnić bezpieczeństwo danych |  |  |  |
| 4 | Zapewnienia regularne (co najmniej raz na rok) testowanie, mierzenie i ocenianie skuteczności środków technicznych i organizacyjnych mających zapewnić bezpieczeństwo przetwarzania |  |  |  |
| 5 | Posiada wdrożoną procedurę zarządzania ryzykiem |  |  |  |
| 6 | Posiada wdrożoną procedurę w zakresie reagowania na incydenty związane z naruszeniami ochrony danych |  |  |  |
| 7 | Stosuje zatwierdzone kodeksy postępowania |  |  |  |
| 8 | Posiada certyfikat w zakresie ochrony danych osobowych |  |  |  |
| 9 | Posiada aktualne oprogramowania, zarówno użytkowe jak i systemowe, z wysokim poziomem odporności na cyberataki |  |  |  |
| 10 | Zabezpiecza posiadane sieci komputerowe, zarówno przewodowe jak i bezprzewodowe, poprzez odpowiednią konfigurację urządzeń i systemów umożliwiającą blokowanie podejrzanej transmisji danych |  |  |  |
| 11 | Zarządza dostępem zarówno do pomieszczeń jak i do systemów oraz programów komputerowych poprzez audytowalny proces nadawania, przeglądu i odbierania uprawnień oraz stosowanie bezpiecznych mechanizmów uwierzytelniania |  |  |  |
| 12 | Używa silnego szyfrowania danych na urządzeniach przenośnych (takich jak laptopy czy smartfony) i pamięciach zewnętrznych (np. karty SD) a także silnego szyfrowania komunikacji odbywającej się przy pomocy sieci zewnętrznej Internet, o ile przenoszone lub przesyłane są dane osobowe, w których posiadanie podmiot przetwarzający wejdzie podczas realizacji powierzonych czynności |  |  |  |
| 13 | Przechowuje kopie bezpieczeństwa posiadanych informacji w bezpiecznej lokalizacji i zabezpiecza je przed nieautoryzowanym dostępem |  |  |  |
| 14 | Zapewnia kontrolowany sposób wprowadzania zmian w środowisku administratora, poprzedzony formalnym procesem testowym |  |  |  |
| 15 | Zapewnienia kontrolowany sposób zarządzania cyklem życia informacji zarówno w formie elektronicznej jak i trwałej, w szczególności jej bezpieczne pozyskiwanie, przetwarzanie, przechowywanie i usuwanie |  |  |  |
| 16 | Zapewnia nadzór nad osobami niebędącymi pracownikami podmiotu przetwarzającego,  a przebywającymi w jego siedzibie, wykluczający ich dostęp do danych osobowych |  |  |  |
| 17 | Przestrzega warunków korzystania z usług innych podmiotów przetwarzających |  |  |  |

………………………………………………… …………………………………………………

Data czytelny podpis

za podmiot przetwarzający (procesora)

*Ankieta ta pomaga administratorowi danych w ocenie, czy podmiot przetwarzający spełnia wszystkie wymogi dotyczące ochrony danych osobowych zgodnie z art. 28 RODO oraz czy może być odpowiednim partnerem do powierzenia przetwarzania danych.*