

## WNIOSEK DO PODMIOTU PRZETWARZAJĄCEGO

Szanowni Państwo,

Realizując zapisy RODO Państwowe Muzeum Etnograficzne w Warszawie dąży do zwiększenia poziomu ochrony danych osobowych, a tym samym zgodnie z art. 28 RODO oczekuje od podmiotów, którym powierza do przetwarzania dane zapewnienia:

- 1) o wdrożeniu odpowiednich środków zabezpieczających powierzone dane osobowe,
- 2) zgodności procesów przetwarzania danych osobowych z obowiązującym prawem.

Zgodnie z uprawnieniem wynikającym z RODO załączam listę pytań w sprawie gwarancji wdrożenia odpowiedniego poziomu zabezpieczenia powierzonych danych osobowych.

Bardzo proszę o udzielenie możliwie wyczerpujących odpowiedzi.

Odpowiedzi proszę odesłać do dnia **18.12.2023 r. godz. 10.00**

Warszawa, dn. 12.12.2023 r.

.....  
*W imieniu Administratora*

---

**RODO** – 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.

**Administrator** – osoba fizyczna lub prawna, organ publiczny, jednostka lub inny podmiot, który samodzielnie lub wspólnie z innymi ustala cele i sposoby przetwarzania danych osobowych (PMW w Warszawie).

**Podmiot przetwarzający** – osoba fizyczna lub prawna, organ publiczny, jednostka lub inny podmiot, który przetwarza dane osobowe w imieniu Administratora, czyli działa na jego zlecenie (YYY).

**Inspektor ochrony danych** – IOD to osoba wyznaczona przez administratora lub podmiot przetwarzający, posiadająca kwalifikacje zawodowe, a w szczególności wiedzę fachową na temat prawa i praktyk w dziedzinie ochrony danych osobowych oraz umiejętności wypełniania zadań wynikających z zapisów RODO.

## LISTA PYTAŃ DO PODMIOTU PRZETWARZAJĄCEGO

1. Czy Podmiot przetwarzający podjął działania, aby przetwarzanie danych osobowych odpowiadało wymogom RODO?

2. Od kiedy w Podmiocie przetwarzającym funkcjonuje system ochrony danych zgodny z RODO?

3. Czy Podmiot przetwarzający wyznaczył IOD - Inspektora ochrony danych (art. 37 RODO)?

**Jeśli tak**, to czy IOD został wyznaczony po uprzedniej weryfikacji, czy kandydat spełnia wszelkie niezbędne warunki do pełnienia tej funkcji?

**Jeśli nie**, to czy Podmiot przetwarzający dokonał oceny konieczności lub braku konieczności powołania IOD z uwzględnieniem specyfiki działania i zakresu przetwarzania danych przez Podmiot przetwarzający?

Czy podmiot przetwarzający wyznaczył koordynatora lub inną osobę nadzorującą przestrzeganie przepisów o ochronie danych osobowych w podmiocie?

4. Czy pracownicy dopuszczeni do przetwarzania danych dokonują przetwarzania na udokumentowane polecenie Podmiotu przetwarzającego (art. 29 RODO)?

5. Czy pracownicy dopuszczeni do przetwarzania danych osobowych zostali zobowiązani do zachowania tych danych w tajemnicy?

6. Czy prowadzona jest ewidencja osób upoważnionych?

7. Czy osoby upoważnione do przetwarzania danych zostały zaznajomione z aktualnymi przepisami prawa o ochronie danych osobowych? Czy odbyły szkolenia, kursy, uczestniczyły w warsztatach praktycznych? Kiedy odbyło się ostatnie szkolenie?

8. Czy Podmiot przetwarzający wdrożył odpowiednie polityki ochrony danych (art. 24 RODO)? Jeśli tak, jakie?

9. Czy Podmiot przetwarzający opracował procedurę nadzoru i rejestrowania naruszeń bezpieczeństwa danych osobowych (art. 33 RODO)?

**10. Czy Podmiot przetwarzający prowadzi „Rejestr czynności przetwarzania” i „Rejestr kategorii czynności przetwarzania” (art. 30 RODO)?**

**11. Czy Podmiot przetwarzający dokonał analizy ryzyka i zagrożeń w celu wdrożenia odpowiednich środków technicznych i organizacyjnych, aby zapewnić bezpieczeństwo przetwarzanym danym? (art. 32 RODO)**

**12. Jakie środki fizyczne wdrożył Podmiot przetwarzający, aby zapewnić bezpieczeństwo i poufność przetwarzanym danym?**

**13. Jakie środki organizacyjne wprowadził Podmiot przetwarzający w celu zapewnienia przejrzystych reguł stosowania przepisów o ochronie danych osobowych?**

**14. Jakie środki techniczne wdrożył Podmiot przetwarzający, aby zapewnić bezpieczne przetwarzanie danych z użyciem systemów informatycznych?**

**15. Czy do przetwarzania powierzonych danych Podmiot przetwarzający korzysta z usług innych podmiotów (czy dochodzi do podpowierzenia danych)?**

**16. Czy powierzone do przetwarzania dane będą przetwarzane (z uwzględnieniem ewentualnego podpowierzenia) poza terenem Unii Europejskiej?**

**17. Czy Podmiot przetwarzający wdrożył normy (np. ISO, AEO), kodeksy dobrych praktyk lub stara się o uzyskanie certyfikatów potwierdzających zgodność przetwarzania danych z RODO?**

**18. Czy podmiot przetwarzający posiada polisy ubezpieczeniowe?**

**19. Czy Podmiot przetwarzający podejmuje systematyczne działania w celu monitorowania zgodności przetwarzania danych z aktualnymi przepisami? Np. zleca regularne audyty, korzysta z usług firmy doradczej?**

.....  
*miejsowość, data*

.....  
*pieczętka i podpis osoby działającej  
w imieniu Podmiotu przetwarzającego*