



POLITYKA

OCHRONY DANYCH W MUZEUM ZIEMI PISKIEJ

POLITYKA OCHRONY DANYCH W MUZEUM ZIEMI PISKIEJ

I. Postanowienia ogólne

1. Politykę Ochrony Danych w Muzeum Ziemi Piskiej wprowadza się w celu wdrożenia i przestrzegania ochrony osób fizycznych w związku z przetwarzaniem danych osobowych w zakresie określonym w:
 - a) Rozporządzeniu Parlamentu Europejskiego i Rady Unii Europejskiej nr 2016/679 z dnia 27.04.2016 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 - ogólne rozporządzenie o ochronie danych (Dz.Urz. UE L 119 z 04.05.2016);
 - b) Ustawie z dnia 10.05.2018 r. o ochronie danych osobowych (Dz.U. 2018 poz. 1000 z późn. zmianami);
 - c) Ustawie z dnia 21.02.2019 r. o zmianie niektórych ustaw w związku z zapewnieniem stosowania 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 (ogólne rozporządzenie o ochronie danych) (Dz.U. 2019 poz. 730);
 - d) Rozporządzeniu Prezesa Rady Ministrów z dnia 31.05.2019 r. w sprawie trybu i sposobu realizacji zadań przez inspektora ochrony danych (Dz.U. 2019 poz. 1041);
 - e) Innych obowiązujących aktach prawnych.
2. Polityka dotyczy wszystkich danych osobowych przetwarzanych w
Muzeum Ziemi Piskiej
NIP: 8491027365;
Regon: 001391497
Siedziba: 12-200 Pisz, Pl. Daszyńskiego 7
niezależnie od formy ich przetwarzania (przetwarzane tradycyjnie zbiory ewidencyjne, systemy informatyczne) oraz od tego, czy dane są lub mogą być przetwarzane w zbiorach danych.
3. Dokument **"Polityka Ochrony Danych w Muzeum Ziemi Piskiej"** jest przechowywany w wersji papierowej w siedzibie Administratora oraz publikowany na stronie internetowej Muzeum.
4. Administratorem Danych Osobowych ADO, **jest Dyrektor Muzeum Ziemi Piskiej – dr Aneta Karwowska.**
5. Administrator Danych Osobowych zgodnie z art. 37 Rozporządzenia Parlamentu Europejskiego i Rady Unii Europejskiej Numer 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 - ogólne rozporządzenie o ochronie danych (Dz. Urz. UE L 119 z 04.05.2016) zwanego w dalszej treści „RODO” wyznacza:
Inspektora Danych Osobowych IOD - pana Robert Polita.
6. Inspektor Ochrony Danych – IOD zostaje powołany w celu:
 - a) informowania, doradzania i rekomendowania określonych działań Administratorowi lub podmiotowi przetwarzającemu,
 - b) realizowania obowiązków informacyjnych,
 - c) monitorowania przestrzegania przepisów prawa - identyfikacji i analizy procesów przetwarzania,

- d) szacowania ryzyka związanego z operacjami przetwarzania z uwzględnieniem charakteru, zakresu i kontekstu celów przetwarzania,
 - e) współpracy z organem nadzorczym i pełnienia funkcji punktu kontaktowego dla organu nadzorczego,
 - f) stałego nadzoru bezpieczeństwa przetwarzania danych osobowych wewnątrz organizacji,
 - g) przeprowadzania szkoleń dla osób zatrudnionych oraz dbania o właściwy poziom wiedzy w obszarze ochrony danych osobowych.
7. Inspektor Ochrony Danych (IOD) jest punktem kontaktowym, z którym możesz się skontaktować w sprawach ochrony swoich danych osobowych i realizacji przysługujących Ci uprawnień.
- Z Inspektorem Ochrony Danych możesz skontaktować się w jeden z poniższych sposobów:
- listownie: IOD Muzeum Ziemi Piskiej, Plac Daszyńskiego 7, 12-200 Pisz;
e-mail: mzppisz@wp.pl (w temacie wiadomości proszę wpisać „Sprawy IOD”)
8. Polityka Ochrony Danych w Muzeum Ziemi Piskiej jest udostępniana do wglądu wszystkim pracownikom (w formie tradycyjnej papierowej) oraz osobom odwiedzającym Muzeum (w formie cyfrowej na stronie internetowej Muzeum) celem zapoznania się z jej treścią.
9. Dla skutecznej realizacji Polityki Ochrony Danych w Muzeum Ziemi Piskiej Administrator Danych Osobowych zapewnia:
- a) odpowiednie do zagrożeń i kategorii danych objętych ochroną środki techniczne i rozwiązania organizacyjne,
 - b) kontrolę i nadzór nad przetwarzaniem danych osobowych,
 - c) monitorowanie zastosowanych środków ochrony.
10. Monitorowanie przez Administratora Danych Osobowych zastosowanych środków ochrony obejmuje m.in.:
- a) działania pracowników i gości Muzeum,
 - b) naruszanie zasad dostępu do danych osobowych,
 - c) zapewnienie integralności plików oraz ochronę przed atakami zewnętrznymi oraz wewnętrznymi.
11. Administrator Danych Osobowych zapewnia, że czynności wykonywane w związku z przetwarzaniem i zabezpieczeniem danych osobowych są zgodne z niniejszą polityką oraz odpowiednimi przepisami prawa.

II. Dane osobowe przetwarzane u administratora danych

1. Dane osobowe przetwarzane przez Administratora Danych Osobowych gromadzone są w zbiorach danych.
2. Administrator Danych Osobowych nie podejmuje czynności przetwarzania, które mogłyby się wiązać z poważnym prawdopodobieństwem wystąpienia wysokiego ryzyka dla praw i wolności osób. W przypadku planowania takiego działania Administrator Danych Osobowych dokona zgodnie z art. 35 i następnymi RODO oceny skutków dla ochrony danych.
3. W przypadku planowania nowych czynności przetwarzania Administrator Danych Osobowych dokonuje analizy ich skutków dla ochrony danych osobowych oraz uwzględnia kwestie ochrony danych w fazie ich projektowania.
4. Administrator danych prowadzi Rejestr Czynności Przetwarzania.

III. Obowiązki i odpowiedzialność w zakresie zarządzania bezpieczeństwem danych osobowych

1. Wszystkie osoby zatrudnione w Muzeum Ziemi Piskiej zobowiązane są do przetwarzania danych osobowych zgodnie z obowiązującymi przepisami i zgodnie z ustaloną przez Administratora Danych Osobowych polityką ochrony danych, a także innymi dokumentami wewnętrznymi i procedurami związanymi z przetwarzaniem danych osobowych w Muzeum.
2. Wszystkie dane osobowe przetwarzane są w Muzeum z poszanowaniem zasad przetwarzania przewidzianych przez przepisy prawa:
 - a) w każdym wypadku występuje chociaż jedna z przewidzianych przepisami prawa podstaw dla przetwarzania danych osobowych,
 - b) dane osobowe przetwarzane są rzetelnie i w sposób przejrzysty,
 - c) dane osobowe zbierane są w konkretnych, wyraźnych i prawnie uzasadnionych celach i nieprzetwarzane dalej w sposób niezgodny z tymi celami,
 - d) dane osobowe są przetwarzane jedynie w takim zakresie, jaki jest niezbędny dla osiągnięcia celu przetwarzania danych,
 - e) dane osobowe są prawidłowe i w razie potrzeby uaktualniane,
 - f) czas przechowywania danych osobowych jest ograniczony do okresu ich przydatności do celów, do których zostały zebrane, a po tym okresie są one anonimizowane bądź usuwane,
 - g) wobec osoby, której dane osobowe dotyczą, wykonywany jest obowiązek informacyjny zgodnie z treścią art. 13 i 14 RODO,
 - h) dane osobowe są zabezpieczone przed naruszeniami zasad ich ochrony.
3. Administrator Danych Osobowych zgodnie z art. 14 ust 5 pkt. d RODO nie przekazuje osobom, których dane osobowe dotyczą, informacji w sytuacji, w której dane osobowe te muszą zostać poufne zgodnie z obowiązkiem zachowania tajemnicy.
4. Za naruszenie lub próbę naruszenia zasad przetwarzania i ochrony danych osobowych uważa się w szczególności:
 - a) naruszenie bezpieczeństwa Systemów Informatycznych, w których przetwarzane są dane osobowe, w razie ich przetwarzania w takich systemach,
 - b) udostępnianie lub umożliwienie udostępniania danych osobowych osobom lub podmiotom do tego nieupoważnionym,
 - c) zaniechanie, choćby nieumyślne, dopełnienia obowiązku zapewnienia ochrony danym osobowym,
 - d) niedopełnienie obowiązku zachowania w tajemnicy danych osobowych oraz sposobów ich zabezpieczenia,
 - e) przetwarzanie danych osobowych niezgodnie z założonym zakresem i celem ich zbierania,
 - f) spowodowanie uszkodzenia, utraty, niekontrolowanej zmiany lub nieuprawnione kopiowanie danych osobowych,
 - g) naruszenie praw osób, których dane osobowe są przetwarzane.
5. W przypadku stwierdzenia okoliczności naruszenia zasad ochrony danych osobowych każdy pracownik Muzeum zobowiązany jest do podjęcia wszystkich niezbędnych kroków, mających na celu ograniczenie skutków naruszenia i do niezwłocznego powiadomienia Inspektora Ochrony Danych Osobowych i Administratora Danych Osobowych.
6. Administrator Danych Osobowych w zakresie zatrudniania, zakończenia lub zmiany warunków zatrudnienia pracowników lub współpracowników (w tym osób podejmujących czynności na rzecz Administratora Danych Osobowych na podstawie innych umów cywilnoprawnych) jest zobowiązany do dopilnowania, aby:
 - a) pracownicy byli odpowiednio przeszkoleni i przygotowani do wykonywania swoich obowiązków,

- b) każdy z przetwarzających dane osobowe był pisemnie upoważniony do przetwarzania zgodnie z „Upoważnieniem do przetwarzania danych osobowych”,
 - c) każdy pracownik przetwarzający dane zobowiązał się poprzez złożenie „Oświadczenia osoby przetwarzającej dane osobowe” do zachowania danych osobowych przetwarzanych w Muzeum w tajemnicy.
7. Pracownicy Muzeum zobowiązani są, pod rygorem kar dyscyplinarnych, do:
- a) ścisłego przestrzegania zakresu nadanego upoważnienia,
 - b) przetwarzania i ochrony danych osobowych zgodnie z przepisami,
 - c) zachowania w tajemnicy danych osobowych oraz sposobów ich zabezpieczenia,
 - d) zgłaszania incydentów związanych z naruszeniem bezpieczeństwa danych oraz niewłaściwym funkcjonowaniem systemu.

IV. Obszar przetwarzania danych osobowych

1. Obszar, w którym przetwarzane są dane osobowe obejmuje wszystkie pomieszczenia Muzeum Ziemi Piskiej zlokalizowane w 12-200 Pisz Pl. Daszyńskiego 7.
2. Dodatkowo obszar, w którym przetwarzane są dane osobowe, stanowią wszystkie komputery przenośne oraz inne nośniki danych znajdujące się poza obszarem wskazanym powyżej.

V. Określenie środków technicznych i organizacyjnych niezbędnych dla zapewnienia poufności, integralności i rozliczalności przetwarzanych danych

1. Administratora Danych Osobowych zapewnia zastosowanie środków technicznych i organizacyjnych niezbędnych dla zapewnienia poufności, integralności, rozliczalności i ciągłości przetwarzanych danych.
2. Zastosowane środki ochrony (techniczne i organizacyjne) powinny być adekwatne do stwierdzonego poziomu ryzyka dla poszczególnych systemów, rodzajów zbiorów i kategorii danych.

Środki te obejmują:

- a) ograniczenie dostępu do pomieszczeń, w których przetwarzane są dane osobowe, jedynie do osób odpowiednio upoważnionych. Inne osoby mogą przebywać w pomieszczeniach wykorzystywanych do przetwarzania danych jedynie w towarzystwie osoby upoważnionej,
- b) zamykanie pomieszczeń tworzących obszar przetwarzania danych osobowych określony w pkt. IV Polityki na czas nieobecności pracowników, w sposób uniemożliwiający dostęp do nich osób trzecich,
- c) wykorzystanie zamykanych szafek lub sejfów do zabezpieczenia dokumentów obejmujących dane osobowe,
- d) przetwarzanie zbiorów danych osobowych wyłącznie na autoryzowanym służbowym sprzęcie informatycznym Muzeum,
- e) wyposażenie stacji roboczych w indywidualną ochronę antywirusową,
- f) dostęp do systemu operacyjnego stacji roboczej, w którym przetwarzane są dane osobowe za pomocą procesu uwierzytelnienia z wykorzystaniem hasła,
- g) przechowywanie kopii zapasowych/archiwalnych zbioru danych osobowych w zamkniętej metalowej szafie,
- h) wykorzystanie „mechanicznej niszczarki dokumentów do skutecznego usuwania dokumentów zawierających dane osobowe,
- i) ochronę sieci lokalnej przed działaniami inicjowanymi z zewnątrz przy użyciu programów typu firewall,
- j) wykonywanie kopii awaryjnych danych na dedykowanym nośniku cyfrowym,

- k) ochronę sprzętu komputerowego wykorzystywanego u Administratora Danych Osobowych przed złośliwym oprogramowaniem,
- l) zabezpieczenie dostępu do urządzeń Muzeum przy pomocy haseł dostępu,
- m) wykorzystanie szyfrowania danych przy ich transmisji.

VI. Naruszenia zasad ochrony danych osobowych

1. W przypadku stwierdzenia naruszenia zasad ochrony danych osobowych Administrator Danych Osobowych wraz z Inspektorem Ochrony Danych dokonuje oceny, czy zaistniałe naruszenie mogło powodować ryzyko naruszenia praw lub wolności osób fizycznych.
2. W każdej sytuacji, w której zaistniałe naruszenie mogło powodować ryzyko naruszenia praw lub wolności osób fizycznych, Administrator Danych Osobowych poprzez Inspektora Ochrony Danych zgłasza fakt naruszenia zasad ochrony danych organowi nadzorczemu – Prezesowi Urzędu Ochrony Danych Osobowych, bez zbędnej zwłoki i nie później niż w terminie 72 godzin po stwierdzeniu naruszenia.
3. Jeżeli ryzyko naruszenia praw i wolności jest wysokie, Administrator Danych Osobowych poprzez Inspektora Ochrony Danych zawiadamia o incydencie także osobę, której dane dotyczą.

VII. Powierzenie przetwarzania danych osobowych

1. Administrator Danych Osobowych może powierzyć przetwarzanie danych osobowych innemu podmiotowi wyłącznie w drodze umowy zawartej w formie pisemnej, zgodnie z wymogami wskazanymi dla takich umów w art. 28 RODO i tylko jeżeli są to dane, które może ujawnić bez naruszenia tajemnicy służbowej.
2. Przed powierzeniem przetwarzania danych osobowych Administrator Danych Osobowych w miarę możliwości uzyska informacje o dotychczasowych praktykach procesora (podmiotu, któremu powierzone zostaną dane) dotyczących zabezpieczenia danych osobowych.

VIII. Monitoring wizyjny

1. Administrator Danych Osobowych może prowadzić monitoring wizyjny Closed-Circuit TeleVision CCTV w pomieszczeniach Muzeum. Celem prowadzenia monitoringu CCTV jest zapewnienie bezpieczeństwa pracownikom i ochrony mienia. Stała obserwacja obiektu prowadzona jest w związku z prawnie uzasadnionym interesem realizowanym przez administratora (RODO art. 6 ust. 1 lit. f). Wizerunek pracowników i gości Muzeum nie jest wykorzystywany do innych celów niż wskazane powyżej. Miejsca objęte monitoringiem CCTV są czytelnie i jednoznacznie oznakowane.
2. Dane osobowe pozyskane z monitoringu będą przechowywane przez okres 30 dni od dnia nagrania, po czym zostaną trwale zniszczone.

IX. Przekazywanie danych do państwa trzeciego

1. Administrator Danych Osobowych co do zasady nie będzie przekazywał danych osobowych do państwa trzeciego.
2. W przypadku wystąpienia konieczności przekazania danych osobowych do państwa trzeciego Administrator Danych Osobowych wykona to tylko i wyłącznie za zgodą osoby, której dane dotyczą.

X. Szkolenie

1. Każdy użytkownik przed dopuszczeniem do pracy w systemie przetwarzającym dane osobowe lub zbiory danych osobowych w wersji cyfrowej i/lub papierowej powinien odbyć przeszkolenie w zakresie ochrony danych osobowych w zbiorach elektronicznych i papierowych.
2. Za przeprowadzenie szkolenia odpowiada Administrator Danych Osobowych.

3. Szkolenie obejmuje swoim zakresem zapoznanie użytkownika z:
 - a. przepisami prawa o ochronie danych osobowych oraz wydanymi na jej podstawie aktami wykonawczymi;
 - b. zasadami przetwarzania danych osobowych w Muzeum Ziemi Piskiej;
 - c. strukturą i zasadami użytkowania systemu informatycznego służącego do przetwarzania danych osobowych;
4. Szkolenie powinno zakończyć się wydaniem przez Administratora upoważnienia do przetwarzania danych osobowych dla osoby szkolonej i przyjęciem od niej Oświadczenia osoby przetwarzającej dane osobowe. Oba dokumenty powinny być zarchiwizowane w Teczce Akt Personalnych pracownika.

XI. Postanowienia końcowe

1. Za niedopełnienie obowiązków wynikających z niniejszej Polityki pracownik ponosi odpowiedzialność na podstawie Kodeksu Pracy, Przepisów o Ochronie Danych Osobowych oraz Kodeksu Karnego w odniesieniu do danych osobowych objętych tajemnicą zawodową.
2. Integralną część niniejszej Polityki bezpieczeństwa stanowią następujące dokumenty:
 - Wykaz pracowników zapoznanych z polityką bezpieczeństwa ochrony danych osobowych.
 - Rejestr czynności przetwarzania danych osobowych.
 - Umowy powierzenia przetwarzania danych osobowych (w przypadku powierzania).
 - Rejestr upoważnień do przetwarzania danych osobowych w Muzeum Ziemi Piskiej.
 - Upoważnienia do przetwarzania danych osobowych.
 - Oświadczenia osoby przetwarzającej dane osobowe.
 - Klauzula informacyjna dla pracowników Muzeum.
 - Klauzula informacyjna dla gości zwiedzających oraz uczestników imprez odbywających się na terenie Muzeum Ziemi Piskiej
 - Klauzula informacyjna dotycząca monitoringu wizyjnego w Muzeum Ziemi Piskiej.
 - Zasady przetwarzania danych osobowych.
 - Procedura zgłoszenia naruszenia ochrony danych.
 - Rejestr naruszeń ochrony danych osobowych.

.....
Dyrektor Muzeum

WYKAZ PRACOWNIKÓW ZAPOZNANYCH Z POLITYKĄ BEZPIECZEŃSTWA OCHRONY DANYCH OSOBOWYCH

Ja niżej podpisany własnoręcznym podpisem potwierdzam fakt zapoznania się z „Polityką Bezpieczeństwa Ochrony Danych Osobowych w Muzeum Ziemi Piskiej”.

Lp.	Imię i nazwisko	Podpis
1.		
2.		
3.		
4.		
5.		
6.		
7.		
8.		
9.		
10.		
11.		
12.		
13.		
14.		
15.		
16.		
17.		
18.		
19.		
20.		
21.		

Lp.	Imię i nazwisko	Podpis
22.		
23.		
24.		
25.		
26.		
27.		
28.		
29.		
30.		
31.		
32.		
33.		
34.		
35.		
36.		
37.		
38.		
39.		
40.		
41.		
42.		
43.		
44.		
45.		