GMINNY OŚRODEK KULTURY
SPORTU I REKREACJI
ul. REKREACYJNA 1, 72-005 PRZECŁAW
NIP: 8513239302 Regon 383734596

Polityka ochrony danych osobowych – dokument główny

Wersja dokumentu 1.00 z dnia 9 marca 2020 roku

ZATWIERDZAM
GMINNY OŚRODEK KULTURY
SPORTU I REKREACJI
Mariusz Skóra
DYREKTOR
.....
podpis Dyrektora

Przecław, marzec 2020 roku

METRYKA

Nazwa jednostki	Gminny Ośrodek Kultury, Sportu i Rekreacji w Przecławiu		
Tytuł dokumentu	Polityka ochrony danych osobowych		
Opis	W skład dokumentu wchodzą: Polityka ochrony danych osobowych wraz z załącznikami		
Zastosowanie	Gminny Ośrodek Kultury, Sportu i Rekreacji w Przecławiu		
Plik	Polityka ochrony danych osobowych		
Status	Dokument zatwierdzony, obowiązujący do stosowania od dnia 10 marca 2020 r.	Liczba stron	24

HISTORIA DOKUMENTU

Wersja	Data wersji	Akcja*	Rozdziały**	Autor / Autorzy	Zatwierdził
1.00	09.03.2020	utworzenie	wszystkie	Krzysztof Rychel	

* Np.: utworzenie nowego dokumentu, modyfikacja, weryfikacja, uzupełnienie.

** Wymienić rozdziały, w których dokonano zmian.

Spis treści

1. Postanowienia wstępne

1.1 *Polityka ochrony danych osobowych* w Gminnym Ośrodku Kultury, Sportu i Rekreacji w Przecławiu (dalej: GOKSiR, jednostka) jest zbiorem zasad i procedur, obowiązujących przy realizacji wszystkich czynności przetwarzania i wykorzystywania danych osobowych we wszystkich zbiorach danych, administrowanych przez GOKSiR w Przecławiu. Celem wprowadzenia polityki jest ograniczenie ryzyka naruszenia praw i wolności osób fizycznych, w tym w szczególności pracowników i osób korzystajacych z usług jednostki, jakie może spowodować przetwarzanie ich danych w związku z realizowanymi zadaniami i obowiązkami. Ponadto polityka ma na celu wykazanie realizacji zasady rozliczalności, przez prowadzenie odpowiedniej dokumentacji, opisującej sposoby ochrony danych, na którą składa się niniejsza polityka wraz z załącznikami stanowiącymi jej integralną część. Niniejsze reguły zostały opracowane z uwzględnieniem zasady: „Człowiek może zawieść – system nie powinien".

1.2 Niniejsza polityka dotyczy wszystkich czynności przetwarzania danych osobowych w zidentyfikowanych, jak i niezidetyfikowanych zbiorach danych osobowych, jak również czynności przetwarzania danych osobowych w ramach zbiorów, jak i spoza nich, które mogą być realizowane w sposób ciągły, jak i doraźny. W polityce przyznano wyższy priorytet realizowanym czynnością przetwarzania danych osobowych i ich identyfikacj w odniesieniu do obowiązku identyfikacji zbiorów danych osobowych. Polityka jest polityką ochrony danych osobowych w rozumieniu *rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z 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) – dalej: RODO.*

1.3 Dane osobowe w GOKSiR mogą być przetwarzane zarówno w sposób tradycyjny w księgach, aktach, wykazach i innych papierowych zbiorach, ewidencjach, jak i w systemach informatycznych.

1.4 Niniejszy dokument ma za zadanie stanowić mapę wymogów, zasad i regulacji związanych z obszarem ochrony danych osobowych w jednostce i zawiera:

- ✓ opis obowiązujących zasad ochrony danych osobowych;
- ✓ odwołania do załączników stanowiących wzorce zachowań, procedur lub dokumentów.

1.5 Integralną częścią dokumentacji niniejszej polityki jest Instrukcja zarządzania systemem informatycznym.

1.6 Odpowiedzialnym za wdrożenie i utrzymanie niniejszej polityki jest najwyższe kierownictwo GOKSiR w osobie Dyrektora.

2. Definicje

Ilekroć w polityce użyte zostaną nw. określenia to oznaczają one:

- ✓ **„administrator danych osobowych"** (dalej:**ADO**) – Gminny Ośrodek Kultury, Sportu i Rekreacji w Przecławiu reprezentowany przez Dyrektora;

- ✓ **„administrator systemu informatycznego”** (dalej **ASI**) – pracownik lub podmiot zewnętrzny odpowiadający za administrowanie systemami informatycznymi użytkowanymi przez ADO;

- ✓ **"dane osobowe"** oznaczają informacje o zidentyfikowanej lub możliwej do zidentyfikowania osobie fizycznej ("osobie, której dane dotyczą"); możliwa do zidentyfikowania osoba fizyczna to osoba, którą można bezpośrednio lub pośrednio zidentyfikować, w szczególności na podstawie identyfikatora takiego jak imię i nazwisko, numer identyfikacyjny, dane o lokalizacji, identyfikator internetowy lub jeden bądź kilka szczególnych czynników określających fizyczną, fizjologiczną, genetyczną, psychiczną, ekonomiczną, kulturową lub społeczną tożsamość osoby fizycznej;

- ✓ **"dane biometryczne"** oznaczają dane osobowe, które wynikają ze specjalnego przetwarzania technicznego, dotyczą cech fizycznych, fizjologicznych lub behawioralnych osoby fizycznej oraz umożliwiają lub potwierdzają jednoznaczną identyfikację tej osoby, takie jak **wizerunek twarzy** lub dane daktyloskopijne;

- ✓ **"dane dotyczące zdrowia"** oznaczają dane osobowe o zdrowiu fizycznym lub psychicznym osoby fizycznej - w tym o korzystaniu z usług opieki zdrowotnej - ujawniające informacje o stanie jej zdrowia;

- ✓ **"dane genetyczne"** oznaczają dane osobowe dotyczące odziedziczonych lub nabytych cech genetycznych osoby fizycznej, które ujawniają niepowtarzalne informacje o fizjologii lub zdrowiu tej osoby i które wynikają w szczególności z analizy próbki biologicznej pochodzącej od tej osoby fizycznej;

- ✓ **„dostępność danych”** - właściwość określająca, że zasób przetwarzanych danych osobowych, niezależnie od sposobu ich przetwarzania jest możliwy do wykorzystania na żądanie, w założonym czasie, przez użytkownika;

- ✓ **„integralność danych”** – określana również jako spójność polegająca na zachowaniu własności przez dane osobowe wykluczające wprowadzenie do nich zmian w nieautoryzowany sposób;

- ✓ **„jednostka”** – Gminny Ośrodek Kultury, Sportu i Rekreacji w Przecławiu;

- ✓ **„kategoria czynności przetwarzania”** (kategoria przetwarzań) to rodzaj usługi realizowanej przez podmiot przetwarzający na zlecenie administratora związanej ze zleconymi czynnościami przetwarzania.

- ✓ **„komórka organizacyjna”** – jedno lub wieloosobowy zespół znajdujący wyodrębnienie w strukturze organizacyjnej, ustanowiony do wykonywania określonych zadań w GOKSiR, podlegający konkretnej osobie, sprawującej nadzór nad jej działaniami. W jednostce zgodnie z przyjętym schematem organizacyjnym **(załącznik nr 1)** przyjęto zasadę, że każdy pracownik podlega bezpośrednio Dyrektorowi.

- ✓ **„kierownik komórki organizacyjnej”** – rozumie się przez to osoby kierujące lub nadzorujące pracę innych osób lub osobę zajmującą samodzielne stanowisko. W GOKSiR przyjęto zasadę, iż bezpośredni nadzór nad pracami pracowników pełni Dyrektor;

- ✓ **"odbiorca"** oznacza osobę fizyczną lub prawną, organ publiczny, jednostkę lub inny podmiot, któremu ujawnia się dane osobowe, niezależnie od tego, czy jest stroną trzecią. Organy

publiczne, które mogą otrzymywać dane osobowe w ramach konkretnego postępowania zgodnie z prawem Unii lub prawem państwa członkowskiego, nie są jednak uznawane za odbiorców; przetwarzanie tych danych przez te organy publiczne musi być zgodne z przepisami o ochronie danych mającymi zastosowanie stosownie do celów przetwarzania;

- ✓ **„ograniczenie przetwarzania"** oznaczenie przechowywanych danych osobowych w celu ograniczenia ich przyszłego przetwarzania;
- ✓ **„osoba upoważniona do przetwarzania danych osobowych lub użytkownik systemu"** – rozumie się przez to osobę, która została upoważniona pisemnie przez ADO i dopuszczona, jako użytkownik do przetwarzania danych osobowych w systemie informatycznym GOKSiR, jak i poza nim w zakresie wskazanym w upoważnieniu;
- ✓ **"organ nadzorczy"** oznacza niezależny organ publiczny ustanowiony przez państwo członkowskie zgodnie z art. 51 RODO – Prezes Urzędu Ochrony Danych Osobowych;
- ✓ **"naruszenie ochrony danych osobowych"** oznacza naruszenie bezpieczeństwa prowadzące do przypadkowego lub niezgodnego z prawem zniszczenia, utracenia, zmodyfikowania, nieuprawnionego ujawnienia lub nieuprawnionego dostępu do danych osobowych przesyłanych, przechowywanych lub w inny sposób przetwarzanych;
- ✓ **"podmiot przetwarzający"** oznacza osobę fizyczną lub prawną, organ publiczny, jednostkę lub inny podmiot, który przetwarza dane osobowe w imieniu administratora;
- ✓ **„poufności danych"** – rozumie się przez to właściwość zapewniającą, że dane nie są udostępniane nieupoważnionym osobom;
- ✓ **„profilowanie"** oznacza dowolną formę zautomatyzowanego przetwarzania danych osobowych, które polega na wykorzystaniu danych osobowych do oceny niektórych czynników osobowych osoby fizycznej, w szczególności do analizy lub prognozy aspektów dotyczących efektów pracy tej osoby fizycznej, jej sytuacji ekonomicznej, zdrowia, osobistych preferencji, zainteresowań, wiarygodności, zachowania, lokalizacji lub przemieszczania się;
- ✓ **„przetwarzanie danych osobowych"** oznacza operację lub zestaw operacji wykonywanych na danych osobowych lub zestawach danych osobowych w sposób zautomatyzowany lub niezautomatyzowany, taką jak zbieranie, utrwalanie, organizowanie, porządkowanie, przechowywanie, adaptowanie lub modyfikowanie, pobieranie, przeglądanie, wykorzystywanie, ujawnianie poprzez przesłanie, rozpowszechnianie lub innego rodzaju udostępnianie, dopasowywanie lub łączenie, ograniczanie, usuwanie lub niszczenie;
- ✓ **"pseudonimizacja"** oznacza przetworzenie danych osobowych w taki sposób, by nie można ich było już przypisać konkretnej osobie, której dane dotyczą, bez użycia dodatkowych informacji, pod warunkiem, że takie dodatkowe informacje są przechowywane osobno i są objęte środkami technicznymi i organizacyjnymi uniemożliwiającymi ich przypisanie zidentyfikowanej lub możliwej do zidentyfikowania osobie fizycznej;
- ✓ **RODO** – rozumie się przez to rozumie się przez to 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);

- ✓ **„rozliczalność danych"** - właściwość pozwalająca przypisać określone działanie związane z przetwarzaniem danych osobowych do osoby, procesu, miejsca oraz umiejscowić je w czasie;
- ✓ **„serwisancie"** – rozumie się przez to firmę lub pracownika firmy, zajmującej się instalacją, naprawą i konserwacją sprzętu komputerowego oraz pozostałych elementów infrastruktury informatycznej;
- ✓ **"strona trzecia"** oznacza osobę fizyczną lub prawną, organ publiczny, jednostkę lub podmiot inny niż osoba, której dane dotyczą, administrator, podmiot przetwarzający czy osoby, które - z upoważnienia administratora lub podmiotu przetwarzającego - mogą przetwarzać dane osobowe;
- ✓ **„systemie informatycznym"** – rozumie się przez to zespół współpracujących ze sobą urządzeń, programów, procedur przetwarzania informacji i narzędzi programowych zastosowanych w celu przetwarzania danych;
- ✓ **„użytkownik"** – pracownik GOKSiR lub inna osoba zatrudniona w niej zatrudniona na podstawie umowy cywilnej, upoważniona do przetwarzania danych osobowych, w tym w sposób tradycyjny, z wykorzystaniem systemu informatycznego, programu komputerowego, aplikacji;
- ✓ **„uwierzytelnianiu** – rozumie się przez to działanie, którego celem jest weryfikacja deklarowanej tożsamości użytkownika;
- ✓ **„zbiór danych"** oznacza uporządkowany zestaw danych osobowych dostępnych według określonych kryteriów, niezależnie od tego, czy zestaw ten jest scentralizowany, zdecentralizowany czy rozproszony funkcjonalnie lub geograficznie;
- ✓ **"zgoda"** osoby, której dane dotyczą oznacza dobrowolne, konkretne, świadome i jednoznaczne okazanie woli, którym osoba, której dane dotyczą, w formie oświadczenia lub wyraźnego działania potwierdzającego, przyzwala na przetwarzanie dotyczących jej danych osobowych;

3. Organizacja przetwarzania danych osobowych

3.1 Przetwarzanie danych osobowych w GOKSiR jest dopuszczalne wyłącznie pod warunkiem przestrzegania przepisów RODO.

3.2 Gminny Ośrodek Kultury, Sportu i Rekreacji w Przecławiu przetwarza dane osobowe zgodnie z zasadami wskazanymi w art. 5 i art. 25 RODO, które stanowią filary ochrony danych osobowych, czyli zgodnie z zasadą:

- ✓ zgodności z prawem,
- ✓ rzetelności i przejrzystości,
- ✓ zasadą ograniczenia celu,

- ✓ minimalizacji danych,
- ✓ prawidłowości danych,
- ✓ ograniczenia przechowywania,
- ✓ integralności i poufności,
- ✓ ochrony danych w fazie projektowania,
- ✓ domyślną ochroną danych
- ✓ zasadą przestrzegania praw jednostki.

3.3 Zasada zgodności z prawem (art. 5 ust. 1 lit. a RODO) oznacza, iż w jednostce przetwarza się dane osobowe na podstawie, co najmniej jednej z przesłanek przetwarzania danych osobowych wynikających z art. 6 oraz 9 RODO. GOKSiR realizuje zadania wynikające ze Statutu określonego Uchwałą Nr V/79/2019 Rady Gminy Kołbaskowo z dnia 25 marca 2019 r. Przetwarzanie danych osobowych w jednostce odbywa się w głównej mierze w oparciu o przesłanki wskazane art. 6 oraz 9 RODO. Stosowanie ww. norm prawa, oznacza stosowanie się do zasady legalizmu i zobowiązuje Dyrektora jednostki do identyfikowanie podstawy prawnej w postaci konkretnej normy prawa w odniesieniu do realizowanych czynności przetwarzania danych osobowych, i jej wskazywanie w **Rejestrze czynności przetwarzania danych osobowych** (dalej: **RCPD**), o którym mowa w art. 30 ust. 1 RODO. Wzór rejestru stanowi **załącznik nr 2.**

3.4 Rejestr Czynności Przetwarzania Danych osobowych jest prowadzony przez Dyrektora GOKSiR, który jest odpowiedzialny za jego prowadzenie.

3.5 Zasadę rzetelności i przejrzystości (art. 5 ust. 1 lit. a RODO) GOKSiR realizuje poprzez wypełnianie obowiązków informacyjnych wskazanych w art. 13 i art. 14 RODO oraz udzielanie odpowiedzi na wnioski osób, których dane dotyczą, szczególnie w zakresie wynikającym z art. 15 RODO. Obowiązki informacyjne realizowane są przez poszczególnych pracowników GOKSiR, którym powierzono prowadzenie sprawy lub jej prowadzenie wynika z przyjętego zakresu obowiązków. Za realizację przedmiotowego obowiązku informacyjnego odpowiada pracownik oraz Dyrektor jednostki. Sposób realizacji obowiązku informacyjnego określa **Procedura realizacji obowiązku informacyjnego.**

3.6 GOKSiR jako administrator przetwarza dane osobowe jedynie w celach związanych z realizacją zadań wskazanych w pkt 3.3. Wyjątek od tej reguły stanowi dalsze przetwarzanie danych osobowych do celów archiwalnych w interesie publicznym, do celów badań naukowych lub historycznych lub do celów statystycznych (zasada ograniczenia celu art. 5 ust. 1 lit. b RODO). Wskazanie celu przetwarzania stanowi obligatoryjny element **Rejestru czynności przetwarzania danych.**

3.7 GOKSiR, jako podmiot przetwarzający w sytuacji, gdy powierzono jemu dane przez innego administratora i na mocy przyjętego w formie umowy powierzenia, zobowiązania polegającego na przetwarzaniu danych w imieniu i na rzecz innego podmiotu (art. 30 ust. 2 RODO), prowadzi **Rejestr Kategorii czynności przetwarzania,** stanowiący **załącznik nr 3. Rejestr kategorii czynności przetwarzania** jest prowadzony na zasadach określonych analogicznie, jak dla **Rejestru czynności przetwarzania danych osobowych** w pkt. 3.4.

3.8 Rejestr kategorii czynności przetwarzania oraz **Rejestr czynności przetwarzania danych osobowych** stanowią formę dokumentowania czynności przetwarzania danych osobowych i są

kluczowymi elementami umożliwiającymi realizację fundamentalnej zasady, na której opiera się cały system ochrony danych osobowych – czyli zasady rozliczalności.

3.9 Dla celów zgodności z zasadą minimalizacji danych (art. 5 ust. 1 lit. c RODO) w jednostce przetwarza się wyłącznie dane osobowe, które są niezbędne do osiągnięcia celu przetwarzania, a osoba przetwarzająca w kontekście realizowanego zadania jest w stanie uzasadnić potrzebę przetwarzania każdej kategorii danych, wskazując przy tym właściwy przepis prawa. Za adekwatność zakresu przetwarzanych danych osobowych ponosi odpowiedzialność pracownik realizujący czynność przetwarzania i Dyrektor jednostki. Kategorie danych podlegające przetwarzaniu muszą znaleźć swoje odzwierciedlenie w **Rejestrze czynności przetwarzania danych osobowych**, o którym mowa w art. 30 ust. 1 RODO, w odniesieniu do konkretnie realizowanej czynności przetwarzania.

3.10 Przetwarzaniu podlegają dane osobowe prawidłowe, aktualne i odpowiadające faktycznemu stanowi rzeczy, co zapewnia zadośćuczynienie zasadzie prawidłowości danych (art. 5 ust. 1 lit. d RODO). Obowiązkiem pracownika przetwarzającego dane jest podjęcie możliwych starań w celu upewnienia się, co do stanu aktualności przetwarzanych danych osobowych.

3.11 Wychodząc naprzeciw zasadzie ograniczenia przechowywania danych osobowych (art. 5 ust. 1 lit. e RODO), dane osobowe w jednostce przechowuje się wyłącznie przez okres niezbędności dysponowania dokumentacją dla realizowania zadań lub przez okres wynikający z Jednolitego Rzeczowego Wykazu Akt, uzgodnionego w trybie ustawy z dnia 14 lipca 1983 r. o narodowym zasobie archiwalnym i archiwach, z właściwym archiwum państwowym. Realizacja zasady ograniczenia przechowywania następuje przez dokumentowanie procesu brakowania dokumentacji niearchiwalnej lub przekazywania materiałów archiwalnych do właściwego archiwum państwowego. Usuwanie danych zawartych w dokumentacji niearchiwalnej następuje w momencie niszczenia dokumentacji na podstawie zgody właściwego archiwum państwowego, po spełnieniu się łącznie dwóch warunków: upływ okresu przechowywania dokumentacji i jej zbędność do celów służbowych. Realizacja zasady ograniczenia przechowywania następuje również przez wskazanie planowanych terminów usunięcia danych w **Rejestrze czynności przetwarzania danych osobowych**, o którym mowa w art. 30 ust. 1 RODO.

3.12 Proces przetwarzania danych osobowych odpowiada zasadzie integralności i poufności (art. 5 ust. 1 lit. f RODO), co zapewnia, dopuszczenie do przetwarzania danych osobowych jedynie osoby upoważnione oraz zastosowanie takich środków technicznych i organizacyjnych, by dane nie były zmieniane przez osoby nieupoważnione, zmienione nieumyślnie lub by dane nie były udostępniane osobom nieupoważnionym.

3.13 Zgodnie z zasadą ochrony danych w fazie projektowania (art. 25 ust. 1 RODO), ochrona prywatności i poufności przetwarzania danych osobowych winna być wbudowana w każdy nowy projekt na etapie jego planowania. W szczególności zasada ta będzie realizowana w zamówieniach publicznych, czy przy zawieraniu umów powierzenia przetwarzania danych osobowych. Wyrazem spełnienia tej zasady jest wprowadzanie obowiązku ochrony przetwarzanych danych bez konieczności jakiejkolwiek aktywności osób, których dane dotyczą.

3.14 Mając na uwadze aktualność zapisów zawartych w **Rejestrze czynności przetwarzania danych osobowych** i w **Rejestrze kategorii przetwarzania**, administrator danych osobowych (Dyrektor GOKSiR) zobowiązany jest do przeprowadzenia okresowej inwentaryzacji:

a) realizowanych czynności przetwarzania w odniesieniu, do których pełni funkcję administratora,
b) realizowanych czynności przetwarzania danych, które wykonuje w drodze zawartych umów powierzenia danych do dalszego przetwarzania.

3.15 Inwentaryzacja, o której mowa powyżej jest wykonywana nie rzadziej niż raz w ciągu roku lub każdorazowo na uzasadniony wniosek Inspektora Ochrony Danych. Czynności inwentaryzacyjne przeprowadzane są przez Dyrektora lub osoby przez niego wyznaczone.

4. Obsługa praw jednostki

4.1 Gminny Ośrodek Kultury, Sportu i Rekreacji w Przecławiu spełnia obowiązki informacyjne względem osób, których dane przetwarza oraz zapewnia obsługę ich praw, realizując otrzymane w tym zakresie żądania, w szczególności:

- ✓ **obowiązki informacyjne** – GOKSiR przekazuje informacje właścicielom danych osobowych w formie tzw. „klauzuli informacyjnej", której minimalny zakres określono w art. 13 oraz 14 RODO. Informacje są przekazywane, właścicielom danych osobowych, których dane są przetwarzane lub ich opiekunom prawnym. Wzory stosownych **Informacji** zostały określone w **załączniku nr 4**, a sposób realizacji obowiązku informacyjnego określa **Procedura realizacji obowiązku informacyjnego.**

- ✓ **możliwość wykonania żądań** – GOKSiR w związku z przyjętą strukturą organizacyjną weryfikuje i zapewnia możliwość efektywnego wykonania każdego typu żądania;

- ✓ **obsługa żądań** – GOKSiR zapewnia odpowiednie nakłady, aby żądania były realizowane w terminach określonych w RODO i należycie dokumentowane. Bezpośredni nadzór nad realizacją zgłaszanych żądań sprawuje Dyrektor lub osoba przez niego wskazana.

4.2 GOKSiR dba o czytelność i styl przekazywanych informacji i komunikacji z osobami, których dane przetwarza przedkładając każdorazowo Inspektorowi Ochrony Danych do zatwierdzenia treść udzielanej informacji (akceptowanie treści tzw. „klauzul informacyjnych".

4.3 GOKSiR ułatwia osobom korzystanie z ich praw poprzez różne działania, w tym: zamieszczanie na swojej stronie internetowej informacji lub odwołań do informacji (w postaci linków) o prawach osób, których dane przetwarza.

4.4 GOKSiR przestrzega prawnych terminów dotyczących obowiązków informacyjnych względem osób oraz dokumentuje obsługę obowiązków informacyjnych, zawiadomień i żądań osób.

4.5 GOKSiR określa sposób informowania osób niezidentyfikowanych o przetwarzaniu ich danych tam, gdzie jest to możliwe (np. tablica informująca o objęciu obszaru monitoringiem wizyjnym, strona internetowa, BIP).

4.6 GOKSiR informuje właścicieli danych o ich sprostowaniu, usunięciu lub ograniczeniu przetwarzania – chyba, że będzie to wymagało niewspółmiernie dużego wysiłku lub będzie niemożliwe.

4.7 W przypadku stwierdzonego naruszenia ochrony danych osobowych, Dyrektor jednostki bez zbędnej zwłoki zawiadomi właścicieli danych, jeżeli naruszenie może powodować wysokie ryzyko naruszenia praw i wolności tych osób (art. 34 RODO) – **Procedura postępowania przy stwierdzeniu naruszenia**,

5. Administrator Danych Osobowych (ADO)

5.1 Administratorem Danych Osobowych (dalej: ADO, administrator) w rozumieniu art. 4 pkt 7 RODO jest Gminny Ośrodek Kultury, Sportu i Rekreacji w Przecławiu reprezentowany przez jego Dyrektora.

5.2 Głównym zadaniem ADO jest ustalenie charakteru, zakresu, kontekstu i celów przetwarzania oraz ryzyka naruszenia praw lub wolności osób fizycznych i wdrożenie odpowiednich środków technicznych i organizacyjnych, mających na celu zapewnienie procesowi przetwarzania zgodność z przepisami wskazanymi w RODO (art. 32 RODO).

5.3 Aby przetwarzanie odbywało się zgodnie z RODO i aby móc to wykazać ADO odpowiada w szczególności za:

- ✓ sporządzenie analizy ryzyka wszystkich zidentyfikowanych zagrożeń dla procesu przetwarzania danych osobowych. Minimalny zakres zagrożeń uwzględnianych w przedmiotowej analizie wynika z zakresu określonego w załączniku C (Przykłady typowych zagrożeń) do PN-ISO/IEC 27005;
- ✓ opracowanie, wprowadzenie i wdrożenie odpowiedniej polityki ochrony danych osobowych;
- ✓ określenie częstotliwości dokonywania przeglądu przedmiotowej polityki pod kątem jej aktualności. Tym samym korzystając z posiadanych kompetencji ADO ustanawia, że przedmiotowy przegląd będzie realizowany, co najmniej raz w roku lub każdorazowo w przypadku istotnych zmian w strukturze organizacyjnej lub zakresie realizowanych zadań;
- ✓ podejmowanie decyzji o celach i środkach przetwarzania danych osobowych z uwzględnieniem przede wszystkim zmian w obowiązującym prawie;
- ✓ organizację administrowania danymi oraz określenie właściwych technik ich zabezpieczenia;
- ✓ upoważnienie poszczególnych pracowników do czynności przetwarzania danych osobowych w zakresie, odpowiadającym powierzonym czynnościom na danym stanowisku pracy (art. 29 RODO). ADO wydaje upoważnienie sporządzone wg wzoru **załącznik nr** 5 **– Upoważnienie do przetwarzania danych osobowych.** Przy wydawaniu upoważnień administrator danych osobowych kieruje się tzw. zasadą wiedzy koniecznej w stosunku do osoby upoważnianej;
- ✓ odwoływanie wydanych upoważnień na podstawie własnej decyzji. Wzór wniosku odwołującego upoważnienie do przetwarzania danych osobowych stanowi **załącznik nr 6 – Odwołanie upoważnienia do przetwarzania danych osobowych**;
- ✓ przestrzeganie procedury nadawania i odbierania upoważnień określonej w **Procedurze nadawania i odbierania uprawnień do przetwarzania danych osobowych**;

- ✓ prowadzenie ewidencji wydanych i odwołanych upoważnień do przetwarzania danych osobowych ***(wg załącznika nr 7 – Rejestr wydanych i odwołanych upoważnień)*** oraz pozostałą dokumentację z zakresu ochrony danych osobowych;
- ✓ zapewnienie pracownikom odpowiedniego wyposażenia stanowiska pracy i warunków pracy, umożliwiających przetwarzanie danych zgodnie z niniejszą polityką;
- ✓ wyznaczenie i powołanie Inspektora Ochrony Danych (dalej: IOD, inspektor) zgodnie z art. 37 oraz 38 RODO oraz wskazanie osoby lub podmiotu, który będzie Administratorem Systemu Informatycznego (dalej: ASI) wraz z określeniem zakresu zadań tej osoby.
- ✓ podejmowanie w porozumieniu z IOD oraz ASI odpowiednich działań w przypadku stwierdzenia naruszenia lub podejrzenia naruszenia przetwarzania danych osobowych, w tym w szczególności jego niezwłoczne zgłoszenie organowi nadzorczemu w nieprzekraczalnym terminie 72 h (art. 33 RODO);
- ✓ dokonanie oceny skutków przetwarzania danych osobowych dla praw lub wolności osób fizycznych (art. 35 RODO) lub zlecenie IOD przeprowadzenie tej oceny;
- ✓ sprawowanie nadzoru nad przestrzeganiem przyjętych zasad ochrony danych osobowych;
- ✓ sprawowanie bezpośredniego nadzoru nad działaniami osoby administrującej systemami informatycznymi w GOKSiR;
- ✓ przeprowadzenie wspólnie z IOD analizy ryzyka procesu przetwarzania danych osobowych w formie zgodnej z przyjętą **Metodologią analizy ryzyka**, która stanowi **Załącznik nr 8** do niniejszej polityki, pod kątem utraty atrybutów: poufności, dostępności, integralności. Przedmiotowa analiza jest wykonywana nie rzadziej niż raz w roku lub na skutek istotnych zmian organizacyjnych, czy też zmian zakresu działań realizowanych przez jednostkę;
- ✓ samodzielne lub we współpracy z IOD zorganizowanie, co najmniej raz w roku szkolenia z zakresu zasad przetwarzania danych osobowych dla pracowników jednostki. Szkolenie może przeprowadzić IOD;
- ✓ określenie w drodze pisemnego upoważnienia, osób odpowiedzialnych za realizację poszczególnych obowiązków jemu przypisanych, jeżeli którekolwiek z nich powierzy innym pracownikom GOKSiR, co jednak nie zwalnia go z odpowiedzialności za sposób ich realizacji;
- ✓ wybór podmiotów przetwarzających dane na rzecz jednostki, określając wymogi w stosunku do przetwarzających, co do warunków przetwarzania, które winny zostać zawarte w umowie powierzenia danych osobowych do dalszego przetwarzania. Wzór **Umowy powierzenia danych osobowych do dalszego przetwarzania** stanowi **załącznik nr 9;**

6. Osoba/podmiot administrujący systemem informatycznym (ASI)

6.1 ADO w osobie Dyrektora wyznacza, powołuje oraz zatwierdza wybór osoby, która będzie administrowała systemami informatycznymi użytkowanymi w jednostce. Niezależnie od sposobu powołania administratora systemu informatycznego (dalej: ASI), Dyrektor o fakcie tym powiadamia pracowników w drodze stosownego zarządzenia lub w innej formie przyjętej dla tego rodzaju komunikatów.

6.2 Funkcję związaną z administrowaniem systemem informatycznym może pełnić: pracownik jednostki, lub podmiot zewnętrzny na zasadzie świadczenia usługi. Niezależnie od sposobu powierzenia funkcji administratora systemu informatycznego, osoba ta realizuje zadania w zakresie zarządzania i bieżącego nadzoru nad systemem informatycznym, w tym zwłaszcza:

- ✓ nadzoruje i zarządza systemem informatycznym, posługując się hasłem dostępu do wszystkich stacji roboczych z pozycji administratora;
- ✓ konfiguruje wszystkie stacje robocze w jednostce w sposób zapewniający, iż tylko z pozycji administratora dostępne będą opcje związane z konfiguracją zainstalowanego systemu operacyjnego oraz instalacją oprogramowania i jego aktualizacją;
- ✓ jest jedyną osobą uprawnioną do instalowania i usuwania oprogramowania systemowego, narzędziowego i jego aktualizacji. Dopuszcza się instalowanie tylko legalnie pozyskanych programów, niezbędnych do wykonywania zadań GOKSiR i posiadających ważną licencję użytkownika oraz dostęp do właściwych aktualizacji;
- ✓ opracowuje i aktualizuje dokumentację opisującą wykorzystywane w jednostce systemy informatyczne;
- ✓ podejmuje odpowiednie działania w przypadku naruszenia lub podejrzenia naruszenia bezpieczeństwa systemu informatycznego;
- ✓ opiniuje wszelkie przedsięwzięcia związane z wprowadzeniem nowych rozwiązań funkcjonalnych oprogramowania oraz urządzeń w odniesieniu do funkcjonującego w jednostce systemu informatycznego. Wydane przez ASI opinie mogą mieć charakter wiążący i rozstrzygający;
- ✓ sprawuje nadzór nad wdrożonymi oraz wdrażaniem nowych środków technicznych i organizacyjnych zapewniających ochronę systemów informatycznych;
- ✓ nadzoruje stosowanie środków fizycznych, a także organizacyjnych i technicznych w celu zapewnienia bezpieczeństwa użytkowanych systemów informatycznych w jednostce;
- ✓ przeciwdziała dostępowi osób niepowołanych do systemu informatycznego, w tym w szczególności do zasobów, w których przetwarzane są dane osobowe;
- ✓ na wniosek Dyrektora, określa dla użytkownika dostęp do poszczególnych zasobów informatycznych funkcjonujących w jednostce, przydzielając każdemu użytkownikowi indywidualny login oraz dokonuje ewentualnych modyfikacji uprawnień;
- ✓ prowadzi rejestr przydzielonych poszczególnym pracownikom loginów w odniesieniu do użytkowanych systemów informatycznych oraz pozostałych rejestrów wymienionych w niniejszym dokumencie;
- ✓ nadzoruje działanie mechanizmów uwierzytelniania użytkowników oraz kontroli dostępu do zasobów informatycznych;
- ✓ podejmuje działania w zakresie ustalania i kontroli identyfikatorów dostępu do systemu informatycznego;
- ✓ wyrejestrowuje użytkowników systemu informatycznego na wniosek przełożonych użytkownika;

- ✓ zapewnia i nadzoruje zmianę haseł w poszczególnych stacjach roboczych w sposób gwarantujący ich znajomość wyłącznie danemu użytkownikowi oraz w razie stanu wyższej konieczności ADO;
- ✓ w sytuacji stwierdzenia naruszenia zabezpieczeń systemu informatycznego, informuje ADO oraz IOD o naruszeniu i współdziała z nimi przy usuwaniu jego skutków;
- ✓ prowadzi szczegółową dokumentację naruszeń bezpieczeństwa danych osobowych, przetwarzanych w systemach informatycznych zgodnie z wymogami określonymi w RODO;
- ✓ sprawuje nadzór: nad wykonywaniem napraw, konserwacją oraz likwidacją urządzeń komputerowych, na których zapisane są dane osobowe, nad wykonywaniem kopii zapasowych i ich przechowywaniem oraz okresowym ich sprawdzaniem pod kątem ich dalszej przydatności do odtwarzania danych w przypadku awarii systemu informatycznego;
- ✓ podejmuje działania, służące zapewnieniu niezawodności zasilania komputerów, innych urządzeń mających wpływ na bezpieczeństwo przetwarzania danych osobowych oraz zapewnieniu bezpiecznej wymiany danych w sieci wewnętrznej i bezpiecznej teletransmisji.

6.3 Administrator systemu informatycznego ma prawo do:

- ✓ wyznaczania, rekomendowania i egzekwowania wykonania zadań związanych z ochroną systemów informatycznych funkcjonujących w jednostce;
- ✓ opiniowania możliwości wdrażania i rozbudowy systemów informatycznych o dodatkowe elementy (urządzenia, programy);
- ✓ wstępu do pomieszczeń w których użytkowane są systemy informatyczne i przeprowadzania niezbędnych badań lub innych czynności mających na celu zapewnienie prawidłowego funkcjonowania użytkowanych systemów informatycznych, w tym również poza godzinami pracy jednostki po wcześniejszym ustaleniu tego z ADO;
- ✓ wnioskowania o złożenie pisemnych lub ustnych wyjaśnień przez pracowników jednostki lub osób współpracujących w zakresie niezbędnym do ustalenia stanu faktycznego, odnoszącego się do funkcjonowania systemów informatycznych oraz przyjętych zabezpieczeń;
- ✓ wglądu do dokumentów i wszelkich danych, mających bezpośredni związek z problematyką kontroli przyczyn naruszenia;
- ✓ dokonywania oględzin urządzeń, nośników służących do przetwarzania danych w systemach informatycznych jednostki.

7. Inspektor Ochrony Danych

7.1 Dyrektor jednostki jako administrator i podmiot przetwarzający jest obowiązany do wyznaczenia inspektora ochrony danych na zasadach określonych w art. 37 RODO.

7.2 Administrator danych osobowych zapewnia:

- ✓ włączenie IOD we wszystkie sprawy dotyczące ochrony danych osobowych;

- ✓ wsparcie IOD w wypełnianiu przez niego zadań, o których mowa w art. 39 RODO;
- ✓ powstrzymywanie się przed wydawaniem IOD instrukcji dotyczących sposobu wykonywania zadań przez IOD;
- ✓ zobowiązanie się IOD do zachowania tajemnicy lub poufności, co do wykonywania swoich zadań.

7.3 Do zadań IOD należy:

- ✓ informowanie administratora oraz pracowników przetwarzających dane osobowe, o obowiązkach spoczywających na nich na mocy niniejszej polityki oraz innych przepisów, w tym w szczególności RODO i doradzanie im w materii ochrony danych osobowych;
- ✓ monitorowanie przestrzegania niniejszej polityki, przepisów RODO, innych przepisów Unii lub państw członkowskich o ochronie danych, w tym podejmowanie działań zwiększających świadomość, szkolenie personelu uczestniczącego w operacjach przetwarzania oraz przeprowadzanie powiązanych z tym audytów;
- ✓ udzielanie na żądanie zaleceń co do oceny skutków dla ochrony danych oraz monitorowanie ich wykonania zgodnie z art. 35 RODO;
- ✓ udzielanie wyjaśnień i pomocy w obszarze ochrony danych osobowych w reakcji na prośbę administratora lub Jego pracowników;
- ✓ weryfikacja pod kątem zgodności z RODO opracowywanych umów powierzenia danych osobowych, klauzul informacyjnych i innych dokumentów z obszaru ochrony danych osobowych przedkładanych przez administratora lub jego pracowników;
- ✓ współpraca z organem nadzorczym, którym jest Prezes Urzędu Ochrony Danych Osobowych;
- ✓ pełnienie funkcji punktu kontaktowego dla organu nadzorczego oraz osób, których dane są przetwarzane we wszystkich kwestiach związanych z przetwarzaniem, w tym z uprzednimi konsultacjami, o których mowa w art. 36 RODO, oraz w stosownych przypadkach prowadzenie konsultacji we wszelkich innych sprawach;
- ✓ doradztwo i pomoc w zakresie rozpatrywania wniosków kierowanych do ADO związanych z realizacją praw osób fizycznych, których dane osobowe są przetwarzane.

8. Osoba upoważniona do przetwarzania danych osobowych

8.1 Osoba upoważniona do przetwarzania danych osobowych **(użytkownik),** to każda osoba spełniająca kryteria definicji zawartej w Rozdziale **2. Definicje**.

8.2 Każdy użytkownik bez jakiegokolwiek wyjątku jest zobowiązany do przestrzegania zasad przetwarzania danych osobowych określonych w niniejszym dokumencie, ze szczególnym uwzględnieniem zapisów zawartych **Rozdziale 3. Organizacja przetwarzania danych osobowych** oraz w **Rozdziale 11. Pozostałe zasady bezpiecznego przetwarzania danych osobowych.**

8.3 Osoba upoważniona do przetwarzania danych osobowych jest zobowiązana do złożenia pisemnego oświadczenia o zachowaniu w tajemnicy danych osobowych i przestrzegania zasad i procedur określonych niniejszym dokumentem, przez cały okres zatrudnienia oraz zachowania tajemnicy danych osobowych po ustaniu okresu zatrudnienia – treść oświadczenia zawiera formularz upoważnienia.

8.4 Naruszenie przez osobę upoważnioną do przetwarzania danych osobowych zasad określonych niniejszą polityką, w tym w szczególności tajemnicy danych osobowych lub procedur bezpiecznego ich przetwarzania na skutek świadomego działania, będzie traktowane, jako ciężkie naruszenie obowiązków pracowniczych, uzasadniające rozwiązanie umowy o pracę bez wypowiedzenia.

8.5 Użytkownik może przetwarzać dane osobowe wyłącznie w zakresie objętym upoważnieniem i tylko w celu wykonywania nałożonych na niego obowiązków służbowych.

8.6 W przypadku sytuacji niezamierzonego nieuprawnionego przetwarzania danych osobowych (np. na skutek otrzymania pisma z zewnątrz zawierającego niechciane i zbędne kategorie danych), użytkownik taki stan rzeczy odnotowuje w **Rejestrze zdarzeń nieuprawnionego przetwarzania danych osobowych** (wzór stanowi **załącznik nr 11**), który jest prowadzony przez Dyrektora.

8.7 Dane osobowe będące przedmiotem niezamierzonego nieuprawnionego przetwarzania, winny bezzwłocznie zostać zanonimizowane (zatarte, zakorektorowane w sposób uniemożliwiający ich odczytanie). W przypadku, kiedy do pisma załączono dokumenty zawierające dane osobowe zbędne dla załatwienia sprawy, dokumenty takie należy niezwłocznie zwrócić nadawcy.

8.8 Wszyscy użytkownicy przetwarzający dane osobowe zobowiązani są do:

- ✓ zapoznania się przepisami Polityki ochrony danych osobowych wraz ze wszystkimi dokumentami wchodzącymi w jej skład (*Instrukcja zarządzania systemem informatycznym*) oraz z przepisami prawa w zakresie ochrony danych osobowych, w tym w szczególności z przepisami RODO;
- ✓ odpowiedniego zabezpieczania danych osobowych przed ich udostępnieniem osobom nieupoważnionym;
- ✓ korzystania z systemu informatycznego administratora danych w sposób zgodny z *Instrukcją zarządzania systemem informatycznym* oraz zgodny ze wskazówkami zawartymi w instrukcji obsługi urządzeń wchodzących w skład systemu informatycznego, oprogramowania i nośników;
- ✓ korzystania z urządzeń wchodzących w skład systemu informatycznego, tylko i wyłącznie w celach służbowych.

9. Środki techniczne i organizacyjne, służące zapewnieniu bezpieczeństwa procesowi przetwarzania danych

9.1 Opisane środki techniczne i organizacyjne powinny być stosowane w celu zapewnienia bezpieczeństwa danych osobowych przetwarzanych w GOKSiR, a tym samym w celu ograniczenia ryzyka naruszenia praw i wolności osób fizycznych, których dane osobowe są przetwarzane.

9.2 Środki techniczne i organizacyjne, które zostały wskazane w niniejszym rozdziale są efektem przeprowadzonej analizy ryzyka zagrożeń procesów przetwarzania danych osobowych w jednostce, w sposób zgodny z metodologią wskazaną w **załączniku nr 8** *(Metodologia analizy ryzyka),* do niniejszej polityki.

9.3 Na zabezpieczenia o charakterze technicznym składają się:

- ✓ ochrona przed nieuprawnionym dostępem do obszarów przetwarzania realizowana poprzez:
  - ➢ stosowanie systemów alarmowych załączanych po godzinach pracy jednostki, monitorowanych przez zewnętrzną, licencjonowaną firmę z branży ochrony osób i mienia,
  - ➢ stosowanie zamków mechanicznych do pomieszczeń stanowiących miejsca przetwarzania danych osobowych,
  - ➢ zabezpieczenie obszarów przetwarzania danych w godzinach pracy przed dostępem osób nieuprawnionych na czas nieobecności w nich osób upoważnionych oraz po godzinach pracy z wykorzystaniem zamków mechanicznych, w które są wyposażone drzwi do wszystkich obszarów przetwarzania,
  - ➢ ograniczenie możliwości przebywania w obszarach przetwarzania danych osobowych, osób nieupoważnionych tylko i wyłącznie do sytuacji, kiedy jest to realizowane w obecności upoważnionych pracowników GOKSiR,

- ✓ ochrona nośników danych osobowych realizowana jest poprzez:
  - ➢ przechowywanie nośników zawierających dane osobowe w miejscach ich przetwarzania wyłącznie w szafach, kontenerach lub biurkach, które są wyposażonych w zamknięcia mechaniczne,
  - ➢ wyposażenie wszystkich pomieszczeń znajdujących się w wykazie miejsc przetwarzania danych osobowych w mechaniczne niszczarki dokumentów,
  - ➢ okresowe działania o charakterze konserwacyjnym w odniesieniu do infrastruktury technicznej, związanej z przetwarzaniem danych osobowych;

- ✓ ochrona przeciwpożarowa jest realizowana poprzez, wyposażenie pomieszczeń składających się na obszary przetwarzania danych osobowych w sprzęt p. poż.;

- ✓ ochrona przed awariami realizowana jest:
  - ➢ wyposażenie urządzeń serwerowych (jeżeli posiada) w awaryjne zasilanie tzw. UPS,
  - ➢ klimatyzowanie pomieszczeń, w których zlokalizowane są serwery (jeżeli serwery znajdują się na terenie GOKSiR i są pod nadzorem GOKSiR);

- ✓ zabezpieczenia realizowane we własnym zakresie przez użytkownika, wynikające z przyjętych przez GOKSiR standardów, do których możemy zaliczyć:
  - ➢ ustawiania ekranów komputerowych tak, aby osoby niepowołane nie mogły oglądać ich zawartości, a zwłaszcza nie naprzeciwko wejścia do pomieszczenia,
  - ➢ dbanie o prawidłową wentylację komputerów (kategoryczny zakaz ustawiania jednostek komputerowych w sposób zasłaniający kratki wentylatorów meblami, ścianą itp.),

- niepodłączania do listew, podtrzymujących napięcie, przeznaczonych do zasilania sprzętu komputerowego innych urządzeń, szczególnie tych łatwo powodujących spięcia (np. grzejnikiów, czajników, wentylatorów),
- wykonywanie kopii roboczych danych, na których się właśnie pracuje, z częstotliwością zapobiegającą ich utratę,
- kończenia pracy stacji roboczej poprzez prawidłowe wylogowanie się z systemu i wyłączenie komputera,
- niszczenie w niszczarce lub chowanie do szaf zamykanych na klucz, wszelkich wydruków zawierających dane osobowe przed opuszczeniem miejsca pracy, po zakończonym dniu pracy,
- niepozostawianie osób postronnych w pomieszczeniu, w którym przetwarzane są dane osobowe, bez obecności osoby upoważnionej do przetwarzania danych osobowych,
- umieszczanie kluczy do szaf w ustalonym, przeznaczonym do tego miejscu po zakończeniu dnia pracy,
- zamykanie okien w razie opadów czy innych zjawisk atmosferycznych, które mogą zagrozić bezpieczeństwu danych osobowych,
- zamykanie okien w razie opuszczania pomieszczenia, w tym zwłaszcza po zakończeniu dnia pracy,
- zamykanie drzwi na klucz po zakończeniu pracy w danym dniu. Jeśli niemożliwe jest umieszczenie wszystkich dokumentów, zawierających dane osobowe w zamykanych szafach, należy powiadomić o tym Dyrektora jednostki, który w danym dniu zgłasza osobie sprzątającej, jednorazową rezygnację z wykonywania usługi sprzątania,
- przestrzeganie „zasady czystego biurka i ekranu" zgodnie, z którą nie należy pozostawiać na biurku po zakończeniu pracy lub na czas krótkotrwałej nieobecności dokumentów oraz niewygaszonych monitorów wyświetlających informacje. Powyższa zasada ma zastosowanie również do urządzeń typu skaner, drukarka, niszczarka. Za niedopuszczalne należy uznać pozostawiania na ww. urządzeniach wydrukowanych, poddawanych skanowaniu, czy też przeznaczonych do zniszczenia dokumentów;
- niezwłoczne usuwanie skanowanych dokumentów z pamięci urządzeń skanujących natychmiast po ich wykorzystaniu (zapisaniu skanu na nośniku lub wydrukowaniu),
- natychmiastowe kasowanie danych na dyskach przenośnych po ich wykorzystaniu,
- chwilowe opuszczanie stanowiska pracy jest możliwe po uprzednim aktywowaniu wygaszacza ekranu lub po zablokowaniu stacji roboczej w inny sposób;

✓ pozostałe zabezpieczenia o charakterze technicznym w odniesieniu do wykorzystywanych systemów informatycznych zostały określone w **Instrukcji zarządzania systemem informatycznym,** stanowiącym integralną część systemu ochrony danych osobowych.

9.4 Na zabezpieczenia o charakterze organizacyjnym składają się:

✓ dokumentacja składająca się na Politykę ochrony danych osobowych zawierająca:
- opis zasad i wymogów w odniesieniu do procesu bezpiecznego przetwarzania danych osobowych zawartych w niniejszym dokumencie i **Instrukcji zarządzania systemem informatycznym**

- opis procesu reakcji na stwierdzone naruszenie – **Procedura reakcji na ujawnione naruszenie,**
- podział obowiązków i kompetencji uczestników procesu przetwarzania danych osobowych,
- obowiązki dokumentowania istotnych okoliczności związanych z przetwarzaniem danych osobowych w formie właściwych rejestrów,
- obowiązek realizacji okresowych rocznych przeglądów wdrożonego systemu bezpieczeństwa,
- realizowany w sposób bieżący nadzór nad adekwatnością przyjętych rozwiązań w stosunku do istniejących zagrożeń, wynikający z faktu przeprowadzenia okresowych analiz ryzyka zagrożeń,

✓ środki o charakterze osobowym, do których zalicza się:

- obowiązek przedłożenia Informacji z Krajowego Rejestru Karnego o niekaralności za przestępstwa umyślne ścigane z oskarżenia publicznego lub umyślne przestępstwa skarbowe przez pracownika zatrudnianego na stanowisku urzędniczym,

- obowiązek złożenia zobowiązania w formie oświadczenia przez wszystkich pracowników jednostki (zajmujących stanowiska urzędnicze, jak i nie urzędnicze) o zachowaniu w poufności danych osobowych, do których przetwarzania zostali upoważnieni oraz danych osobowych, do których uzyskali dostęp w sposób niezamierzony – wzór **Oświadczenia dla osób zatrudnionych na pomocniczych stanowiskach pracy** stanowi **załącznik nr 12**;

✓ objęcie systemem szkoleń indywidualnych i grupowych wszystkich użytkowników z zakresu:
- przepisów i procedur, dotyczących ochrony danych osobowych,
- sposobów ochrony danych przed osobami postronnymi i procedur udostępniania danych osobom, których dane dotyczą,
- obowiązków osób upoważnionych do przetwarzania danych osobowych,
- odpowiedzialności za naruszenie obowiązków z zakresu ochrony danych osobowych;

✓ zabezpieczenia realizowane we własnym zakresie przez użytkownika, wynikające z przyjętych przez GOKSiR standardów, do których możemy zaliczyć:
- niepozostawianie bez kontroli dokumentów i nośników danych, w strefach określanych mianem publicznych, do których zaliczamy ciągi komunikacyjne oraz miejsca w GOKSiR, do których mają swobodny niczym nieograniczony dostęp klienci,
- pilne strzeżenia akt i wymiennych nośników pamięci,
- nieużywanie powtórnie dokumentów zadrukowanych jednostronnie,
- niezapisywanie hasła wymaganego do uwierzytelnienia się w systemie na papierze lub innym nośniku,
- powstrzymywanie się przez osoby upoważnione do przetwarzania danych osobowych, przed samodzielną ingerencją w oprogramowanie i konfigurację powierzonego sprzętu, nawet gdy z pozoru mogłoby to usprawnić pracę lub podnieść poziom bezpieczeństwa danych,

- niewynoszenie poza siedzibę GOKSiR, na jakichkolwiek nośnikach całych zbiorów danych oraz szerokich z nich wypisów, nawet w postaci zaszyfrowanej,
- zachowanie tajemnicy danych, w tym także wobec najbliższych,
- przestrzeganie przez osoby upoważnione do przetwarzania danych osobowych swoich uprawnień w systemie, tj. właściwego korzystania z baz danych, używania tylko własnego loginu i hasła oraz stosowania się do zaleceń ASI,
- kopiowanie tylko jednostkowych danych (pojedyńczych plików). Obowiązuje zakaz robienia kopii całych zbiorów danych lub takich ich części, które nie są konieczne do wykonywania powierzonych pracownikowi obowiązków. Jednostkowe dane mogą być kopiowane na nośniki magnetyczne, optyczne, elektroniczne i inne po ich zaszyfrowaniu i przechowywane w zamkniętych na klucz szafach. Po ustaniu przydatności tych kopii, dane należy trwale skasować lub fizycznie zniszczyć nośniki, na których są przechowywane

- ✓ powołanie Inspektora Ochrony Danych, który ze względu na posiadaną autonomię w działaniu, wspomaga administratora w sprawowaniu nadzoru nad procesami związanymi z przetwarzaniem danych osobowych.

10. Infrastruktura przetwarzania danych osobowych

10.1 Infrastrukturę przetwarzania danych osobowych tworzą budynki i pomieszczenia, systemy informatycznie oraz pozostałe aktywa będące nośnikami danych wykorzystywane przez jednostkę.

10.2 Opis infrastruktury informatycznej oraz nośników danych wykorzystywanych przez jednostkę zawiera dokument **Instrukcja zarządzania systemem informatycznym**.

10.3 Wykaz budynków pomieszczeń lub części pomieszczeń stanowiących obszary przetwarzania (wg załacznika nr 10) określa wszystkie pomieszczenia, w których:

- ✓ dokonuje się przetwarzania danych osobowych;
- ✓ przechowuje się wszelkie nośniki zawierające dane osobowe;
- ✓ przechowuje się uszkodzone, wycofane z użytku komputery, nośniki danych.

10.4 Wykaz budynków pomieszczeń lub części pomieszczeń stanowiących obszary przetwarzania jest prowadzony w sposób bieżący przez Dyektora GOKSiR lub przez osobę przez niego wyznaczoną.

10.5 Ze względu na nagromadzenie danych osobowych, szczególnie chronione powinny być pomieszczenia:

- ✓ serwerowni jeżeli jednostka je posiada;
- ✓ w których przechowywana jest dokumentacja kadrowo - płacowa;
- ✓ w których przechowywana jest dokumentacja związana z ewidencją klientów GOKSiR;
- ✓ pomieszczenia archiwum.

10.6 W pomieszczeniach, o których mowa w pkt. 11.5 mogą przebywać wyłącznie osoby upoważnione do przetwarzania danych osobowych, pracownicy merytoryczni, których stanowiska pracy są

przypisane do przedmiotowych pomieszczeń, ADO, ASI, IOD, a inne osoby wyłącznie pod ich nadzorem.

10.7 Zabrania się przetwarzania danych osobowych w pomieszczeniach innych niż wymienione w wykazie, o którym mowa w pkt. 10.3.

10.8 Informacje zawarte w **załączniku nr 10** do niniejszej polityki mają charakter informacji wyłącznie do użytku wewnętrznego i nie podlegają upublicznieniu.

11. Pozostałe zasady bezpiecznego przetwarzania danych osobowych

11.1 Wykorzystywanie akt i dokumentów, zawierających dane osobowe po godzinach pracy jednostki oraz poza jej siedzibą tj. poza określonymi w **załącznku nr 10** obszarami jest zabronione.

11.2 Wykorzystywanie służbowych urządzeń przenośnych służących przetwarzaniu danych osobowych (laptopy, netbooki) jest możliwe tylko po uzyskaniu pisemnej zgody, udzielanej przez ADO oraz zgłoszeniu tego faktu administratorowi systemu informatycznego. Wzór **Zgody na użytkowanie urządzeń służbowych poza siedzibą jednostki** stanowi **załącznik nr 13**.

11.3 W sytuacji, o której mowa w pkt. 11.2 administrator systemu informatycznego jest zobowiązany do zaszyfrowania dysków zainstalowanych w jednostce komputerowej oraz prowadzi ewidencję sprzętu użytkowanego poza siedzibą jednostki przez uprawnionych pracowników.

11.4 Pracownicy wykorzystujący sprzęt poza siedzibą jednostki, są obowiązani do ochrony informacji w nich zapisanych. Ponadto odpowiadają materialnie w pełnej wysokości odpowiadającej wartości odtworzeniowej użytkowanego sprzętu z uwzględnieniem wartości odtworzeniowej zainstalowanego oprogramowania oraz wartości innych wydatków, jakie ewentualnie będzie musiał ponieść GOKSiR wynikających z utraty informacji, których nośnikiem był utracony sprzęt.

11.5 Osoby upoważnione do przetwarzania danych osobowych powinny pamiętać zwłaszcza, że:

- ✓ dane osobowe z nośników przenośnych, niebędących kopiami zapasowymi po wprowadzeniu do systemu informatycznego administratora danych, powinny być trwale usuwane z tych nośników programem trwale usuwającym pliki lub gdy nie ma takiej możliwości zniszczone (np. płyty CD-ROM);

- ✓ jeśli istnieje uzasadniona konieczność, dane pojedyńczych osób (a nie całe zbiory czy szerokie wypisy ze zbiorów), mogą być przechowywane na specjalnie oznaczonych nośnikach. Nośniki te muszą być przechowywane w zamkniętych na klucz szafach, nieudostępnianych osobom postronnym. Po ustaniu przydatności tych danych, nośniki powinny być trwale kasowane lub niszczone;
- ✓ uszkodzone nośniki przed ich wyrzuceniem należy zniszczyć fizycznie;
- ✓ zabrania się powtórnego używania do sporządzania brudnopisów, pism jednostronnie zadrukowanych, jeśli zawierają one dane osobowe;
- ✓ po wykorzystaniu wydruków zawierających dane osobowe, należy codziennie przed zakończeniem pracy zniszczyć je w niszczarce. O ile to możliwe, nie należy przechowywać takich

wydruków w czasie dnia na biurku, ani też wynosić poza obszary przetwarzania danych osobowych.

12. Przeglądy okresowe, zapobiegające naruszeniom obowiązku szczególnej staranności administratora danych

12.1 ADO zleca przeprowadzenie raz w roku przeglądu czynności przetwarzania danych osobowych pod kątem celowości i zasadności ich realizacji. Powyższy przegląd może zostać zrealizowany w ramach rocznego przeglądu Polityki Bezpieczeństwa Informacji, którego obowiązek wykonania wynika z Krajowych Ram Interoperacyjności. Osoby upoważnione do przetwarzania danych osobowych, w tym zwłaszcza osoby przetwarzające dane osobowe, są obowiązane współpracować z osobą dokonującą przeglądu i wskazywać jej czynności, które powinny zostać usunięte, ze względu na zrealizowanie celu przetwarzania lub brak ich adekwatności do realizowanego celu.

12.2 ADO może zarządzić przeprowadzenie dodatkowego przeglądu w wyżej określonym zakresie w razie zmian w obowiązującym prawie, ograniczających dopuszczalny zakres przetwarzanych danych osobowych. Dodatkowy przegląd jest możliwy, także w sytuacji zmian organizacyjnych u administratora danych, jak i każdej innej sytuacji, która w ocenie ADO lub IOD, będzie wymagała przeprowadzenia takiego przeglądu.

13. Udostępnianie danych osobowych

13.1 Udostępnianie danych osobowych policji, sądom innym organom odpowiadajacym za porządek publiczny, może nastąpić w związku z prowadzonym przez te instytucje postępowaniem.

13.2 Udostępnianie informacji wskazanej w pkt. 13.1 odbywa się według **Procedury udostępniania danych osobowych – załącznik nr 15**:

- ✓ udostępnianie danych osobowych może nastąpić po przedłożeniu wniosku o przekazanie lub udostępnienie informacji. Wniosek ten powinien mieć formę pisemną i zawierać:
  - oznaczenie wnioskodawcy,
  - wskazanie przepisów uprawniających do dostępu do informacji,
  - określenie rodzaju i zakresu potrzebnych informacji oraz formy ich przekazania lub udostępnienia,
  - wskazanie imienia, nazwiska i stopnia służbowego funkcjonariusza upoważnionego do pobrania informacji lub zapoznania się z ich treścią.

13.3 Udostępnianie danych osobowych na podstawie ustnego wniosku, zawierającego wszystkie powyższe cztery elementy wniosku pisemnego, może nastąpić tylko wtedy, gdy zachodzi konieczność niezwłocznego działania, np. w trakcie pościgu za osobą podejrzaną o popełnienie czynu zabronionego albo podczas wykonywania czynności mających na celu ratowanie życia i zdrowia ludzkiego lub mienia.

13.4 Osoba udostępniająca dane osobowe, jest obowiązana zażądać od funkcjonariusza pokwitowania pobrania dokumentów, zawierających informacje przekazane na podstawie pisemnego wniosku albo potwierdzenia faktu uzyskania wglądu w treść informacji.

13.5 Jeśli informacje są przekazywane na podstawie ustnego wniosku, należy stosownie do okoliczności

zwrócić się z prośbą o pokwitowanie albo potwierdzenie. Jeśli pokwitowanie albo potwierdzenie ze względu na okoliczności udostępniania nie jest możliwe, osoba udostępniająca informacje sporządza na tę okoliczność notatkę służbową.

14. Odpowiedzialność osób upoważnionych do przetwarzania danych osobowych

14.1 Niezastosowanie się do wprowadzonej przez administratora danych Polityki ochrony danych osobowych, której założenia określa niniejszy dokument i naruszenie procedur ochrony danych przez pracowników upoważnionych do przetwarzania danych osobowych, może być potraktowane, jako ciężkie naruszenie obowiązków pracowniczych, skutkujące rozwiązaniem stosunku pracy bez wypowiedzenia na podstawie art. 52 Kodeksu Pracy.

15. Postanowienia końcowe

15.1 Każda osoba, upoważniona do przetwarzania danych osobowych, zobowiązana jest do zapoznania się przed dopuszczeniem do przetwarzania danych z niniejszym dokumentem oraz do złożenia stosownego oświadczenia, potwierdzającego znajomość jego treści.
15.2 W odniesieniu do załączników mających formę rejestrów dopuszcza się możliwość ich prowadzenia w formie elektronicznej z wykorzystaniem narzędzi użytkowanego w jednostce oprogramowania biurowego.

Załączniki:

Załącznik nr 1 – Struktura organizacyjna jednostki;

Załącznik nr 2 – Rejestr czynnosci przetwarzania danych osobowych;

Załącznik nr 3 – Rejestr kategorii czynności przetwarzania;

Załącznik nr 4 – Klauzule informacyjne (z art. 13 oraz art. 14 RODO);

Załącznik nr 5 - Upoważnienia do przetwarzania danych osobowych;

Załącznik nr 6 – Odwołanie upoważnienia do przetwarzania danych osobowych;

Załącznik nr 7 – Rejestr wydanych i odwołanych upoważnień;

Załącznik nr 8 - Metodologia analizy ryzyka;

Załącznik nr 9 – Wzór umowy powierzenia danych osobowych do dalszego przetwarzania;

Załącznik nr 10 – Wykaz budynków, pomieszczeń lub części pomieszczeń stanowiących obszary przetwarzania;

Załącznik nr 11 - Rejestr zdarzeń nieuprawnionego przetwarzania danych osobowych;

Załącznik nr 12 – Oświadczenie dla osób zatrudnionych na pomocniczych stanowiskach pracy;

Załącznik nr 13 – Zgoda na użytkowanie urządzeń służbowych poza siedzibą jednostki;

Załącznik nr 14 - Procedura reakcji na ujawnione naruszenie;

Załącznik nr 15 - Procedura udostępniania danych osobowych;

Załącznik nr 16 – Rejestr naruszeń;

Załącznik nr 17 – Rejestr udostępnienia danych osobowych.