POLITYKA BEZPIECZEŃSTWA OCHRONY DANYCH OSOBOWYCH

w MOSiR w Zielonej Górze

Miejski Ośrodek Sportu i Rekreacji
ul. Sulechowska 41
65-022 Zielona Góra

tel. (68) 412 50 01
fax (68) 4121 50 09
e-mail: mosir@mosir.zgora.pl

Metryka dokumentu:

Tytuł:	Polityka Bezpieczeństwa Ochrony Danych Osobowych
Komentarz:	Edycja 3
Liczba stron:	19
Data utworzenia:	10 listopad 2015 r.
Data ostatniej wersji:	03 czerwiec 2016 r.

Wykaz załączników:

Załącznik P1	Wykaz zbiorów danych osobowych wraz ze wskazaniem programów stosowanych do przetwarzania tych danych
Załącznik P2	Opis struktury zbiorów danych osobowych
Załącznik P3	Sposób przepływu danych
Załącznik P4	Oświadczenie
Załącznik P5	Umowa powierzenia
Załącznik P6	Umowa o poufności
Załącznik P7	Upoważnienie do przetwarzania danych osobowych
Załącznik P8	Ewidencja upoważnień do przetwarzania danych osobowych

SPIS TREŚCI

1. Preambuła 4
2. Zakres Polityki Bezpieczeństwa Ochrony Danych Osobowych 5
3. Definicje 5
4. Osoby odpowiedzialne za ochronę danych osobowych 7
   - 4.1 Administrator Danych Osobowych 8
   - 4.2 Administrator Bezpieczeństwa Informacji 8
   - 4.3 Kierownicy Działów/komórek organizacyjnych 9
   - 4.4 Pracownik ds. Kadr 10
   - 4.5 Administrator Systemu Informatycznego 11
   - 4.6 Pracownicy MOSiR posiadający dostęp do danych osobowych 12
5. Procedura nadawania upoważnień do przetwarzania danych osobowych w zbiorach 12
6. Udostępnianie danych osobowych 14
7. Powierzenie przetwarzania danych osobowych 14
8. Wykaz budynków, pomieszczeń lub części pomieszczeń, tworzących obszar, w którym przetwarzane są dane osobowe 14
9. Wykaz zbiorów danych osobowych wraz ze wskazaniem programów zastosowanych do przetwarzania tych danych 16
10. Opis struktury zbiorów danych osobowych wskazujący zawartość poszczególnych pól informacyjnych i powiązania między nimi 16
11. Sposób przepływu danych osobowych pomiędzy poszczególnymi systemami informatycznymi 16
12. Środki techniczne i organizacyjne niezbędne dla zapewnienia poufności, integralności i rozliczalności przetwarzanych danych osobowych 16
13. Instrukcja alarmowa 17
14. Szkolenia użytkowników 18
15. Uwagi 19

1. Preambuła

Celem niniejszego dokumentu jest zapewnienie zgodności przetwarzania danych osobowych z polskim ustawodawstwem. Polityka Bezpieczeństwa Ochrony Danych Osobowych wraz z Instrukcją Zarządzania Systemem Informatycznym stanowi dokumentację przetwarzania danych osobowych w rozumieniu § 1 pkt 1 Rozporządzenia Ministra Spraw Wewnętrznych i Administracji z dnia 29 kwietnia 2004 r. w sprawie dokumentacji przetwarzania danych osobowych oraz warunków technicznych i organizacyjnych, jakim powinny odpowiadać urządzenia i systemy informatyczne służące do przetwarzania danych osobowych (Dz.U. 2004 nr 100, poz. 1024).

Polityka Bezpieczeństwa Ochrony Danych Osobowych wraz z Instrukcją Zarządzania Systemem Informatycznym stanowi dokumentację bezpieczeństwa w MOSiR. W kwestiach nieuregulowanych w dokumentacji bezpieczeństwa obowiązują wewnętrzne akty prawne.
Wszelkie wątpliwości dotyczące sposobu interpretacji postanowień niniejszego dokumentu, powinny być rozstrzygane na korzyść zapewnienia możliwie najwyższego poziomu ochrony danych osobowych oraz realizacji praw osób, których dane dotyczą.

Każda osoba która będzie przetwarzać dane osobowe z upoważnienia Administratora Danych Osobowych, zobowiązana jest do zapoznana się z Polityką Bezpieczeństwa Ochrony Danych Osobowych oraz do jej przestrzegania w zakresie wynikającym z przydzielonych zadań. Dotyczy to w szczególności pracowników zatrudnionych przez Administratora Danych Osobowych. Osoby o których mowa, zobowiązane są do złożenia na piśmie oświadczenia o zapoznaniu się z treścią Polityki Bezpieczeństwa Ochrony Danych Osobowych oraz do stosowania zawartych w niej postanowień.

Poprzez bezpieczeństwo danych osobowych należy rozumieć zapewnienie ich poufności, integralności, dostępności oraz rozliczalności, poprzez wdrożenie i eksploatację niezbędnych do tego celu mechanizmów technicznych i procedur organizacyjnych.
Atrybuty bezpieczeństwa danych osobowych należy rozumieć jako:

- poufność danych osobowych - zapewnienie, że dane osobowe są dostępne wyłącznie dla osób i podmiotów upoważnionych,
- integralność danych osobowych - zapewnienie, że dane osobowe są poprawne, kompletne oraz nie zostały zmienione lub zniszczone w sposób nieautoryzowany,
- dostępność danych osobowych – zapewnienie, że dane osobowe są osiągalne i możliwe do wykorzystania na żądanie, w założonym czasie, przez upoważnione osoby/podmioty,
- rozliczalność danych osobowych- zapewnienie, że działania osoby/podmiotu mogą być przypisane w sposób jednoznaczny tylko tej osobie/podmiotowi.

2. Zakres Polityki Bezpieczeństwa Ochrony Danych Osobowych

Dokument Polityki Bezpieczeństwa Ochrony Danych Osobowych opisuje zasady i procedury przetwarzania danych osobowych i ich zabezpieczenia przed nieuprawnionym dostępem. Jest to zestaw praw, reguł i praktycznych doświadczeń dotyczących sposobu zarządzania, ochrony i dystrybucji danych osobowych wewnątrz MOSiR. Polityka Bezpieczeństwa Ochrony Danych Osobowych, odnosi się całościowo do problemu zabezpieczenia danych osobowych tj. zarówno do zabezpieczenia danych przetwarzanych tradycyjnie, jak i danych przetwarzanych w systemach informatycznych.

Na Politykę Bezpieczeństwa Ochrony Danych Osobowych składają się następujące informacje:

1) wykaz miejsc, w których przetwarzane są dane osobowe,
2) wykaz zbiorów danych osobowych wraz ze wskazaniem programów zastosowanych do przetwarzania tych danych,
3) opis struktury zbiorów danych wskazujący zawartość poszczególnych pól informacyjnych i powiązania między nimi,
4) sposób przepływu danych pomiędzy poszczególnymi systemami,
5) określenie środków technicznych i organizacyjnych niezbędnych dla zapewnienia poufności, integralności i rozliczalności przetwarzanych danych.

Politykę Bezpieczeństwa Ochrony Danych Osobowych stosuje się do wszelkich czynności, stanowiących w myśl ustawy o ochronie danych osobowych, przetwarzanie danych osobowych. Bez względu na źródło pochodzenia danych osobowych, ich zakres, cel zebrania, sposób przetwarzania lub czas przetwarzania, należy stosować zasady przetwarzania danych osobowych opisane w niniejszym dokumencie, pod warunkiem, że przepisy prawa nie stanowią inaczej.

3. Definicje

Przez użyte w Polityce Bezpieczeństwa Ochrony Danych Osobowych określenia należy rozumieć:

Polityka Bezpieczeństwa Ochrony Danych Osobowych (Polityka ODO) - rozumie się przez to Politykę Bezpieczeństwa Ochrony Danych Osobowych w MOSiR.

Administrator Danych Osobowych (ADO) – Dyrektor Miejskiego Ośrodka Sportu i Rekreacji w Zielonej Górze z siedzibą przy ul. Sulechowskiej 41, 65-022 Zielona Góra, decydujący o celach i środkach przetwarzania danych osobowych.

Administrator Bezpieczeństwa Informacji (ABI) – osoba fizyczna nadzorująca z upoważnienia ADO przestrzeganie przepisów o ochronie danych osobowych, a w szczególności nadzorująca Administratora Systemu Informatycznego w zakresie bezpieczeństwa teleinformatycznego oraz kontrolującą bezpieczeństwo informacji, bezpieczeństwo danych

osobowych, zgodność z przepisami prawa dokumentacji ODO, procedur oraz procesów przetwarzania danych osobowych w zbiorach danych MOSiR.

Administrator Systemu Informatycznego (ASI) – pracownik odpowiedzialny za prawidłowe funkcjonowanie systemu informatycznego, sieci teleinformatycznej oraz za przestrzeganie zasad i wymagań bezpieczeństwa względem systemów informatycznych i sieci teleinformatycznych.

administrator systemu - osoba nadzorująca pracę systemu informatycznego oraz wykonująca w nim czynności wymagające specjalnych uprawnień.

baza danych osobowych - zbiór uporządkowanych powiązanych ze sobą tematycznie danych zapisanych np. w pamięci zewnętrznej komputera. Baza danych jest złożona z elementów o określonej strukturze - rekordów lub obiektów, w których są zapisane dane osobowe.

dane osobowe - wszelkie informacje dotyczące zidentyfikowanej lub możliwej do zidentyfikowania osoby fizycznej.

dokumentacja bezpieczeństwa - Polityka Bezpieczeństwa Ochrony Danych Osobowych oraz Instrukcja Zarządzania Systemem Informatycznym.

Dział/komórka organizacyjna - dział lub samodzielne stanowisko pracy w MOSiR, wskazane w Regulaminie Organizacyjnym MOSiR w Zielonej Górze.

Instrukcja Zarządzania Systemem Informatycznym (IZSI) - Instrukcja Zarządzania Systemem Informatycznym służącym do przetwarzania danych osobowych w MOSiR.

MOSiR – Miejski Ośrodek Sportu i Rekreacji w Zielonej Górze z siedzibą przy ul. Sulechowskiej 41, 65-022 Zielona Góra.

odbiorca danych - rozumie się przez to każdego, komu udostępnia się dane osobowe, z wyłączeniem:

- osoby, której dane dotyczą,
- osoby upoważnionej do przetwarzania danych,
- przedstawiciela, o którym mowa w art. 31a ustawy o ochronie danych osobowych,
- podmiotu, o którym mowa w art. 31 ustawy o ochronie danych osobowych,
- organów państwowych lub organów samorządu.

ODO - ochrona danych osobowych w MOSiR.

pracownik ds. Kadr - osoba, która zajmuje się w MOSiR prowadzeniem dokumentacji personalnej, sporządzaniem dokumentacji związanej z przebiegiem zatrudnienia oraz obsługą pracowników w zakresie umów o pracę.

przetwarzanie danych osobowych (przetwarzanie) - wykonywanie jakichkolwiek operacji na danych osobowych, np. zbieranie, utrwalanie, opracowywanie, udostępnianie, zmienianie, usuwanie.

Podmiot zewnętrzny - osoba fizyczna bądź prawna świadczącą usługi na rzecz MOSiR jak również osoba fizyczna bądź prawna współpracującą z MOSiR.

Rozporządzenie - Rozporządzenie Ministra Spraw Wewnętrznych i Administracji z dnia 29 kwietnia 2004 r. w sprawie dokumentacji przetwarzania danych osobowych oraz warunków technicznych i organizacyjnych, jakim powinny odpowiadać urządzenia i systemy informatyczne służące do przetwarzania danych osobowych (Dz.U. z 2004 r. nr 100, poz. 1024).

system informatyczny - zespół współpracujących ze sobą urządzeń, programów, procedur przetwarzania informacji i narzędzi programowych zastosowanych w celu przetwarzania danych.

system teleinformatyczny - system informacyjny, w którym chociaż jeden z jego procesów odbywa się w formie elektronicznej, system, który tworzą urządzenia, narzędzia, metody postępowania i procedury stosowane przez wyspecjalizowanych pracowników, w sposób zapewniający wytwarzanie, przechowywanie, przetwarzanie lub przekazywanie informacji.

usuwanie danych osobowych - rozumie się przez to zniszczenie danych osobowych lub taką ich modyfikację , która nie pozwoli na ustalenie tożsamości osoby, której dane dotyczą.

Ustawa - rozumie się przez to ustawę z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (Dz.U. 2015 r. poz. 2135 z późn. zm.).

użytkownik systemu - pracownik upoważniony do korzystania z systemu informatycznego, a w przypadku przetwarzania danych osobowych - posiadający pisemne upoważnienie wydane przez ADO lub osoby upoważnione przez ADO.

zabezpieczenie systemu informatycznego - należy przez to rozumieć wdrożenie stosownych środków administracyjnych, technicznych i fizycznych w celu zabezpieczenia zasobów technicznych oraz ochrony przed modyfikacją, zniszczeniem, nieuprawnionym dostępem i ujawnieniem lub pozyskaniem danych osobowych, a także ich utratą,

zbiór danych osobowych - zestaw danych osobowych posiadający określoną strukturę, prowadzony wg określonych kryteriów oraz celów.

zgoda osoby, której dane dotyczą - rozumie się przez to oświadczenie woli, którego treścią jest zgoda na przetwarzanie danych osobowych tego, kto składa oświadczenie; zgoda nie może być domniemana lub dorozumiana z oświadczenia woli o innej treści.

4. Osoby odpowiedzialne za ochronę danych osobowych

Za przetwarzanie danych osobowych oraz ich ochronę zgodnie z postanowieniami Ustawy, Rozporządzenia, Polityki ODO oraz Instrukcji Zarządzania Systemem Informatycznym odpowiadają:

a) Administrator Danych Osobowych,
b) Administrator Bezpieczeństwa Informacji,
c) Administrator Systemów Informatycznych,
d) kierownicy Działów/komórek organizacyjnych,

e) każda osoba będąca pracownikiem MOSiR, w rozumieniu przepisów kodeksu pracy, która uzyskała upoważnienie do przetwarzania danych osobowych,
f) praktykanci i stażyści którym powierzono przetwarzanie danych osobowych,
g) Podmioty zewnętrzne którym powierzono przetwarzanie danych osobowych.

4.1 Administrator Danych Osobowych

4.1.1 Administratorem Danych Osobowych jest Dyrektor Miejskiego Ośrodka Sportu i Rekreacji w Zielonej Górze z siedzibą przy ul. Sulechowskiej 41, 65-022 Zielona Góra.

4.1.2 Zmiany na stanowisku Dyrektora MOSiR nie wymagają zmiany Polityki Bezpieczeństwa Ochrony Danych Osobowych.

4.2 Administrator Bezpieczeństwa Informacji

4.2.1 Funkcję ABI w MOSiR z siedzibą w Zielonej Górze pełni osoba wskazana przez ADO.

4.2.2 Zmiana osoby pełniącej funkcję Administratora Bezpieczeństwa Informacji następuje na skutek pisemnej decyzji Administratora Danych Osobowych.

4.2.3 Do najważniejszych zadań ABI należy:

a) sprawdzanie zgodności przetwarzania danych osobowych z przepisami o ochronie danych osobowych oraz opracowanie w tym zakresie sprawozdania dla ADO,
b) nadzorowanie opracowania i aktualizowania dokumentacji bezpieczeństwa, oraz przestrzegania zasad w niej określonych,
c) zapewnianie zapoznania osób upoważnionych do przetwarzania danych osobowych z przepisami o ochronie danych osobowych,
d) prowadzenie rejestru zbiorów danych przetwarzanych przez administratora danych, z wyjątkiem zbiorów zawierających dane wrażliwe.

4.2.4 Pozostałe zadania ABI:

a) organizacja ochrony danych osobowych,
b) monitorowanie działania i skuteczności zabezpieczeń wdrożonych w celu ochrony danych osobowych,
c) opiniowanie w sprawie możliwości oraz prawidłowości zbierania danych osobowych w celu utworzenia zbioru danych osobowych, zbierania nowych kategorii danych do istniejącego już zbioru,
d) opiniowanie umów dotyczących powierzenia przetwarzanych danych,
e) udzielanie Generalnemu Inspektorowi Ochrony Danych Osobowych lub innym organom odpowiedzi i wyjaśnień w sprawie zbiorów danych osobowych przetwarzanych w MOSiR,

f) udział w kontrolach prowadzonych przez inspektorów Biura Generalnego Inspektora Ochrony Danych Osobowych,

g) udzielanie odpowiedzi na zapytania kierowane do MOSiR przez Podmioty zewnętrzne, dotyczące administrowanych zbiorów danych osobowych,

h) informowanie osób zgłaszających zastrzeżenia w związku z przetwarzaniem ich danych osobowych o legalności procesu przetwarzania danych – o podstawie prawnej,

i) prowadzenie postępowania wyjaśniającego w przypadku naruszenia ochrony danych osobowych,

j) wyznaczanie w porozumieniu z ADO terminów szkoleń oraz określanie formy szkoleń z zakresu ochrony danych osobowych,

4.2.5 Do uprawnień Administratora Bezpieczeństwa Informacji należy:

a) wydawanie pisemnych/ustnych zaleceń wszelkim osobom przetwarzającym dane osobowe celem przetwarzania ich zgodnie z Ustawą, Rozporządzeniem, Polityką ODO oraz Instrukcją Zarządzania Systemem Informatycznym służącym do przetwarzania danych osobowych,

b) inicjowanie wykonania zadań związanych z ODO,

c) wstęp do pomieszczeń, w których zlokalizowane są zbiory danych osobowych w celu oceny zgodności przetwarzania danych osobowych z Ustawą,

d) wgląd do dokumentów mających bezpośredni związek z problematyką przetwarzania danych osobowych,

e) wgląd do urządzeń, nośników oraz systemów informatycznych służących do przetwarzania danych osobowych (w obecności ASI lub upoważnionego pracownika).

4.3 Kierownicy Działów/komórek organizacyjnych

4.3.1 Do najważniejszych obowiązków kierowników Działów w zakresie ochrony danych osobowych należy:

a) nadzór nad realizacją zadań wynikających z Polityki ODO i IZSI w stosunku do podległych im pracowników, stażystów, praktykantów a w szczególności:

- wskazanie pracownikowi ds. Kadr wymaganego zakresu upoważnienia do przetwarzania danych osobowych podległego im pracownika,
- przekazanie pracownikowi, przed dopuszczeniem do przetwarzania danych osobowych, dokumentacji bezpieczeństwa (Polityki ODO oraz IZSI),

- zapewnienie podpisania przez pracownika oświadczenia o zapoznaniu się z dokumentacją bezpieczeństwa przed dopuszczeniem go do przetwarzania danych osobowych *Załącznik P4 Oświadczenie użytkownika,*
- przekazanie oświadczenia o którym mowa powyżej pracownikowi ds. Kadr,
- wnioskowanie o rejestrację/zmianę uprawnień pracownika w systemie informatycznym. Wniosek o wyrejestrowanie użytkownika z sytemu informatycznego należy przekazać ASI.

b) w zakresie podległych im Działów, poinformowanie bez zbędnej zwłoki innych ADO, którym udostępniono zbiór danych, o dokonanym uaktualnieniu lub sprostowaniu danych.

c) w zakresie podległych im Działów, zapewnienie w podpisywanych umowach zapisów bezpieczeństwa dot. powierzenia przetwarzania danych osobowych, zachowania w poufności danych osobowych, w przypadku gdy realizacja umowy, będzie wiązać się z dostępem przez Podmiot zewnętrzny do danych osobowych *Załącznik P5 Umowa powierzenia, Załącznik P6 Umowa o poufności.*

Uwaga:
Osoby upoważnione do przetwarzania danych osobowych podpisują Załącznik P4 Oświadczenie – „Oświadczenie użytkownika".
Obsługa techniczna (sprzątaczki, pracownicy gospodarczy) podpisuje Załącznik P4 Oświadczenie – „Oświadczenie obsługi technicznej".

4.4 Pracownik ds. Kadr

4.4.1 Do najważniejszych obowiązków pracownika ds. Kadr w zakresie ochrony danych osobowych należy:

a) gromadzenie oświadczeń pracowników o zapoznaniu się z dokumentacją bezpieczeństwa oraz zachowaniu w tajemnicy służbowej wszelkich informacji nie będących informacją publiczną lub informacją powszechnie dostępną *Załącznik P4 Oświadczenie,*

b) gromadzenie upoważnień do przetwarzania danych osobowych *Załącznik P7 Upoważnienie do przetwarzania danych osobowych,*

c) prowadzenie ewidencji osób upoważnionych do przetwarzania danych osobowych *Załącznik P8 Ewidencja upoważnień do przetwarzania danych osobowych.*

d) poinformowanie bez zbędnej zwłoki innych ADO, którym udostępniono zbiór danych, o dokonanym uaktualnieniu lub sprostowaniu danych,

e) współpraca z ADO oraz ABI, ASI oraz kierownikami Działów w zakresie tworzenia i gromadzenia dokumentacji pracowników, wymaganej przez Politykę ODO i Instrukcję Zarządzania Systemem Informatycznym.

4.5 Administrator Systemu Informatycznego

4.5.1 Do uprawnień i obowiązków Administratora Systemów Informatycznych w zakresie ochrony danych osobowych należą, w szczególności:

a) zapewnienie prawidłowego funkcjonowania systemów informatycznych,

b) stosowanie zasad i wymagań bezpieczeństwa systemów informatycznych zawartych w Instrukcji Zarządzania Systemem Informatycznym oraz odrębnych procedurach,

c) nadawanie/usuwanie/modyfikacja uprawnień do przetwarzania danych osobowych w systemach informatycznych,

d) stosowaniem środków zapewniających bezpieczeństwo przetwarzania danych osobowych w systemach informatycznych, a w szczególności przeciwdziałających dostępowi osób niepowołanych do tych systemów,

e) podejmowanie odpowiednich działań w przypadku wykrycia naruszeń w systemie zabezpieczeń,

f) identyfikacja i analiza zagrożeń, na które może być narażone przetwarzanie danych osobowych w systemach informatycznych,

g) sprawowanie nadzoru nad kopiami zapasowymi opisanymi w Procedurze tworzenia kopii zapasowych,

h) inicjowanie i nadzór nad wdrażaniem nowych narzędzi, procedur organizacyjnych oraz sposobów zarządzania systemami informatycznymi, które mają doprowadzić do wzmocnienia bezpieczeństwa przy przetwarzaniu danych osobowych w systemach informatycznych,

i) podejmowanie innych czynności w zakresie zabezpieczenia przetwarzania danych w systemach informatycznych, o których mowa w Instrukcji Zarządzania Systemem Informatycznym,

j) informowanie Administratora Bezpieczeństwa Informacji o konieczności wprowadzenia zmian w Instrukcji Zarządzania Systemem Informatycznym z powodu np. zmian procedur tworzenia kopii zapasowych lub zmiany zabezpieczeń systemów informatycznych.

4.6 Pracownicy MOSiR posiadający dostęp do danych osobowych

4.6.1 Każdy pracownik, który uzyskał upoważnienie do przetwarzania danych osobowych, zobowiązany jest do ich ochrony w sposób zgodny z przepisami Ustawy, Rozporządzenia, Polityki Bezpieczeństwa Ochrony Danych Osobowych, Instrukcji Zarządzania Systemem Informatycznym.

4.6.2 Dostęp do określonego zbioru danych osobowych pracownik MOSiR uzyskuje na podstawie pisemnego upoważnienia, otrzymanego w trybie określonym w pkt 5 niniejszej Polityki ODO.

4.6.3 Pracownicy zatrudnieni - na podstawie umowy o pracę, bądź świadczący usługi na podstawie umów cywilnoprawnych - przy przetwarzaniu danych osobowych zobowiązani są do zachowania w tajemnicy danych osobowych oraz sposobów ich zabezpieczenia. Obowiązek ten istnieje także po ustaniu zatrudnienia.

4.6.4 Naruszenie obowiązku ochrony danych osobowych, a w szczególności obowiązku zachowania danych osobowych w tajemnicy, skutkuje poniesieniem odpowiedzialności karnej na podstawie przepisów Ustawy oraz stanowi ciężkie naruszenie obowiązków pracowniczych i może być podstawą rozwiązania stosunku pracy w trybie art. 52 Kodeksu Pracy.

5. Procedura nadawania upoważnień do przetwarzania danych osobowych w zbiorach

5.1 MOSiR realizując niniejszą Politykę Bezpieczeństwa Ochrony Danych Osobowych w zakresie udostępniania danych osobowych w ramach własnej (wewnętrznej) struktury, zezwala na ich przetwarzanie w systemie informatycznym lub w wersji papierowej wyłącznie pracownikom, którzy uzyskali uprzednio stosowne upoważnienie do przetwarzania danych osobowych.

5.2 Upoważnienie do przetwarzania danych osobowych mogą uzyskać pracownicy, praktykanci, stażyści oraz zleceniobiorcy MOSiR.

5.3 Upoważnienie do przetwarzania danych osobowych wydawane jest każdemu z pracowników osobno, w zakresie adekwatnym do pełnionych obowiązków służbowych.

5.4 Upoważnienie do przetwarzania danych osobowych nadaje Administrator Danych Osobowych.

5.5 Upoważnienia do przetwarzania danych osobowych gromadzi pracownik ds. Kadr.

5.6 Upoważnienia wydawane są zgodnie z następującą procedurą:

a) kierownicy Działów, przed dopuszczeniem pracownika do przetwarzania danych osobowych, przekazują do zapoznania się Politykę Bezpieczeństwa Ochrony Danych Osobowych oraz Instrukcję Zarządzania Systemem Informatycznym,

b) pracownik przed nadaniem mu upoważnienia, poświadcza na piśmie zapoznanie się z obowiązującą Polityką Bezpieczeństwa Ochrony Danych Osobowych oraz Instrukcją Zarządzania Systemem Informatycznym. Za zapoznanie się z ww. dokumentacją bezpieczeństwa oraz podpisanie oświadczenia o którym mowa powyżej, odpowiadają kierownicy Działów w zakresie podległych im pracowników,

c) kierownicy Działów wskazują pracownikowi ds. Kadr w jakim zakresie podległy im pracownik powinien uzyskać upoważnienie,

d) pracownik ds. Kadr wypełnia upoważnienie do przetwarzania danych osobowych wg wytycznych kierowników Działów i przedkłada do podpisu ADO.

e) za wskazanie pracownikowi ds. Kadr zakresu upoważnienia do przetwarzania danych osobowych kierowników Działów odpowiadają sami kierownicy Działów, z tą różnicą, że zakres upoważnienia najpierw weryfikuje a następnie podpisuje ADO.

5.7 Upoważnienie jest drukowane w dwóch egzemplarzach, z których każdy musi być podpisany przez pracownika, któremu nadano upoważnienie.

5.8 Jeden egzemplarz upoważnienia jest przechowywany jako część dokumentacji kadrowej przez pracownika ds. Kadr, drugi jest wydawany pracownikowi, któremu nadano upoważnienie.

5.9 Kierownicy Działów, w zakresie podległych im pracowników, zobowiązani są do poinformowania ASI o konieczności nadania, zmiany oraz cofnięcia dostępu do przetwarzania danych osobowych w zbiorach przetwarzanych w systemach informatycznych.

5.10 Tryb nadania, zmiany, odebrania uprawnień do systemów informatycznych przetwarzających dane osobowe zawiera Instrukcja Zarządzania Systemem Informatycznym

5.11 Utrata prawa do przetwarzania danych osobowych określonych w upoważnieniu następuje w szczególności w przypadku:

a) zmiany stanowiska pracy w MOSiR na stanowisko, na którym nie ma konieczności posiadania dostępu do danych osobowych lub w szczególności, gdy ustaje zasadność i celowość dalszego wykonywania prawa do przetwarzania danych w związku ze zmianą realizowanych przez pracownika zadań wynikających z jego indywidualnego zakresu czynności,

b) umyślnego naruszenia zasad ochrony danych osobowych określonych w Ustawie, Rozporządzeniu, Polityce Bezpieczeństwa Ochrony Danych Osobowych, Instrukcji Zarządzania Systemem Informatycznym,

c) rozwiązania stosunku pracy,

d) rozwiązania umowy cywilnoprawnej.

6. Udostępnianie danych osobowych

6.1 Udostępnianie danych osobowych, nie będących informacją publiczną, wymaga zachowania szczególnej staranności. Udostępnienie danych osobowych przez MOSiR należy realizować na piśmie.

6.2 Szczegóły dot. udostępniania danych zawarto w Instrukcji Zarządzania Systemem Informatycznym.

7. Powierzenie przetwarzania danych osobowych

7.1 Dopuszcza się, by dane osobowe których Administratorem Danych Osobowych jest MOSiR, były przetwarzane przez Podmioty zewnętrzne. Może się to odbywać wyłącznie poprzez:

a) powierzenie danego zbioru w określonym celu i zakresie Podmiotowi zewnętrznemu na mocy umowy powierzenia przetwarzania danych osobowych lub zamieszczenie stosownych zapisów w umowie z podmiotem,

b) podpisanie umowy o poufności lub wprowadzenie stosownych zapisów o poufności do umowy z podmiotem, w przypadku gdy Podmiot zewnętrzny będzie przetwarzać dane wyłącznie na terenie MOSiR.

7.2 Pisemna umowa powierzenia przetwarzania danych osobowych, o której mowa w niniejszym punkcie musi być zgodna z postanowieniami art. 31 Ustawy.

7.3 W przypadku, gdy powierzenie danych osobowych wynika wprost z zawartej z danym podmiotem umowy, nie ma konieczności sporządzania dodatkowo pisemnej umowy powierzenia danych osobowych.

8. Wykaz budynków, pomieszczeń lub części pomieszczeń, tworzących obszar, w którym przetwarzane są dane osobowe

8.1 Lokalizacja obiektów tworzących obszar przetwarzania danych osobowych:

Lokalizacja nr 1: Centrum Rekreacyjno-Sportowe (CRS)
ul. Sulechowskiej 41, 65-022 Zielona Góra
Obszary przetwarzania danych osobowych w Lokalizacji nr 1:

- Centrum Obsługi Klienta
- Kasy,
- dział finansowo – księgowy,
- dział administracyjny,
- dział techniczny zespołu obiektów,
- dział sportu i marketingu,

- Serwerownie.

Lokalizacja nr 2: Stadion Żużlowy (W69)
ul. Wrocławska 69, 65-218 Zielona Góra
Obszary przetwarzania danych osobowych w Lokalizacji nr 2:

- Serwerownie.

Lokalizacja nr 3: Hala Akrobatyczno-Sportowa
ul. Urszuli 22, 65-147 Zielona Góra
Obszary przetwarzania danych osobowych w Lokalizacji nr 3:

- Portiernia/Pomieszczenie obsługi technicznej.

Lokalizacja nr 4: Hala lekkoatletyczna
ul. Sulechowska Boczna, 66-036 Zielona Góra
Obszary przetwarzania danych osobowych w Lokalizacji nr 4:

- Pomieszczenie obsługi technicznej/Punkt sprzedaży.

Lokalizacja nr 5: Korty tenisowe
ul. Sulechowska, 65-036 Zielona Góra
Obszary przetwarzania danych osobowych w Lokalizacji nr 5:

- Pomieszczenie trenerów.

Lokalizacja nr 6: Kompleks sportowy
ul. Wyspiańskiego 17, 65-036 Zielona Góra
Obszary przetwarzania danych osobowych w Lokalizacji nr 6:

- Pomieszczenie specjalisty kompleksu sportowego/Punkt sprzedaży.

Lokalizacja nr 7: Ośrodek jeździecki
ul. Stajenna 22, 66-004 Zielona Góra
Obszary przetwarzania danych osobowych w Lokalizacji nr 7:

- Pomieszczenie specjalisty ds. obsługi obiektu

Lokalizacja nr 8: Centrum Promocji i Informacji Turystycznej
ul. Stary Rynek 1, 65-067 Zielona Góra
Obszary przetwarzania danych osobowych w Lokalizacji nr 8:

- Pomieszczenia biurowe.

Lokalizacja nr 9: Pawilon biurowy
ul. Urszuli, 65-147 Zielona Góra
Obszary przetwarzania danych osobowych w Lokalizacji nr 9:

- Archiwum.

Lokalizacja nr 10: Centrum Promocji i Informacji Turystycznej
ul. Wrocławska 12a, 65-427 Zielona Góra
Obszary przetwarzania danych osobowych w Lokalizacji nr 10:

- Punkt informacyjny.

9. Wykaz zbiorów danych osobowych wraz ze wskazaniem programów zastosowanych do przetwarzania tych danych

Wykaz zbiorów danych w postaci dokumentacji papierowej i elektronicznej wraz ze wskazaniem programów zastosowanych do przetwarzania tych danych, zmieszczono w *Załączniku P1 Wykaz zbiorów danych osobowych wraz ze wskazaniem programów stosowanych do przetwarzania tych danych.*

10. Opis struktury zbiorów danych osobowych wskazujący zawartość poszczególnych pól informacyjnych i powiązania między nimi

Opis struktury zbiorów danych osobowych przedstawiono w *Załączniku P2 Opis struktury zbiorów danych osobowych.*

11. Sposób przepływu danych osobowych pomiędzy poszczególnymi systemami informatycznymi

Sposób przepływu danych osobowych pomiędzy poszczególnymi systemami informatycznymi, w których przetwarzane są dane osobowe przedstawiono w *Załączniku P3 Sposób przepływu danych.*

12. Środki techniczne i organizacyjne niezbędne dla zapewnienia poufności, integralności i rozliczalności przetwarzanych danych osobowych

12.1 Zabezpieczenia organizacyjne:

a) wyznaczono Administratora Systemów Informatycznych oraz Administratora Bezpieczeństwa Informacji,
b) opracowano Politykę Bezpieczeństwa Ochrony Danych Osobowych,
c) opracowano Instrukcję Zarządzania Systemem Informatycznym,
d) dopuszczenie do przetwarzania danych osobowych wyłącznie osoby posiadające upoważnienia,
e) prowadzenie ewidencji osób upoważnionych do przetwarzania danych osobowych,

f) osoby zatrudnione przy przetwarzaniu danych osobowych zostały zaznajomione z przepisami dotyczącymi ODO oraz z przepisami w zakresie zabezpieczeń systemów informatycznych przetwarzających dane osobowe,

g) osoby zatrudnione przy przetwarzaniu danych zobowiązane zostały do zachowania ich w tajemnicy,

h) stosuje się pisemne umowy powierzenia oraz umowy o poufności dla współpracy z podwykonawcami przetwarzającymi dane osobowe lub stosowne zapisy w umowach.

12.2 Zabezpieczenia ochrony fizycznej danych osobowych:

a) budynek MOSiR chroniony jest przez pracownika ochrony, przebywającego na obiekcie przez całą dobę,

b) szafy z dokumentacją zamykane są na klucz,

c) drzwi do pomieszczeń biurowych zamykane są na klucz,

d) monitory w miarę możliwości są skierowane tak, aby podgląd tego co wyświetla się na ekranie, miał wyłącznie użytkownik pracujący na danej jednostce komputerowej.

12.3 Zabezpieczenia sprzętowe infrastruktury informatycznej i telekomunikacyjnej.

Zabezpieczenia stosuje się dla fizycznych elementów systemu informatycznego, ich połączeń oraz systemów operacyjnych. Szczegółowy opis zabezpieczeń zawarty jest w Instrukcji Zarządzania Systemem Informatycznym.

12.4 Zabezpieczenia narzędzi programowych i baz danych.

Zabezpieczenia (techniczne i programowe) stosuje się dla procedur, aplikacji, programów i innych narzędzi programowych przetwarzających dane osobowe. Szczegółowy opis zabezpieczeń zawarty jest w Instrukcji Zarządzania Systemem Informatycznym.

13. Instrukcja alarmowa

Instrukcja opisuje postępowanie w razie zaistnienia zagrożenia dla bezpieczeństwa przetwarzanych danych osobowych lub naruszenia zasad przetwarzania danych osobowych oraz zawiera wykaz typowych zagrożeń i incydentów zagrażających bezpieczeństwu danych osobowych.
Celem instrukcji jest minimalizacja skutków wystąpienia incydentów bezpieczeństwa, ograniczenie ryzyka powstania zagrożeń i występowania incydentów w przyszłości.

13.1 Każdy pracownik MOSiR w przypadku stwierdzenia zagrożenia lub naruszenia ochrony danych osobowych, zobowiązany jest niezwłocznie poinformować bezpośredniego przełożonego. Przełożony niezwłocznie informuje o incydencie/zagrożeniu/naruszeniu ABI.

13.2 W przypadku stwierdzenia naruszenia bezpieczeństwa danych osobowych w systemach informatycznych pracownik, zobowiązany jest niezwłocznie poinformować bezpośredniego przełożonego oraz ASI. ASI niezwłocznie informuje o incydencie/zagrożeniu/naruszeniu ABI.

13.3 Do typowych zagrożeń bezpieczeństwa danych osobowych należą:

a) niewłaściwe zabezpieczenie fizyczne pomieszczeń, urządzeń i dokumentów,

b) niewłaściwe zabezpieczenie sprzętu IT, oprogramowania przed wyciekiem, kradzieżą i utratą danych osobowych,

c) nieprzestrzeganie zasad ochrony danych osobowych przez pracowników np. niestosowanie zasady czystego biurka/ekranu, ochrony haseł.

13.4 Do typowych incydentów naruszenia bezpieczeństwa danych osobowych należą:

a) zdarzenia losowe zewnętrzne (pożar obiektu/pomieszczenia, zalanie wodą, utrata zasilania, utrata łączności),

b) zdarzenia losowe wewnętrzne (awarie serwera, komputerów, twardych dysków, oprogramowania, pomyłki informatyków, użytkowników, utrata/zagubienie danych),

c) umyślne incydenty (włamanie do systemu informatycznego lub pomieszczeń, kradzież danych/sprzętu, wyciek informacji, ujawnienie danych osobom nieupoważnionym, świadome zniszczenie dokumentów/danych, działanie wirusów i innego szkodliwego oprogramowania).

13.5 ABI przeprowadza sprawdzenie doraźne po:

a) stwierdzeniu naruszenia bezpieczeństwa danych osobowych

b) stwierdzeniu wystąpienia zagrożenia

c) powzięciu uzasadnionego podejrzenia, że naruszenie miało miejsce.

Sprawdzenie jest dokonywane możliwie jak najszybciej.

14. Szkolenia użytkowników

14.1 Każdy użytkownik powinien cyklicznie uczestniczyć w szkoleniu z zakresu ochrony danych osobowych w zbiorach elektronicznych i papierowych.

14.2 Szkolenia prowadzi ABI lub inna osoba posiadająca odpowiednie kompetencje z zakresu ochrony danych.

14.3 Zakres szkolenia powinien obejmować zaznajomienie użytkownika z przepisami Ustawy oraz wydanymi na jej podstawie aktami wykonawczymi oraz dokumentacją bezpieczeństwa obowiązującą u Administratora Danych Osobowych.

14.4 Uczestnictwo w szkoleniu użytkowników wymaga pisemnego potwierdzenia wzięcia udziału w szkoleniu poprzez wpisanie się na listę obecności.

15. Uwagi

15.1 Kierownicy Działów są obowiązani zapoznać każdego pracownika z treścią Polityki Bezpieczeństwa Ochrony Danych Osobowych oraz Instrukcji Zarządzania Systemem Informatycznym.

15.2 Wszystkie regulacje dotyczące systemów informatycznych, określone w Polityce Bezpieczeństwa Ochrony Danych Osobowych dotyczą również przetwarzania danych w bazach danych osobowych prowadzonych w jakiejkolwiek innej formie.

15.3 Użytkownicy zobowiązani są do stosowania przy przetwarzaniu danych postanowień zawartych w niniejszej Polityce Bezpieczeństwa Ochrony Danych Osobowych.

15.4 Przypadki, nieuzasadnionego zaniechania obowiązków wynikających z niniejszego dokumentu potraktowane będą jako ciężkie naruszenie obowiązków pracowniczych.

15.5 Wobec osoby, która w przypadku naruszenia zabezpieczeń systemu informatycznego lub uzasadnionego domniemania takiego naruszenia nie podjęła działania określonego w niniejszym dokumencie, a w szczególności nie powiadomiła odpowiedniej osoby zgodnie z określonymi zasadami, a także, gdy nie zrealizowała stosownego działania dokumentującego ten przypadek, można wszcząć postępowanie dyscyplinarne.

15.6 Kara dyscyplinarna orzeczona wobec osoby uchylającej się od powiadomienia nie wyklucza odpowiedzialności karnej tej osoby, zgodnie z Ustawą oraz możliwości wniesienia wobec niej sprawy z powództwa cywilnego przez pracodawcę o zrekompensowanie poniesionych strat.

15.7 W sprawach nieuregulowanych w niniejszej Polityce Bezpieczeństwa Ochrony Danych Osobowych mają zastosowanie przepisy ustawy z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (Dz.U. 2015 r. poz. 2135 z późn. zm.), oraz wydanych na jej podstawie aktów wykonawczych.