

**Polityka Bezpieczeństwa Danych Osobowych
w Zespole Szkół Mistrzostwa Sportowego nr 2**

Al. Niepodległości 32

61-714 Poznań

SPIS TREŚCI

1. CEL POLITYKI BEZPIECZEŃSTWA DANYCH OSOBOWYCH	3
2. PODSTAWOWE POJĘCIA I DEFINICJE	3
3. PODSTAWY PRAWNE OCHRONY DANYCH OSOBOWYCH	5
4. DEKLARACJA ZGODNOŚCI	5
5. PODZIAŁ OBOWIĄZKÓW W ZAKRESIE OCHRONY DANYCH OSOBOWYCH	5
6. REJESTR CZYNNOŚCI PRZETWARZANIA DANYCH OSOBOWYCH	7
7. ŚRODKI TECHNICZNE I ORGANIZACYJNE OCHRONY DANYCH OSOBOWYCH	8
8. REALIZACJA OBOWIĄZKU INFORMACYJNEGO	9
9. PRAWA OSÓB, KTÓRYCH DANE SĄ PRZETWARZANE PRZEZ ORGANIZACJĘ	11
10. REALIZACJA UDOSTĘPNIENÍ DANYCH OSOBOWYCH	13
11. ZASADY POWIERZANIA DANYCH OSOBOWYCH	13
12. NARUSZENIA OCHRONY DANYCH OSOBOWYCH	14
13. AUDYT OCHRONY DANYCH OSOBOWYCH	15
14. SZKOLENIA	16
15. RETENCJA DANYCH	16
16. ZGODY NA PRZETWARZANA DANYCH OSOBOWYCH	17
17. UPOWAŻNIENIA DO PRZETWARZANIA DANYCH OSOBOWYCH	18
18. ANALIZA RYZYKA PROCESÓW PRZETWARZANIA DANYCH OSOBOWYCH	18

1. CEL POLITYKI BEZPIECZEŃSTWA DANYCH OSOBOWYCH

1.1. Zespół Szkół Mistrzostwa Sportowego nr 2 z siedzibą przy al. Niepodległości 32

61-714 Poznań jako Administrator przetwarzanych w Organizacji danych osobowych jest zobowiązany do zapewnienia przestrzegania mających zastosowanie regulacji prawnych w obszarze ochrony danych osobowych.

1.2. Celem niniejszej Polityki Bezpieczeństwa Danych Osobowych jest określenie ról, odpowiedzialności, zasad i standardów, które zapewnią, że przetwarzanie danych osobowych w **Zespole Szkół Mistrzostwa Sportowego nr 2** będzie odbywać się zgodnie z regulacjami prawnymi obowiązującymi na terenie Rzeczypospolitej Polskiej.

1.3. Niniejsza Polityka Bezpieczeństwa Danych Osobowych ma zastosowanie dla:

1.3.1. wszystkich informacji stanowiących dane osobowe,

1.3.2. wszystkich nośników zawierających dane osobowe, niezależnie od ich formy i postaci,

1.3.3. wszystkich sposobów przechowywania i przekazywania informacji zawierających dane osobowe,

1.3.4. wszystkich pracowników i współpracowników **Zespołu Szkół Mistrzostwa Sportowego nr 2**, których obowiązki wymagają przetwarzania danych osobowych,

1.3.5. wszystkich lokalizacji i pomieszczeń **Zespołu Szkół Mistrzostwa Sportowego nr 2**, w których przetwarzane są dane osobowe.

1.4. Każda z osób przetwarzających dane ze zbiorów danych osobowych **Zespołu Szkół Mistrzostwa Sportowego nr 2** zobowiązana jest znać i przestrzegać przepisy powszechnie obowiązujące, dotyczące ochrony danych osobowych, niezależnie od postanowień niniejszego dokumentu.

1.5. Niniejszy dokument zawiera zestaw wymagań przyjętych w Organizacji, niezbędnych do zapewnienia zgodności z mającymi zastosowanie regulacjami prawnymi.

2. PODSTAWOWE POJĘCIA I DEFINICJE

Administrator Danych Osobowych - oznacza osobę fizyczną lub prawną, organ publiczny, jednostkę lub inny podmiot, który samodzielnie lub wspólnie z innymi ustala cele i sposoby przetwarzania danych osobowych; Administrator Danych Osobowych to **Zespół Szkół Mistrzostwa Sportowego nr 2** reprezentowany przez **Annę Mrówczyńską Dyrektora**

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;

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;

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 danych osobowych przez 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;

Organ nadzorczy - oznacza niezależny organ publiczny ustanowiony przez państwo członkowskie zgodnie z art. 51 Rozporządzenia – Urząd Ochrony Danych Osobowych;

Podmiot przetwarzający - oznacza osobę fizyczną lub prawną, organ publiczny, jednostkę lub inny podmiot, który przetwarza dane osobowe w imieniu administratora;

Podmiot zewnętrzny – to osoba fizyczna, jednostka organizacyjna nieposiadająca osobowości prawnej lub osoba prawna z siedzibą w Polsce lub za granicą, organ administracji publicznej, oraz inne podmioty wykonujące zadania na rzecz organizacji, w tym konsultanci, doradcy i inne osoby w nich zatrudnione;

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 - 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;

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;

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 - osoba, której dane dotyczą wyraża dobrowolne, konkretne, świadome i jednoznaczne okazanie woli, w którym w formie oświadczenia lub wyraźnego działania potwierdzającego, przyzwala na przetwarzanie dotyczących jej danych osobowych;

3. PODSTAWY PRAWNE OCHRONY DANYCH OSOBOWYCH

3.1. Podstawę prawną zasad określonych w niniejszej Polityce stanowią w szczególności:

3.1.1. Ustawa z dnia 10 maja 2018r. o ochronie danych osobowych (Dz. U. 2018r. poz. 1000);

3.1.2. Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE

4. DEKLARACJA ZGODNOŚCI

4.1. Administrator Danych Osobowych deklaruje, że przetwarzanie danych osobowych w **Zespole Szkół Mistrzostwa Sportowego nr 2** jest zgodne z mającymi zastosowanie wymaganiami prawnymi.

4.2. Administrator Danych Osobowych zapewnia, że dane osobowe są:

4.2.1. przetwarzane rzetelnie i w sposób przejrzysty dla osoby, której dane dotyczą,

4.2.2. zbierane w konkretnych, wyraźnych i prawnie uzasadnionych celach i przetwarzane w sposób zgodny z tymi celami,

4.2.3. adekwatne, stosowne oraz ograniczone do tego, co niezbędne do celów, w których są przetwarzane,

4.2.4. prawidłowe i w razie potrzeby uaktualniane,

4.2.5. przechowywane w formie umożliwiającej identyfikację osoby, której dane dotyczą, przez okres nie dłuższy, niż jest to niezbędne do celów, w których dane te są przetwarzane,

4.2.6. przetwarzane w sposób zapewniający odpowiednie bezpieczeństwo danych osobowych, w tym ochronę przed niedozwolonym lub niezgodnym z prawem przetwarzaniem oraz przypadkową utratą, zniszczeniem lub uszkodzeniem, za pomocą odpowiednich środków technicznych lub organizacyjnych.

5. PODZIAŁ OBOWIĄZKÓW W ZAKRESIE OCHRONY DANYCH OSOBOWYCH

5.1. Administrator Danych Osobowych jest odpowiedzialny za:

5.1.1. wprowadzenie środków technicznych i organizacyjnych zapewniających ochronę przetwarzanych danych osobowych,

5.1.2. dostarczenie niezbędnych zasobów do zapewnienia zgodności z mającymi zastosowanie wymaganiami prawnymi w obszarze ochrony danych osobowych,

- 5.1.3. powoływanie i odwoływanie Inspektora Ochrony Danych Osobowych oraz wspieranie Inspektora w wypełnianiu przez niego zadań,
- 5.1.4. zapewnienie kwalifikacji Inspektora Ochrony Danych Osobowych, a w szczególności fachowej wiedzy nt. prawa i praktyk w dziedzinie ochrony danych osobowych
- 5.1.5. prowadzenie dokumentacji przetwarzania danych osobowych wymaganych przez mające zastosowanie regulacje prawne i wymagania wewnętrzne,
- 5.1.6. utrzymywanie aktualnego Rejestru czynności przetwarzania danych osobowych (Załącznik nr 1 do niniejszej Polityki).

5.2. Inspektor Ochrony Danych Osobowych jest odpowiedzialny za:

- 5.2.1. nadzorowanie opracowania, tworzenie i aktualizację uregulowań wewnętrznych (niniejsza Polityka, procedury, instrukcje inne dokumenty) dotyczących ochrony danych osobowych oraz nadzór nad ich przestrzeganiem,
- 5.2.2. kontakty z właściwym organem ds. ochrony danych osobowych związane ze składaniem wyjaśnień oraz współpracą w przypadku kontroli przeprowadzanej przez inspektorów organu ds. ochrony danych osobowych,
- 5.2.3. prowadzenie szkoleń w zakresie ochrony danych osobowych oraz zapewnienie zapoznania osób upoważnionych do przetwarzania danych osobowych z przepisami o ochronie danych osobowych,
- 5.2.4. okresowe dokonywanie przeglądów zasobów informacyjnych Organizacji, zawierających dane osobowe, oceny stanu bezpieczeństwa tych zasobów oraz raportowanie o wynikach i niezbędnych działaniach doskonalących do Administratora Danych Osobowych,
- 5.2.5. sprawdzanie zgodności przetwarzania danych osobowych z przepisami o ochronie danych osobowych oraz opracowanie w tym zakresie sprawozdania dla Administratora Danych Osobowych,
- 5.2.6. dokonywanie weryfikacji zgodności przetwarzania danych osobowych z mającymi zastosowanie regulacjami prawnymi w obszarze ochrony danych osobowych na żądanie organu ds. ochrony danych lub Administratora Danych Osobowych,
- 5.2.7. konsultowanie umów powierzenia przetwarzania danych osobowych,
- 5.2.8. nadzór nad realizacją analizy ryzyka oraz raportowanie wyników oceny do Administratora Danych Osobowych.

5.3. Administrator Systemu Informatycznego jest odpowiedzialny za:

- 5.3.1. współpracę z Administratorem Danych Osobowych oraz Inspektorem Ochrony Danych Osobowych w zakresie wymaganych na podstawie mających zastosowanie regulacji prawnych w obszarze ochrony danych osobowych (m.in. prowadzenie Rejestru czynności przetwarzania, udział w analizie ryzyka, usuwanie/modyfikowanie/uzupełnianie danych osobowych na wniosek osoby, której dane dotyczą),

- 5.3.2. eksploatację i konserwację systemów teleinformatycznych oraz dokumentowanie tych działań,
- 5.3.3. zapewnienie bezpieczeństwa przechowywanych w systemie teleinformatycznym danych osobowych,
- 5.3.4. realizację oraz bieżący nadzór nad uprawnieniami użytkowników w systemach teleinformatycznych.

5.4. Wszystkie osoby przetwarzające dane osobowe w Zespole Szkół Mistrzostwa Sportowego nr 2 są odpowiedzialne za:

- 5.4.1. przestrzeganie zasad ochrony danych osobowych określonych w Polityce i Instrukcji oraz dokumentach z nimi związanymi; w tym celu każdy pracownik zobowiązany jest zapoznać się przed dopuszczeniem do przetwarzania danych z wyżej wymienionymi dokumentami oraz złożyć stosowne oświadczenie, potwierdzające znajomość ich treści oraz zobowiązanie do zachowania w poufności danych osobowych (Załącznik nr 2 do niniejszej Polityki),
- 5.4.2. spełnienia wymogu wynikającego z obowiązku informacyjnego, w szczególności poinformowania osoby, której dane dotyczą zgodnie z zakresem wskazanym w punkcie 8.1 niniejszej Polityki,
- 5.4.3. uczestnictwo w obowiązkowym szkoleniu z zakresu ochrony danych osobowych,
- 5.4.4. bezzwłoczne zgłoszenie Inspektorowi Ochrony Danych Osobowych lub Administratorowi Systemu Informatycznego wszelkich dostrzeżonych nieprawidłowości w działaniu systemu informatycznego, w którym przetwarzane są dane osobowe,
- 5.4.5. bezzwłocznego zgłaszania wszelkich naruszeń, nieprawidłowości i dostrzeżonych zagrożeń, związanych z bezpieczeństwem danych osobowych,
- 5.4.6. wnioskowanie do Administratora Danych Osobowych o uzupełnienie lub uaktualnienie Rejestru czynności przetwarzania danych osobowych, potrzebie dokonania zmian w procesie przetwarzania danych osobowych oraz informowanie o ustaniu celu przetwarzania tych danych,
- 5.4.7. niezwłoczne usunięcie/zaprzestanie przetwarzania danych osobowych w momencie ustania celu ich przetwarzania,
- 5.4.8. informowanie Administratora Danych Osobowych lub Inspektora Ochrony Danych o zamiarze powierzenia przetwarzania danych osobowych lub ich udostępnienia innemu podmiotowi oraz konsultowanie z Inspektorem Ochrony Danych Osobowych umowy o powierzeniu przetwarzania danych osobowych,
- 5.4.9. dołożenia szczególnej staranności podczas przetwarzania danych osobowych, aby proces przetwarzania odbywał się zgodnie z prawem, dane osobowe były merytorycznie poprawne, a ich przetwarzanie odbywało się wyłącznie w celu i zakresie, dla którego zostały zebrane.

6. REJESTR CZYNNOŚCI PRZETWARZANIA DANYCH OSOBOWYCH

- 6.1. Dla wszystkich zidentyfikowanych kategorii danych osobowych Administrator Danych osobowych przy współpracy z Inspektorem Ochrony Danych Osobowych oraz Administratorem Systemu Informatycznego prowadzi Rejestr czynności przetwarzania danych osobowych.
- 6.2. Na rejestr czynności przetwarzania danych osobowych składają się co najmniej następujące pola:
 - 6.2.1. opis kategorii osób, których dane dotyczą,
 - 6.2.2. cel przetwarzania danych osobowych,
 - 6.2.3. informacja o przetwarzaniu danych wrażliwych,
 - 6.2.4. systemy teleinformatyczne, w których przetwarzane są dane osobowe,
 - 6.2.5. informacja o przetwarzaniu danych osobowych w formie papierowej,
 - 6.2.6. planowany termin usunięcia danych osobowych,
 - 6.2.7. stosowane zabezpieczenia organizacyjne i techniczne,
 - 6.2.8. informacje o podmiotach, którym powierzono do dalszego przetwarzania dane osobowe,
 - 6.2.9. informacje o podmiotach, którym udostępniono dane osobowe,
 - 6.2.10. informacje o przekazaniu danych osobowych do państwa trzeciego,
 - 6.2.11. imię i nazwisko lub nazwę oraz dane kontaktowe administratora.
- 6.3. Rejestr czynności przetwarzania danych osobowych może być prowadzony w formie papierowej, elektronicznej lub w systemie teleinformatycznym.

7. ŚRODKI TECHNICZNE I ORGANIZACYJNE OCHRONY DANYCH OSOBOWYCH

- 7.1. W celu zapewnienia ochrony danych osobowych przetwarzanych w **Zespole Szkół Mistrzostwa Sportowego nr 2** stosuje się następujące zabezpieczenia organizacyjne i techniczne:
 - 7.1.1. opracowano i wdrożono Politykę Bezpieczeństwa Danych Osobowych,
 - 7.1.2. opracowano i wdrożono Instrukcję zarządzania systemami informatycznymi przetwarzającymi dane osobowe,
 - 7.1.3. opracowano procedurę oceny ryzyka oraz regularnie przeprowadza się analizę ryzyka dla procesów ochrony danych osobowych, a na podstawie jej wyników podejmuje adekwatne działania zapewniające właściwy poziom bezpieczeństwa przetwarzanych danych osobowych,
 - 7.1.4. zapewnia się realizację szkoleń w zakresie ochrony danych osobowych dla wszystkich pracowników dopuszczonych do przetwarzania danych osobowych,
 - 7.1.5. do przetwarzania danych osobowych dopuszcza się jedynie pracowników, którzy uprzednio pisemnie zobowiązali się do zachowania ich w poufności,

- 7.1.6. przetwarzania danych osobowych dokonuje się w warunkach zabezpieczających dane przed dostępem osób nieupoważnionych, w szczególności poprzez: kontrolę dostępu do pomieszczeń i budynków, instalację alarmową, zapewnienie środków przetwarzania danych osobowych z trwałym znaczeniem otwarcia, w których przetwarza się dane osobowe (szafy, biurka zamykane na klucz),
- 7.1.7. każdą osobę przetwarzającą dane osobowe zobowiązuje się do przestrzegania podstawowych zasad bezpieczeństwa informacji (Załącznik nr 8 do niniejszej Polityki),
- 7.1.8. przebywanie osób nieupoważnionych w pomieszczeniach, gdzie przetwarzane są dane osobowe, dopuszcza się tylko w obecności osoby upoważnionej do przetwarzania danych osobowych oraz w warunkach zapewniających bezpieczeństwo danych,
- 7.1.9. stosuje się pisemne umowy powierzenia przetwarzania danych osobowych przy współpracy z podmiotami zewnętrznymi przetwarzającymi dane osobowe,
- 7.1.10. przetwarzanie danych osobowych odbywa się wyłącznie w ramach wykonywanych zadań służbowych,
- 7.1.11. zapewnia się zdolność do szybkiego przywrócenia dostępności danych osobowych w razie naruszenia fizycznego lub technicznego,
- 7.1.12. zapewnia się zdolność do ciągłego zapewnienia poufności, integralności i dostępności danych osobowych przetwarzanych w systemach teleinformatycznych,
- 7.1.13. dokonuje się regularnych audytów i testów skuteczności środków technicznych i organizacyjnych, mających zapewnić bezpieczeństwo przetwarzania danych osobowych,
- 7.1.14. tam, gdzie to możliwe zapewnia się zdolność systemów teleinformatycznych do spełnienia praw osób, których dane dotyczą (usunięcie, sprostowanie, sprzeciw, ograniczenie).

8. REALIZACJA OBOWIĄZKU INFORMACYJNEGO

- 8.1. Każdorazowo, podczas zbierania danych osobowych, należy przekazać osobie, której dane dotyczą:
 - 8.1.1. tożsamość i dane kontaktowe Administratora Danych Osobowych,
 - 8.1.2. dane kontaktowe Inspektora Ochrony Danych Osobowych,
 - 8.1.3. cele przetwarzania danych osobowych oraz podstawę prawną przetwarzania,
 - 8.1.4. informacje, że przetwarzanie dokonywane jest do celów wynikających z prawnie uzasadnionych interesów realizowanych przez Administratora Danych Osobowych,
 - 8.1.5. informacje o odbiorcach danych osobowych lub o kategoriach odbiorców, jeśli istnieją,
 - 8.1.6. gdy ma to zastosowanie – informacje o zamiarze przekazania danych osobowych do państwa trzeciego lub organizacji międzynarodowej oraz wzmiankę o stosowanych zabezpieczeniach, możliwościach uzyskania kopii tych danych lub o miejscu ich udostępnienia,

- 8.1.7. okres, przez który dane osobowe będą przechowywane, a gdy nie jest to możliwe, kryteria ustalania tego okresu,
 - 8.1.8. informacje o prawie do żądania od Organizacji dostępu do danych osobowych dotyczących osoby, której dane dotyczą, ich sprostowania, usunięcia lub ograniczenia przetwarzania lub o prawie do wniesienia sprzeciwu wobec przetwarzania, a także o prawie do przenoszenia danych,
 - 8.1.9. jeżeli przetwarzanie odbywa się na podstawie uzyskanej zgody - informacje o prawie do cofnięcia zgody na przetwarzanie danych osobowych,
 - 8.1.10. informację o prawie do wniesienia skargi do organu nadzorczego,
 - 8.1.11. informację o zautomatyzowanym podejmowaniu decyzji, w tym o profilowaniu, istotnych zasadach ich podejmowania, a także o znaczeniu i przewidywanych konsekwencjach takiego przetwarzania dla osoby, której dane dotyczą.
- 8.2. W przypadku, gdy dane osobowe zbierane są bezpośrednio od osoby, której dane dotyczą, należy przekazać informację, czy podanie danych osobowych jest wymogiem ustawowym lub umownym lub warunkiem zawarcia umowy oraz czy osoba, której dane dotyczą jest zobowiązana do ich podania i konsekwencjach niepodania danych.
- 8.3. W przypadku, gdy dane osobowe pozyskiwane są w inny sposób niż od osoby, której dane dotyczą, należy przekazać ponadto informację o:
- 8.3.1. kategoriach przetwarzanych danych osobowych,
 - 8.3.2. źródle pochodzenia danych osobowych (w tym informacji, że pochodzą one ze źródeł publicznie dostępnych, jeżeli z takiego źródła zostały pozyskane),
- 8.4. W przypadku, gdy planuje się dalej przetwarzać dane osobowe w celu innym niż cel, w którym dane osobowe zostały zebrane, należy poinformować osobę, której dane dotyczą, o nowym celu przetwarzania oraz udzielić jej stosowanych informacji zawartych w niniejszym rozdziale.
- 8.5. Do realizacji obowiązku informacyjnego zobowiązani są wszyscy pracownicy i współpracownicy Organizacji.
- 8.6. Obowiązek informacyjny w **Zespole Szkół Mistrzostwa Sportowego nr 2** należy realizować:
- 8.6.1. ustnie – w przypadku bezpośredniego kontaktu z osobą, której dane dotyczą,
 - 8.6.2. pisemnie – jako integralną część umowy lub innego dokumentu z podmiotem zewnętrznym zawierającym dane osobowe,
 - 8.6.3. w formie elektronicznej – jako informacja w systemie teleinformatycznym przetwarzającym dane osobowe lub
 - 8.6.4. mailowo – w przypadku korespondencji mailowej.
- 8.7. Informacje zawarte w niniejszym punkcie nie mają zastosowania w przypadku, gdy osoba, której dane dotyczą dysponuje już tymi informacjami.

- 8.8. Przykładowa treść spełniająca wymagania obowiązku informacyjnego została zamieszczona w Załączniku nr 3 do niniejszej Polityki.
- 8.9. Podstawowe informacje z zakresu danych osobowych obejmujące informacje o Administratorze Danych Osobowych, Inspektorze Danych Osobowych oraz przetwarzanych kategoriach danych udostępniane są na stronie Zespół Szkół Mistrzostwa Sportowego nr 2

9. PRAWA OSÓB, KTÓRYCH DANE SĄ PRZETWARZANE PRZEZ ORGANIZACJĘ

9.1. Prawo dostępu przysługujące osobie, której dane dotyczą

- 9.1.1. Każda osoba, której dane dotyczą jest uprawniona do uzyskania potwierdzenia, czy w Organizacji przetwarzane są jej dane osobowe.
- 9.1.2. Na wniosek osoby, której dane dotyczą, należy przekazać informację o:
- 9.1.2.1. celu przetwarzania danych osobowych,
 - 9.1.2.2. kategoriach przetwarzanych danych osobowych,
 - 9.1.2.3. odbiorcach lub kategoriach odbiorców, którym dane osobowe zostały lub zostaną ujawnione, w szczególności o odbiorcach w państwach trzecich lub organizacjach międzynarodowych oraz zabezpieczeniach wykorzystywanych w związku z tym przekazaniem,
 - 9.1.2.4. planowanym okresie przechowywania danych osobowych, a gdy nie jest możliwe jego określenie - kryteriach tego okresu,
 - 9.1.2.5. prawie do żądania od Administratora Danych Osobowych sprostowania, usunięcia lub ograniczenia przetwarzania danych osobowych oraz prawie wniesienia sprzeciwu wobec stosowanego przetwarzania,
 - 9.1.2.6. prawie wniesienia skargi do organu nadzorczego,
 - 9.1.2.7. źródle pozyskiwania danych osobowych, jeśli nie zostały zebrane od osoby, której dane dotyczą,
 - 9.1.2.8. zautomatyzowanym podejmowaniu decyzji, w tym o profilowaniu, istotnych zasadach ich podejmowania, a także o znaczeniu i przewidywanych konsekwencjach takiego przetwarzania dla osoby, której dane dotyczą.
- 9.1.3. W przypadku wystąpienia przez osobę, której dane dotyczą, o kopię danych osobowych, należy zgłosić taki fakt Inspektorowi Ochrony Danych Osobowych.
- 9.1.4. Inspektor Ochrony Danych Osobowych dostarcza osobie, której dane dotyczą kopię danych podlegających przetwarzaniu.
- 9.1.5. Inspektor Ochrony Danych Osobowych podejmuje decyzję o formie, w której zostanie przekazana kopia danych oraz wysokości opłat za wszelkie kolejne kopie.
- 9.1.6. Inspektor Ochrony Danych Osobowych ma prawo odmowy przekazania kopii danych osobowych w przypadku, gdy może to wpłynąć na prawa i wolności innych.

9.2. Prawo do sprostowania, usunięcia, ograniczenia, przenoszenia danych osobowych oraz sprzeciwu wobec ich przetwarzania

- 9.2.1. Prawo do sprostowania - każda osoba, której dotyczą dane ma prawo do żądania niezwłocznego sprostowania dotyczących jej danych osobowych, które są nieprawidłowe. Występująca osoba, której dane dotyczą, ma prawo żądania uzupełnienia niekompletnych danych osobowych, w tym poprzez przedstawienie dodatkowego oświadczenia.
- 9.2.2. Prawo do usunięcia danych („Prawo do bycia zapomnianym”) - każda osoba, której dane dotyczą, ma prawo żądania niezwłocznego usunięcia dotyczących jej danych osobowych.
- 9.2.3. Prawo do ograniczenia przetwarzania - osoba, której dane dotyczą, ma prawo żądania od Administratora Danych Osobowych ograniczenia przetwarzania jej danych osobowych.
- 9.2.4. Prawo do przenoszenia danych - osoba, której dane dotyczą, ma prawo otrzymać w ustrukturyzowanym, powszechnie używanym formacie nadającym się do odczytu maszynowego, dane osobowe jej dotyczące, które dostarczyła administratorowi oraz ma prawo przesłać te dane osobowe innemu administratorowi bez przeszkód ze strony administratora, któremu dostarczono te dane osobowe.
- 9.2.5. Prawo do sprzeciwu - osoba, której dane dotyczą ma prawo wnieść sprzeciw wobec przetwarzania jej danych osobowych.

9.3. Zasady realizacji praw osób, których dane dotyczą

- 9.3.1. Wnioski o realizację praw osób, których dane dotyczą kierowane są na adres: **iod6_oswiata@um.poznan.pl**
- 9.3.2. W przypadku, gdy wniosek zostanie skierowany do pracownika Organizacji, należy niezwłocznie przekazać go do Inspektora Ochrony Danych Osobowych.
- 9.3.3. Inspektor Ochrony Danych Osobowych dokonuje analizy wniosku oraz weryfikuje zasadność realizacji prawa osoby, której dane dotyczą.
- 9.3.4. W przypadku braku zasadności realizacji prawa, Inspektor Ochrony Danych Osobowych zobligowany jest do niezwłocznego (nie dłużej niż 1 miesiąc) przekazania tej informacji osobie wnioskującej wraz z właściwym uzasadnieniem decyzji.
- 9.3.5. W przypadku pozytywnej oceny wniosku, Inspektor Ochrony Danych Osobowych zobligowany jest do wszczęcia postępowania mającego na celu realizację prawa osoby wnioskującej. Po zakończeniu działań związanych z realizacją prawa osoby wnioskującej, Inspektor Ochrony Danych Osobowych informuje o tym fakcie osobę wnioskującą. W przypadku, gdy pojawia się ryzyko przedłużenia czasu realizacji prawa (dłużej niż 1 miesiąc), Inspektor Ochrony Danych Osobowych przekazuje osobie wnioskującej odpowiedź wraz z planowanym terminem realizacji prawa, o które wnioskowała.

9.3.6. W przypadku realizacji prawa osoby, której dane dotyczą, Inspektor Ochrony Danych Osobowych ma obowiązek przekazania obowiązku realizacji tego prawa do wszystkich podmiotów, którym powierzono dane do przetwarzania.

9.3.7. W sytuacji, w której realizacja prawa osoby, której dane dotyczą wymaga zaangażowania pracowników Organizacji, na wniosek Inspektora Ochrony Danych Osobowych pracownicy ci są zobligowani do wykonania zadań niezbędnych do realizacji prawa osoby wnioskującej.

10. REALIZACJA UDOSTĘPNIENÍ DANYCH OSOBOWYCH

10.1. Dane osobowe udostępniane są wyłącznie na pisemny umotywowany wniosek, chyba że przepisy prawa stanowią inaczej.

10.2. Udostępnienia danych osobowych do Odbiorcy może dokonać wyłącznie Administrator Danych Osobowych lub Inspektor Ochrony Danych Osobowych. Wszyscy pracownicy Organizacji, w przypadku otrzymania wniosku o udostępnienie danych osobowych, zobligowani są do przekazania wniosku Administratorowi Danych Osobowych lub Inspektorowi Ochrony Danych Osobowych.

10.3. Wniosek musi zawierać informacje umożliwiające wyszukanie w zbiorze żądanych danych osobowych oraz wskazywać ich zakres i przeznaczenie.

10.4. Zgodę na udostępnienie danych osobowych wydaje Inspektor Ochrony Danych Osobowych w uzgodnieniu z przedstawicielami Administratora Danych Osobowych, jeżeli uzna to za stosowne.

10.5. W przypadku wyrażenia zgody na udostępnienie, Inspektor Ochrony Danych Osobowych przygotowuje udostępniane dane osobowe oraz odnotowanie faktu udostępnienia w Rejestrze udostępnień danych osobowych, stanowiącym (Załącznik nr 4 do niniejszej Polityki).

10.6. W przypadku udostępniania danych z systemów informatycznych, które nie odnotowują udostępnienia automatycznie, plik przekazywanych danych jest przechowywany przez Inspektora Ochrony Danych Osobowych wraz z dokumentem wskazującym na podstawę udostępnienia i dodatkowym opisem wskazującym datę udostępnienia danych oraz określeniem odbiorcy danych (np. nazwa i adres instytucji).

11. ZASADY POWIERZANIA DANYCH OSOBOWYCH

11.1. Powierzenie przetwarzania danych osobowych przez **Zespół Szkół Mistrzostwa Sportowego nr 2** podmiotom zewnętrznym następuje wyłącznie w drodze umowy powierzenia przetwarzania danych osobowych zawartej na piśmie. Wzór umowy powierzenia danych osobowych stanowi Załącznik nr 5 do niniejszej Polityki. Dopuszczalne jest wykorzystanie innego wzoru jedynie w przypadku, gdy treść umowy spełnia minimalne wymagania wskazane w punkcie 11.6.

11.2. Administratorem Danych Osobowych, które zostały powierzone do przetwarzania jest **Zespół Szkół Mistrzostwa Sportowego nr 2**

- 11.3. Podmiot zewnętrzny, któremu powierzono przetwarzanie danych nie może powierzyć do dalszego przetwarzania powierzonych mu danych bez wyraźnej zgody Administratora Danych Osobowych.
- 11.4. Podmiot zewnętrzny, któremu powierzono przetwarzanie danych zobowiązany jest przetwarzać powierzone mu dane wyłącznie w celach, które zostały wskazane w zawartej z nim umowie.
- 11.5. Podmiot zewnętrzny, któremu powierzono przetwarzanie danych zobowiązany jest do spełnienia mających zastosowanie wymagań prawnych w obszarze danych osobowych.
- 11.6. Umowa o powierzeniu przetwarzania danych osobowych powinna w szczególności zawierać zapisy dotyczące:
- 11.6.1. przedmiotu i czasu trwania przetwarzania danych osobowych,
 - 11.6.2. charakteru i celu przetwarzania danych osobowych,
 - 11.6.3. rodzaju danych osobowych oraz kategorii osób, których dane dotyczą,
 - 11.6.4. obowiązków i praw Administratora Danych Osobowych,
 - 11.6.5. zobowiązań pracowników podmiotu przetwarzającego do zachowania powierzonych danych osobowych w tajemnicy,
 - 11.6.6. zapewnienia bezpieczeństwa organizacyjnego i technicznego przetwarzania danych osobowych,
 - 11.6.7. zasad dalszego powierzania danych osobowych administrowanych przez **Zespół Szkół Mistrzostwa Sportowego nr 2**
 - 11.6.8. udziału w procesie udzielania odpowiedzi na żądanie osoby, której dane dotyczą, oceny skutków dla przetwarzania danych osobowych, zgłaszania incydentów,
 - 11.6.9. usunięcia lub zwrócenia powierzonych danych osobowych po zakończeniu świadczenia usługi,
 - 11.6.10. udostępniania Administratorowi Danych Osobowych wszelkich informacji niezbędnych do wykazania spełnienia obowiązków określonych w mających zastosowanie przepisach prawa w obszarze ochrony danych osobowych (np. audyty drugiej strony),
 - 11.6.11. możliwości żądania natychmiastowego wstrzymania przetwarzania danych osobowych powierzonych w razie stwierdzenia niedostatecznej ochrony danych osobowych.
- 11.7. Wszyscy pracownicy i współpracownicy Organizacji mają obowiązek zasięgnąć opinii Inspektora Ochrony Danych Osobowych w każdej sytuacji, w której ma nastąpić podpisanie umowy, której przedmiot choćby pośrednio wiąże się z powierzeniem innej firmie danych osobowych bądź z przyjęciem przez **Zespół Szkół Mistrzostwa Sportowego nr 2** danych osobowych do przetwarzania.

12. NARUSZENIA OCHRONY DANYCH OSOBOWYCH

- 12.1. Za naruszenie ochrony danych osobowych uznaje się 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.

12.2. Każdy z pracowników Organizacji, w przypadku zidentyfikowania zdarzenia mogącego stanowić naruszenie ochrony danych osobowych, jest zobowiązany do niezwłocznego kontaktu z Inspektorem Ochrony Danych Osobowych osobiście lub poprzez:

12.2.1. telefon: **(61) 878 49 07**.

12.2.2. e-mail: **iod6_oswiata@um.poznan.pl**

12.3. W uzasadnionych przypadkach osoba, która zgłosiła naruszenie zobowiązana jest postępować zgodnie z wytycznymi Inspektora Ochrony Danych Osobowych w zakresie zabezpieczenia materiału dowodowego i jeśli zajdzie taka potrzeba, zaprzestania wykonywania obowiązków służbowych w celu nienaruszania materiałów dowodowych

12.4. W przypadku zakwalifikowania zdarzenia jako naruszenie ochrony danych osobowych, Inspektor Ochrony Danych Osobowych bez zbędnej zwłoki zgłasza organowi nadzorczemu fakt wystąpienia zdarzenia mogącego naruszyć bezpieczeństwo danych osobowych.

12.5. Jeżeli istnieje małe prawdopodobieństwo, iż naruszenie ochrony danych osobowych skutkować będzie naruszeniem praw lub wolności osób fizycznych, Inspektor Ochrony Danych Osobowych nie jest zobligowany do zgłoszenia takiego naruszenia do organu nadzorczego.

12.6. Wszystkie zdarzenia zakwalifikowane, jako naruszenie ochrony danych osobowych należy udokumentować zgodnie z wzorem Rejestru naruszeń ochrony danych osobowych stanowiącym Załącznik nr 6 do niniejszej Polityki.

12.7. W przypadku, gdy naruszenie ochrony danych osobowych może powodować wysokie ryzyko naruszenia praw lub wolności osób, których dotyczy naruszenie, należy je bez zbędnej zwłoki o tym poinformować, o ile to technicznie możliwe.

13. AUDYT OCHRONY DANYCH OSOBOWYCH

13.1. Inspektor Ochrony Danych Osobowych jest zobowiązany do prowadzenia cyklicznych audytów przestrzegania zasad ochrony danych osobowych opisanych w regulacjach wewnętrznych **Zespołu Szkół Mistrzostwa Sportowego nr 2** oraz mających zastosowanie wymaganiach prawnych. Zaleca się, aby audyty ochrony danych osobowych prowadzone były przynajmniej raz na trzy lata.

13.2. Podczas określania zakresu audytu ochrony danych osobowych należy wziąć pod uwagę w szczególności:

13.2.1. obszary, w których zostały zidentyfikowane naruszenia ochrony danych osobowych,

13.2.2. rezultaty wcześniejszych audytów ochrony danych osobowych,

13.2.3. zmiany w otoczeniu wewnętrznym i zewnętrznym organizacji,

13.2.4. informacje zwrotną od zainteresowanych stron.

13.3. Audytowi ochrony danych osobowych podlegają:

13.3.1. systemy informatyczne przetwarzające dane osobowe,

13.3.2. zabezpieczenia fizyczne,

13.3.3. zabezpieczenia organizacyjne,

13.3.4. bezpieczeństwo osobowe,

13.3.5. zgodność stanu faktycznego z wymaganiami mających zastosowanie aktów prawnych oraz dokumentacji wewnętrznej Organizacji.

13.4. Do audytu ochrony danych osobowych upoważniony jest Inspektor Ochrony Danych Osobowych lub osoba przez niego wyznaczona posiadająca niezbędną wiedzę i kwalifikacje.

13.5. Po dokonaniu audytu osoba przeprowadzająca audyt przygotowuje i przekazuje raport Administratorowi Danych Osobowych.

13.6. W przypadku wystąpienia braku zgodności z wymaganiami prawnymi lub regulacjami wewnętrznymi, Inspektor Ochrony Danych Osobowych inicjuje adekwatne działania doskonalące.

14. SZKOLENIA

14.1. Każdy pracownik przed dopuszczeniem do pracy z systemem informatycznym przetwarzającym dane osobowe lub danymi osobowymi w wersji papierowej, musi być poddany przeszkoleniu w zakresie ochrony danych osobowych.

14.2. Za przeprowadzenie szkolenia odpowiada Inspektor Ochrony Danych Osobowych lub osoby przez niego upoważnione. Odbycie szkolenia warunkuje dopuszczenie do przetwarzania danych osobowych.

14.3. Szkolenie powinno obejmować zaznajomienie pracownika z wymaganiami w zakresie ochrony danych osobowych zawartych w mających zastosowanie przepisach prawa oraz regulacjach wewnętrznych obowiązujących w **Zespole Szkół Mistrzostwa Sportowego nr 2**

14.4. Każdorazowo w przypadku znaczącej zmiany wymagań prawnych w zakresie ochrony danych osobowych, Inspektor Ochrony Danych Osobowych jest zobowiązany do zapewnienia skutecznego przekazania tych zmian pracownikom i współpracownikom Organizacji.

14.5. Inspektor Ochrony Danych Osobowych jest zobowiązany do budowy świadomości i organizacji cyklicznych szkoleń lub kampanii informacyjnych poświęconych tematyce ochrony danych osobowych oraz podstawowym zasadom bezpieczeństwa informacji. Zaleca się, aby każdy pracownik brał udział w takim szkoleniu nie rzadziej niż raz na 3 lata.

14.6. Opisywane powyżej szkolenia mogą odbywać się w dowolnej formie, ogólnie przyjętej u Administratora Danych Osobowych.

14.7.

15. RETENCJA DANYCH

- 15.1. Dane osobowe przetwarzane w **Zespole Szkół Mistrzostwa Sportowego nr 2** przechowywane są przez okres nie dłuższy niż jest to niezbędne. Okres przechowywania danych dostosowywany jest do celu, w którym zostały zebrane.
- 15.2. Okres retencji może:
- 15.2.1. wynikać z przepisów prawa,
 - 15.2.2. zostać określony przez organ nadzorczy w zakresie ochrony danych osobowych,
 - 15.2.3. być ustalany przez komórki biznesowe, będące właścicielami przetwarzanych danych osobowych.
- 15.3. Okres retencji danych osobowych odnotowany jest w Rejestrze czynności przetwarzania w stosunku do określonej kategorii i celu, w jakim dane osobowe zostały zebrane.
- 15.4. W przypadku dokumentacji w formie papierowej, za zniszczenie danych po ustaniu okresu retencji odpowiedzialny jest każdy pracownik przetwarzający te dane.
- 15.5. W przypadku danych osobowych przetwarzanych w systemach teleinformatycznych, każdy pracownik przetwarzający te dane jest odpowiedzialny, w miarę możliwości, za usunięcie tych danych lub zgłoszenie potrzeby ich usunięcia (dowolną drogą) do Administratorów Systemów Informatycznych.
- 15.6. Przynajmniej raz w roku, wszyscy pracownicy i współpracownicy Organizacji są odpowiedzialni za przeprowadzenie weryfikacji, czy cel przetwarzania danych osobowych w stosunku do danych, które przetwarzają jest nadal aktualny oraz czy nie przetwarzają danych dłużej aniżeli zostało to określone w Rejestrze czynności przetwarzania.
- 15.7. W przypadku zidentyfikowania nieprawidłowości, wyniki przeglądu są raportowane do Administratora Danych Osobowych.

16. ZGODY NA PRZETWARZANIE DANYCH OSOBOWYCH

- 16.1. W każdej sytuacji, w której nie zidentyfikowano podstawy prawnej innej niż zgoda osoby, której dane dotyczą, niezbędne jest uzyskanie takiej zgody.
- 16.2. Forma wyrażenia zgody na przetwarzanie danych osobowych jest dowolna (np. treść wiadomości mailowej, wydruk, checkbox w systemie teleinformatycznym). Forma zgody powinna jednak gwarantować możliwość potwierdzenia uzyskania takiej zgody.
- 16.3. Wyrażenie zgody na przetwarzanie danych osobowych nie może stanowić podstawy do odmowy wykonania umowy/świadczenia usługi, jeśli przetwarzanie danych osobowych nie jest niezbędne do ich wykonania.
- 16.4. Za uzyskanie zgody na przetwarzanie danych osobowych odpowiedzialny jest pracownik pozyskujący dane osobowe od osoby, której dane dotyczą.
- 16.5. Zgoda na przetwarzanie danych osobowych musi zawierać przynajmniej:

- 16.5.1. tożsamość Administratora Danych Osobowych,
 - 16.5.2. zamierzone cele przetwarzania, dla których dane osobowe są zbierane,
 - 16.5.3. fakt wyrażenia zgody,
 - 16.5.4. informację o możliwości wycofania zgody.
- 16.6. Nie dopuszcza się sytuacji, w których łączy się zgody na przetwarzanie danych osobowych zbieranych dla spełnienia różnych celów. W przypadku zbierania danych osobowych dla kilku celów jednocześnie, należy uzyskać indywidualną zgodę dla każdego z celów.
- 16.7. W przypadku, gdy zgoda dotyczy danych wrażliwych, konieczne jest zebranie jej w formie pisemnego oświadczenia od osoby, której dane dotyczą.
- 16.8. Osoba, której dane dotyczą ma prawo w dowolnym momencie wycofać zgodę.
- 16.9. W przypadku uzyskania wniosku o wycofanie zgody na przetwarzanie danych osobowych, każdy pracownik jest zobowiązany do powiadomienia o tym fakcie Inspektora Ochrony Danych Osobowych, który podejmuje właściwe kroki.

17. UPOWAŻNIENIA DO PRZETWARZANIA DANYCH OSOBOWYCH

- 17.1. Przed uzyskaniem dostępu do przetwarzania danych osobowych, każdy pracownik musi zostać formalnie upoważniony przez Administratora Danych Osobowych do ich przetwarzania.
- 17.2. Za formę upoważnienia do przetwarzania danych osobowych w **Zespole Szkół Mistrzostwa Sportowego nr 2** przyjmuje się wskazanie w umowie lub zakresie obowiązków pracownika właściwej klauzuli informującej o fakcie upoważnienia pracownika do przetwarzania danych osobowych, w stopniu i zakresie niezbędnym do realizacji obowiązków służbowych i poleceń przełożonych.
- 17.3. Przetwarzanie danych osobowych w zakresie innym niż zawarty w upoważnieniu jest zabronione.

18. ANALIZA RYZYKA PROCESÓW PRZETWARZANIA DANYCH OSOBOWYCH

- 18.1. Analiza ryzyka procesów przetwarzania danych osobowych jest procesem realizowanym w celu:
- 18.1.1. oceny ryzyka naruszenia praw lub wolności osób, których dane dotyczą,
 - 18.1.2. planowania zarządzania ryzykiem, w tym zabezpieczeń (organizacyjnych i technicznych) oraz środków i mechanizmów bezpieczeństwa mających zapewnić ochronę danych osobowych i wykazać przestrzeganie mających zastosowanie regulacji prawnych.
- 18.2. Proces analizy ryzyka jest realizowany cyklicznie i inicjowany przez Inspektora Ochrony Danych Osobowych lub każdorazowo, gdy zajdzie taka potrzeba (np. wdrożenie nowego systemu teleinformatycznego).

- 18.3. W proces analizy ryzyka zaangażowane są osoby odpowiedzialne za zapewnienie bezpieczeństwa danych osobowych w systemach informatycznych oraz pomieszczeniach wykorzystywanych przez **Zespół Szkół Mistrzostwa Sportowego nr 2**
- 18.4. Wyniki analizy ryzyka procesów przetwarzania danych osobowych oraz propozycje działań w planie postępowania z ryzykiem przedstawiane są Administratorowi Danych Osobowych w celu ich akceptacji i uruchomienia ich realizacji.
- 18.5. Szczegółowy opis czynności został określony w Procedurze analizy ryzyka procesów przetwarzania danych osobowych stanowiącej załącznik nr 7 do niniejszej Polityki.

Dyrektor Zespołu Szkół Mistrzostwa
Sportowego nr 2
Anna Mrówczyńska

1. ZAŁĄCZNIKI

Załącznik nr 1 - Rejestr czynności przetwarzania danych osobowych

Załącznik nr 2 – Zobowiązanie do zachowania poufności

Załącznik nr 3 – Wzór treści spełniającej obowiązek informacyjny

Załącznik nr 4 – Rejestr udostępnień danych osobowych

Załącznik nr 5 – Wzór umowy powierzenia danych osobowych

Załącznik nr 6 – Rejestr naruszeń ochrony danych osobowych

Załącznik nr 7 – Procedura analizy ryzyka procesów przetwarzania danych osobowych

Załącznik nr 8 – Podstawowe zasady bezpieczeństwa