DZIENNIK URZĘDOWY
MINISTRA SPORTU

Warszawa, dnia 14 lutego 2020 r.

Poz. 13

ZARZĄDZENIE NR 3
MINISTRA SPORTU[1)]

z dnia 13 lutego 2020 r.

w sprawie ustalenia Polityki Ochrony Danych Osobowych w Ministerstwie Sportu

Na podstawie art. 24 ust. 1 i ust. 2 rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych), (Dz. Urz. UE z 4.5.2016 r. L 119, str. 1) zarządza się, co następuje:

§ 1. Ustala się Politykę Ochrony Danych Osobowych w Ministerstwie Sportu, stanowiącą załącznik do zarządzenia.

§ 2. Zarządzenie wchodzi w życie z dniem następującym po dniu ogłoszenia.

Minister Sportu

Danuta Dmowska-Andrzejuk

[1)] Minister Sportu kieruje działem administracji rządowej – kultura fizyczna, na podstawie § 1 ust. 2 rozporządzenia Prezesa Rady Ministrów z dnia 10 grudnia 2019 r. w sprawie szczegółowego zakresu działania Ministra Sportu (Dz.U. poz. 2380).

Załącznik Nr 1 do zarządzenia Nr 3
Ministra Sportu
z dnia 13 lutego 2020 r.

POLITYKA OCHRONY DANYCH OSOBOWYCH W MINISTERSTWIE SPORTU

Rozdział 1.
Postanowienia ogólne

§ 1. Polityka Ochrony Danych Osobowych, zwana dalej „Polityką”, określa sposób przetwarzania danych osobowych oraz środki techniczne i organizacyjne zapewniające ochronę przetwarzanych danych osobowych, dla których Minister Sportu, zwany dalej „Ministrem”, jest Administratorem oraz danych osobowych przetwarzanych w Ministerstwie Sportu, zwanym dalej „Ministerstwem”.

§ 2. Użyte w Polityce określenia i skróty oznaczają:

1) Administrator – Ministra właściwego do spraw kultury fizycznej;
2) BG – Biuro Dyrektora Generalnego Ministerstwa;
3) EZD – system Elektronicznego Zarządzania Dokumentacją;
4) identyfikator – ciąg znaków literowych, cyfrowych lub innych jednoznacznie identyfikujący użytkownika w systemie informatycznym;
5) Inspektor Ochrony Danych (IOD) – pracownika Ministerstwa wyznaczonego przez Administratora, nadzorującego i kontrolującego przestrzeganie zasad ochrony danych osobowych w Ministerstwie;
6) Instrukcja – instrukcję zarządzania systemem informatycznym służącym do przetwarzania danych osobowych;
7) kierujący komórką organizacyjną – dyrektora departamentu lub biura albo inną osobę, której powierzono kierowanie departamentem lub biurem, a także Szefa Gabinetu Politycznego Ministra;
8) komórka organizacyjna – departament, biuro oraz Gabinet Polityczny Ministra;
9) naruszenie ochrony danych osobowych – 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;
10) ocena skutków dla ochrony danych – (*DPIA*) ocenę skutków dla ochrony danych dokonywaną przez Administratora w przypadku planowanych operacji przetwarzania z dużym prawdopodobieństwem mogących powodować wysokie ryzyko naruszenia praw lub wolności osób fizycznych;
11) administrator systemu informatycznego – pracownika Ministerstwa wyznaczonego przez Administratora, nadzorującego i kontrolującego funkcjonowanie całości systemu informatycznego Ministerstwa, w szczególności części systemu, w których przetwarzane są dane osobowe;
12) podatność – słabość systemu bezpieczeństwa danych osobowych, która może mieć wpływ na wystąpienie zagrożenia np. związanego z uzyskaniem nieautoryzowanego dostępu do danych, w szczególności do systemu informatycznego przetwarzającego dane osobowe, prowadząca do zawieszenia tego systemu lub utraty funkcjonalności;
13) podmiot danych – osobę fizyczną, której przetwarzane dane dotyczą;
14) podmiot przetwarzający - osobę fizyczną lub prawną, organ publiczny, jednostkę lub inny podmiot, który przetwarza dane osobowe w imieniu i na rzecz Administratora;
15) pracownik – osobę zatrudnioną w Ministerstwie na podstawie stosunku pracy;
16) rozporządzenie - rozporządzenie Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie

swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (Dz. Urz. UE L 119 z 04.05.2016, str.1);

17) organ nadzorczy – organ w rozumieniu rozporządzenia;

18) ryzyko – możliwość niezrealizowania celu w kontekście ochrony danych osobowych;

19) system informatyczny – zespół współpracujących ze sobą urządzeń, programów, procedur przetwarzania informacji i narzędzi programowych zastosowanych w celu przetwarzania danych osobowych;

20) ustawa – ustawę z dnia 10 maja 2018 r. o ochronie danych osobowych (Dz. U. z 2019 r. poz. 1781);

21) usuwanie danych osobowych – zniszczenie danych osobowych lub taką ich modyfikację, która nie pozwoli na ustalenie tożsamości osoby, której dane dotyczą;

22) użytkownik - pracownika, stażystę, wolontariusza, praktykanta lub inną osobę wykonującą usługi na podstawie umów cywilnoprawnych, która uzyskała upoważnienie do przetwarzania danych osobowych w określonym zakresie, w tym również za pomocą systemu informatycznego;

23) zabezpieczenie danych osobowych – wdrożenie i eksploatację środków organizacyjnych, technicznych i fizycznych, w celu zabezpieczenia zasobów technicznych oraz ochrony przed zniszczeniem, nieuprawnionym dostępem i modyfikacją, ujawnieniem lub pozyskaniem danych osobowych, bądź ich utratą;

24) zbiór danych – uporządkowany zestaw danych osobowych dostępnych według określonych kryteriów, niezależnie od tego, czy zestaw ten jest scentralizowany, zdecentralizowany czy rozproszony funkcjonalnie lub geograficznie;

25) Zespół Systemu Zarządzania Bezpieczeństwem Informacji – zespół, o którym mowa w zarządzeniu nr 13 Ministra Sportu i Turystyki z dnia 15 kwietnia 2019 r. w sprawie ustanowienia Systemu Zarządzania Bezpieczeństwem Informacji w Ministerstwie Sportu i Turystyki (Dz. Urz. Min. Spor. poz. 31).

Rozdział 2.
Obowiązek informacyjny

§ 3. 1. Administrator udziela informacji, o których mowa w art. 13 i 14 rozporządzenia, osobie, której dane dotyczą, a także prowadzi wszelką komunikację dotyczącą art. 14 - 22 i 34 rozporządzenia w zwięzłej, przejrzystej, zrozumiałej i łatwo dostępnej formie, jasnym i prostym językiem.

2. Informacji, o których mowa w ust. 1 udziela się pisemnie lub elektronicznie, w szczególności przez wskazanie właściwego adresu w Biuletynie Informacji Publicznej Ministerstwa. Jeżeli osoba, której dane dotyczą, tego zażąda, informacji można udzielić ustnie pod warunkiem, że zostanie potwierdzona tożsamość osoby, której dane dotyczą, za pomocą danych będących w posiadaniu komórki organizacyjnej.

§ 4. 1. Za wypełnianie obowiązków informacyjnych, o których mowa w § 3 ust. 1 odpowiedzialny jest kierujący właściwą komórką organizacyjną lub podmiot, któremu powierzono przetwarzanie danych osobowych na podstawie art. 28 rozporządzenia oraz zgodnie z § 6, jeżeli umowa taki obowiązek określa.

2. Za aktualność i zgodność z przepisami klauzul informacyjnych funkcjonujących na portalach i serwisach, których Administratorem jest Minister, odpowiedzialni są kierujący właściwymi komórkami organizacyjnymi.

Rozdział 3.
Umowy powierzenia przetwarzania danych osobowych oraz rejestr czynności przetwarzania

§ 5. 1. Udostępnianie danych osobowych, których Administratorem jest Minister oraz danych osobowych przetwarzanych w Ministerstwie może nastąpić wyłącznie na podstawie przepisów prawa.

2. Udostępnienia danych osobowych, o którym mowa w ust. 1, dokonuje kierujący komórką organizacyjną, w której dane te zostały zgromadzone, po uzgodnieniu z IOD.

§ 6. 1. Przetwarzanie danych osobowych, których Administratorem jest Minister, może zostać powierzone innemu podmiotowi pod warunkiem zawarcia z tym podmiotem pisemnej umowy powierzenia przetwarzania danych osobowych.

2. Projekty umów powierzenia przetwarzania danych osobowych oraz umów cywilnoprawnych, w których zawarte są zapisy powierzające przetwarzanie danych osobowych, są opiniowane przez IOD.

3. Informacja na temat zawartej umowy powierzenia przetwarzania danych osobowych przekazywana jest niezwłocznie do IOD przez komórkę organizacyjną odpowiedzialną merytorycznie za podpisanie umowy.

4. Kierujący komórką organizacyjną merytorycznie odpowiedzialną za prawidłowość realizacji postanowień umowy powierzenia przetwarzania danych, monitoruje tryb zawierania przez podmiot przetwarzający kolejnych umów powierzenia.

5. Informacja, o której mowa w ust. 3, stanowi część Rejestru czynności przetwarzania danych osobowych w Ministerstwie, którego wzór stanowi **załącznik nr 1** do Polityki.

6. Kierujący komórkami organizacyjnymi właściwymi w przedmiocie zawartych umów powierzenia przetwarzania danych osobowych odpowiadają za kompletność i aktualność Rejestrów, o których mowa w ust. 8, prowadzonego w zakresie komórki organizacyjnej.

7. W przypadku zawarcia umowy powierzenia przetwarzania danych osobowych, w której Minister występuje w roli podmiotu przetwarzającego, kierujący komórką organizacyjną właściwą w przedmiocie zawartej umowy, przekazuje do IOD informację na temat zawartej umowy. Informacja powinna obejmować zakres danych określony w Rejestrze kategorii przetwarzania danych osobowych w Ministerstwie, którego wzór stanowi **załącznik nr 2** do Polityki.

8. Rejestry, o których mowa w ust. 5 i 7 prowadzone są przez IOD w imieniu i pod nadzorem Administratora na podstawie informacji otrzymanych od kierujących komórkami organizacyjnymi.

Rozdział 4.
Realizacja praw osób, których dane dotyczą

§ 7. Każdej osobie, której dane osobowe są przetwarzane w Ministerstwie i dla których Minister jest Administratorem, przysługują prawa, o których mowa w Rozdziale III rozporządzenia.

§ 8. 1. Na żądanie osoby, której dane dotyczą, udziela się bez zbędnej zwłoki, nie później jednak niż w terminie miesiąca od otrzymania żądania, informacji o działaniach podjętych w związku z żądaniem skierowanym na podstawie art. 15-22 rozporządzenia.

2. Termin, o którym mowa w ust. 1 może zostać przedłużony o kolejne dwa miesiące z uwagi na skomplikowany charakter żądania lub liczbę żądań. W terminie miesiąca od otrzymania żądania informuje się osobę, której dane dotyczą, o przedłużeniu terminu, z podaniem przyczyn opóźnienia.

3. W przypadku niepodjęcia działań w związku z żądaniem osoby, której dane dotyczą, niezwłocznie – najpóźniej w terminie miesiąca od otrzymania żądania – informuje się osobę, której dane dotyczą, o powodach niepodjęcia działań oraz o możliwości wniesienia skargi do organu nadzorczego oraz skorzystania ze środków ochrony prawnej, o których mowa w ustawie.

4. Za udzielenie odpowiedzi na żądanie, o którym mowa w ust. 1, odpowiedzialny jest kierujący komórką organizacyjną przetwarzającą dane osoby występującej z wnioskiem.

5. W sytuacji, kiedy nie można określić, w której komórce organizacyjnej przetwarzane są dane osoby występującej z wnioskiem, żądanie należy skierować do wszystkich komórek organizacyjnych Ministerstwa. W przypadku, gdy dane osoby występującej z wnioskiem przetwarzane są w kilku komórkach organizacyjnych, odpowiedzi na żądanie udziela BG na podstawie informacji uzyskanych od właściwych komórek.

6. Projekt odpowiedzi, o której mowa w ust. 3 lub ust. 5, opiniowany jest przez IOD.

7. Informacji, o których mowa w ust. 1, udziela się na piśmie. W przypadku, gdy wniosek został złożony drogą elektroniczną, informacji udziela się drogą elektroniczną, pod warunkiem, że potwierdzono tożsamość osoby występującej z żądaniem za pomocą danych będących w posiadaniu komórki organizacyjnej oraz przy uwzględnieniu odpowiednich środków zabezpieczających poufność transmisji danych.

§ 9. 1. W razie wykazania przez osobę, której dane osobowe dotyczą, że dane osobowe przetwarzane przez Ministerstwo, lub dla których Minister jest Administratorem, są niekompletne, nieaktualne, nieprawdziwe, lub zostały zebrane z naruszeniem rozporządzenia albo są zbędne do realizacji celu, dla którego zostały zebrane, Administrator lub osoba przez niego upoważniona są zobowiązani do niezwłocznego uzupełnienia, uaktualnienia, sprostowania danych osobowych, ograniczenia przetwarzania kwestionowanych danych osobowych lub ich usunięcia, zgodnie z żądaniem osoby, której dane dotyczą.

2. Zapewnienie prawa do usunięcia danych uzyskanych na podstawie zgody podmiotu danych realizowane jest na etapie pozyskiwania tej zgody. Przed pozyskaniem danych osobowych każdorazowo ustala się tryb wycofania zgody, który może w szczególności polegać na przesłaniu żądania na wskazany adres poczty elektronicznej lub za pomocą Elektronicznej Platformy Usług Administracji Publicznej (ePUAP).

3. O dokonanym sprostowaniu, usunięciu lub ograniczeniu przetwarzania danych osobowych Administrator lub osoba przez niego upoważniona informuje każdego odbiorcę, któremu ujawniono dane osobowe, chyba że okaże się to niemożliwe lub będzie wymagać niewspółmiernie dużego wysiłku.

4. Czynności, o których mowa w ust. 1 – 3, wykonywane są we współpracy z IOD.

Rozdział 5.
Upoważnienie do przetwarzania danych osobowych

§ 10. 1. Do przetwarzania danych osobowych mogą być dopuszczeni jedynie użytkownicy posiadający upoważnienie udzielone przez Administratora albo osobę przez niego upoważnioną, którego wzór określony jest w **załączniku nr 3** do Polityki.

2. W Ministerstwie prowadzona jest Ewidencja osób upoważnionych do przetwarzania danych osobowych, której wzór określa **załącznik nr 4** do Polityki.

3. Ewidencja, o której mowa w ust. 2, nie obejmuje osób, dla których, w związku z zawartymi umowami powierzającymi przetwarzanie danych osobowych, obowiązek wydania upoważnień spoczywa na podmiocie przetwarzającym.

4. Użytkownik, przed rozpoczęciem przetwarzania danych osobowych, potwierdza zapoznanie się z przepisami, procedurami i zasadami, dotyczącymi ochrony danych osobowych, przez złożenie podpisu na upoważnieniu, o którym mowa w ust. 1.

5. Upoważnienie, o którym mowa w ust. 1, traci moc w przypadku:

1) ustania stosunku pracy,

2) zmiany komórki organizacyjnej,

3) zmiany zakresu obowiązków użytkownika powodujących zaprzestanie czynności przetwarzania danych osobowych, do którego upoważnienie posiada,

4) wygaśnięcia upoważnienia wydanego na czas określony.

6. Projekt upoważnienia, o którym mowa w ust. 1, przygotowywany we właściwej komórce organizacyjnej przekazywany jest do dyrektora BG.

7. W przypadkach, o których mowa w ust. 5 lit. 2-4, kierujący komórką organizacyjną zobowiązany jest do niezwłocznego przekazania do dyrektora BG aktualnego projektu upoważnienia, o którym mowa w ust. 1

8. Na wniosek kierującego komórką organizacyjną Administrator albo osoba przez niego upoważniona może odwołać wydane upoważnienie, o którym mowa w ust. 1.

9. Prawo dostępu do danych osobowych przetwarzanych w systemie informatycznym przyznane użytkownikowi, który nie jest pracownikiem Ministerstwa, ma charakter czasowy i jest przyznane na okres obowiązywania umowy zawartej z tym użytkownikiem, w zakresie niezbędnym do jej realizacji.

10. Kierujący komórką organizacyjną, przy uwzględnieniu ryzyka dla zarządzanego obszaru, odpowiada za zorganizowanie właściwej ochrony danych osobowych przetwarzanych w komórce organizacyjnej, w tym za zgodne z przepisami przetwarzanie tych danych przez podległych pracowników w ramach realizacji zadań na poszczególnych stanowiskach pracy.

Rozdział 6.
Obowiązki użytkowników

§ 11. Użytkownicy są w szczególności zobowiązani do:

1) przetwarzania danych osobowych zgodnie z rozporządzeniem, ustawą, dokumentami wewnętrznymi, w tym Polityką, oraz zgodnie z celem, dla którego te dane zostały zebrane;

2) zachowania w tajemnicy danych osobowych oraz sposobów ich zabezpieczania, również po ustaniu zatrudnienia lub innego zobowiązania wynikającego z zawartych umów;

3) przetwarzania danych osobowych w odpowiednio zabezpieczonych pomieszczeniach służbowych lub wyznaczonych ich częściach;

4) bezwzględnego przestrzegania zasad bezpieczeństwa przetwarzania informacji w systemie informatycznym, określonych w Instrukcji lub dokumentach, o których mowa w § 10 ust. 4;

5) zabezpieczania zbiorów danych osobowych oraz dokumentów zawierających dane osobowe przed dostępem osób nieupoważnionych;

6) niszczenia wszystkich zbędnych dokumentów zawierających dane osobowe w sposób uniemożliwiający ich odczytanie lub odtworzenie;

7) nieudzielania innym podmiotom informacji o przetwarzanych danych osobowych, chyba że obowiązek taki wynika wprost z przepisów prawa i tylko w sytuacji, gdy przesłanki określone w tych przepisach zostały spełnione;

8) zgłaszania IOD incydentów związanych z naruszeniem bezpieczeństwa danych oraz niewłaściwym funkcjonowaniem systemu ochrony danych.

§ 12. 1. Za naruszenie obowiązków w zakresie ochrony danych osobowych, pracownicy podlegają odpowiedzialności na podstawie przepisów określonych w ustawie, odpowiedzialności dyscyplinarnej wynikającej z przepisów ustawy z dnia 21 listopada 2008 r. o służbie cywilnej (Dz. U. z 2018 r. poz. 1559 oraz z 2019 r. poz. 730) lub odpowiedzialności porządkowej wynikającej z przepisów prawa pracy.

2. Użytkownicy niebędący pracownikami Ministerstwa, za naruszenie obowiązków, o których mowa w ust.1, podlegają odpowiedzialności na podstawie odrębnych ustaw.

Rozdział 7.
Zapewnienie przestrzegania przepisów o ochronie danych osobowych

§ 13. 1. Dla zapewnienia przestrzegania przepisów o ochronie danych osobowych w Ministerstwie Administrator powołuje Inspektora Ochrony Danych.

2. IOD realizuje zadania samodzielnie oraz we współpracy z:

1) koordynatorem do spraw ochrony danych osobowych w BG;

2) koordynatorami do spraw ochrony danych osobowych w komórkach organizacyjnych;

3) administratorem systemu informatycznego;

4) Zespołem Systemu Zarządzania Bezpieczeństwem Informacji.

§ 14. Do zadań IOD należy w szczególności:

1) informowanie Administratora oraz użytkowników, którzy przetwarzają dane osobowe, o obowiązkach spoczywających na nich na mocy rozporządzenia oraz innych przepisów Unii Europejskiej lub przepisów krajowych o ochronie danych osobowych i doradzanie im w tej sprawie;

2) monitorowanie przestrzegania rozporządzenia, innych przepisów Unii Europejskiej lub przepisów krajowych o ochronie danych osobowych oraz polityk obowiązujących w Ministerstwie w dziedzinie ochrony danych osobowych, w tym:

   a) zbieranie informacji w celu identyfikacji procesów przetwarzania,

   b) analizowanie i sprawdzanie zgodności tego przetwarzania,

   c) informowanie, doradzanie i rekomendowanie Administratorowi określonych działań;

3) doradztwo w zakresie podziału obowiązków w celu przestrzegania regulacji dotyczących ochrony danych osobowych;

4) prowadzenie działań zwiększających świadomość w zakresie obowiązków wynikających z regulacji dotyczących ochrony danych osobowych;

5) przeprowadzanie lub organizowanie szkoleń dla użytkowników uczestniczących w operacjach przetwarzania;

6) udzielanie na żądanie zaleceń i przygotowywanie opinii w ramach konsultacji z Ministrem co do oceny skutków dla ochrony danych oraz monitorowania wykonania oceny skutków dla ochrony danych, zgodnie z art. 35 rozporządzenia;

7) przeprowadzanie systematycznych, okresowych lub doraźnych audytów w zakresie przestrzegania regulacji dotyczących ochrony danych;

8) współpraca z organem nadzorczym, w tym odpowiadanie na wszelkie zapytania organu nadzorczego;

9) pełnienie funkcji punktu kontaktowego dla organu nadzorczego w kwestiach związanych z przetwarzaniem danych osobowych, w tym w przypadku prowadzenia przez organ nadzorczy postępowań kontrolnych, postępowań w związku ze skargą osoby, której dane dotyczą, uprzednimi konsultacjami, o których mowa w art. 36 rozporządzenia oraz w stosownych przypadkach, jak również prowadzenie konsultacji we wszelkich innych sprawach;

10) współpraca z komórkami organizacyjnymi Ministerstwa w kwestiach dotyczących identyfikowania zagrożeń w procesach przetwarzania danych osobowych oraz przeprowadzanie analizy ryzyka;

11) doradzanie i rekomendowanie wdrożenia odpowiednich środków zabezpieczenia oraz najlepszych praktyk pozwalających zminimalizować ryzyko związane z przetwarzaniem danych osobowych;

12) prowadzenie, w imieniu Administratora i pod jego nadzorem, rejestru czynności przetwarzania danych osobowych, o którym mowa w art. 30 rozporządzenia;

13) sprawowanie nadzoru nad wdrożeniem stosownych środków technicznych i organizacyjnych w celu zapewnienia bezpieczeństwa danych osobowych przetwarzanych w Ministerstwie;

14) pełnienie funkcji punktu kontaktowego dla osób, których dotyczą przetwarzane dane, zgodnie z art. 38 ust. 4 rozporządzenia oraz udział w procesie wykonywania praw przysługujących im na mocy rozporządzenia;

15) wykrywanie naruszeń oraz przyjmowanie zgłoszeń sytuacji naruszenia lub podejrzenia naruszenia zasad ochrony danych osobowych, podejmowanie właściwych działań w takich sytuacjach oraz prowadzenie rejestru naruszeń;

16) przygotowywanie do podpisu Ministra zgłoszenia naruszenia ochrony danych osobowych do organu nadzorczego oraz informacji o takim naruszeniu do osób, których dane dotyczą w przypadku przewidzianym prawem;

17) współpraca z komórkami organizacyjnymi Ministerstwa we wszystkich sprawach dotyczących ochrony danych osobowych, w tym opiniowanie dokumentów przygotowywanych przez komórki organizacyjne w zakresie dotyczącym ochrony danych osobowych, w szczególności projektów aktów prawnych oraz projektów umów odnoszących się do danych osobowych w innym zakresie niż powierzenie ich przetwarzania;

18) opiniowanie projektów umów z podmiotami przetwarzającymi w rozumieniu art. 28 rozporządzenia;

19) opiniowanie projektów umów powierzających przetwarzanie danych osobowych Ministrowi przez podmioty zewnętrzne;

20) prowadzenie rejestrów, o których mowa w § 6 ust. 5 i 7 oraz § 19 ust. 11.

§ 15. Do zadań Zespołu Systemu Zarządzania Bezpieczeństwem Informacji, należy wspieranie IOD w realizacji zadań, w szczególności przez:

1) inicjowanie, opracowywanie i aktualizacje wewnętrznych regulacji dotyczących ochrony danych osobowych, w szczególności polityk Administratora;

2) analizę naruszeń ochrony danych osobowych pod kątem zasadności dokonania przez Administratora zgłoszenia organowi nadzorczemu w trybie art. 33 rozporządzenia;

3) przeprowadzanie we współpracy z IOD analizy ryzyka zgodnie z § 26 ust. 2.

§ 16. 1. Kierujący komórką organizacyjną wyznacza spośród swoich pracowników koordynatora do spraw ochrony danych osobowych. W przypadku jego niewyznaczenia, zadania o których mowa w ust. 2, wykonuje kierujący komórką organizacyjną.

2. Do zadań koordynatorów do spraw ochrony danych osobowych, w zakresie ich właściwości w komórkach organizacyjnych, należy w szczególności:

1) bieżąca współpraca z IOD oraz zgłaszania potencjalnych zagrożeń w zakresie ochrony przetwarzania danych osobowych w komórce organizacyjnej;

2) przygotowywanie i weryfikacja projektów upoważnień, o których mowa w § 10 ust. 1;

3) prowadzenie wykazu osób upoważnionych do przetwarzania danych osobowych w komórce organizacyjnej Ministerstwa;

4) monitorowanie aktualności i zakresu wydanych pracownikom komórki organizacyjnej upoważnień do przetwarzania danych osobowych;

5) prowadzenie i aktualizacja wykazu zbiorów danych osobowych przetwarzanych w komórce organizacyjnej;

6) monitorowanie w zakresie właściwości komórki organizacyjnej aktualności rejestrów, o których mowa § 6 ust. 5 i 7 oraz zgłaszanie ewentualnych zmian do IOD;

7) współpraca z IOD w inicjowaniu szkoleń w zakresie ochrony danych osobowych w Ministerstwie;

8) współpraca z IOD w zakresie audytów oraz monitorowanie przestrzegania rozporządzenia oraz Polityki.

3. Do zadań koordynatora do spraw ochrony danych osobowych w BG, poza zadaniami, o których mowa w ust. 2, należy prowadzenie Ewidencji, o której mowa w § 10 ust. 2 zgodnie z zakresem upoważnienia udzielonego przez Administratora lub osobę przez niego upoważnioną.

§ 17. Do zadań administratora systemu informatycznego należy w szczególności:

1) opracowywanie:

a) Instrukcji,

b) dokumentacji opisującej środki techniczne i organizacyjne niezbędne dla zapewnienia poufności, integralności i rozliczalności przetwarzanych danych, o których mowa w **Załączniku nr 5**,

c) dokumentacji w zakresie określania sposobu przepływu danych osobowych pomiędzy poszczególnymi systemami informatycznymi – **Załącznik nr 7**;

2) udział w przeprowadzanych przez IOD audytach zgodności przetwarzania danych osobowych z przepisami o ochronie danych osobowych;

3) opiniowanie projektów umów powierzenia przetwarzania danych osobowych, w których przedmiotem są w szczególności: prace lub usługi wdrożeniowe, przeniesienia, rozbudowy, utrzymania, rozwoju, szkolenia oraz wsparcie techniczne systemów informatycznych;

4) opracowanie oraz opiniowanie projektów wewnętrznych aktów normatywnych Ministerstwa w zakresie przetwarzania danych osobowych w systemach informatycznych;

5) monitorowanie konieczności posiadania przez użytkownika upoważnienia do przetwarzania danych osobowych, przed nadaniem uprawnień do systemu informatycznego przetwarzającego dane osobowe.

§ 18. Środki techniczne i organizacyjne niezbędne dla zapewnienia poufności, integralności i rozliczalności przetwarzania danych osobowych w Ministerstwie zostały określone w **załączniku nr 5** do Polityki.

Rozdział 8.
Postępowanie w przypadku wystąpienia naruszenia ochrony danych osobowych

§ 19. 1. Za naruszenie ochrony danych osobowych uznaje się w szczególności przypadki, gdy:

1) dane osobowe są przetwarzane bez upoważnienia do przetwarzania danych osobowych;

2) nastąpiło nieuprawnione udostępnienie danych osobowych lub nastąpiła kradzież danych;

3) wystąpiły sytuacje losowe lub nieprzewidziane oddziaływanie czynników zewnętrznych, zagrażające bezpieczeństwu danych osobowych (np. zalanie pomieszczeń, wybuch gazu, pożar, katastrofa budowlana, działania terrorystyczne);

4) wystąpiło zaniechanie, choćby nieumyślne, dopełnienia obowiązku zapewnienia ochrony danych osobowych;

5) wystąpiło uszkodzenie, utrata, niekontrolowana zmiana lub nieuprawnione kopiowanie danych;

6) wystąpiła awaria urządzenia, na którym są przetwarzane dane osobowe;

7) odnotowano atak szkodliwego oprogramowania na systemy informatyczne, w których przetwarzane są dane osobowe;

8) wystąpił błąd w oprogramowaniu, które wykorzystywane jest do przetwarzania danych osobowych;

9) stwierdzono naruszenie zabezpieczenia systemu informatycznego wywołane przez użytkownika lub osobę niebędącą użytkownikiem (tzw. hakera, krakera, itp.).

2. Użytkownik, w przypadku podejrzenia wystąpienia naruszenia ochrony danych osobowych, jest zobowiązany do niezwłocznego poinformowania o tym fakcie kierującego właściwą komórką organizacyjną oraz IOD, a jeżeli jest to związane z przetwarzaniem danych osobowych w systemie informatycznym, również administratora systemu informatycznego nie później jednak niż w ciągu 24 godzin od stwierdzenia naruszenia. Przepis stosuje się odpowiednio do podmiotu przetwarzającego.

3. Użytkownik ma obowiązek pozostawienia miejsca zdarzenia w stanie nienaruszonym do czasu przybycia IOD lub innej osoby nadzorującej użytkownika oraz o ile taka możliwość istnieje, podjęcia czynności zmierzających do zmniejszenia ewentualnych skutków naruszenia.

4. Okoliczności naruszenia są dokumentowane przez właściwego kierującego komórką organizacyjną lub inną osobę odpowiedzialną za wyjaśnienie naruszenia, przy współpracy z IOD.

5. Do czynności wyjaśniających i dowodowych należy w szczególności:

a) sporządzenie notatki z przeprowadzonych oględzin miejsca zdarzenia,

b) sporządzenie kopii obrazu/zrzutu z ekranu monitora komputera związanego z naruszeniem,

c) sporządzenie kopii zapisów rejestrów systemu informatycznego służącego do przetwarzania danych osobowych lub zapisów konfiguracji technicznych środków zabezpieczeń systemu,

d) odebranie pisemnych wyjaśnień od osoby zgłaszającej naruszenie.

6. W przypadku zgłoszenia naruszenia, niezwłocznie zwoływane jest posiedzenie Zespołu Systemu Zarządzania Bezpieczeństwem Informacji.

7. IOD, na podstawie materiału dowodowego oraz przy wykorzystaniu wyników analizy ryzyka, o której mowa w § 15 pkt 2 rekomenduje Administratorowi podjęcie decyzji o zaniechaniu lub konieczności zgłoszenia organowi nadzorczemu naruszenia, a także powiadomieniu osoby, której dane dotyczą, z wyjątkiem sytuacji o której mowa w ust. 10.

8. Przy podejmowaniu decyzji, o której mowa w ust. 7, Administrator uwzględnia analizę dokonaną przez Zespół Systemu Zarządzania Bezpieczeństwem Informacji pod kątem skutków przetwarzania danych osobowych, które mogą powodować wysokie ryzyko naruszenia praw i wolności osób fizycznych, w szczególności:

a) dyskryminacji,

b) kradzieży tożsamości,

c) straty finansowej,

d) naruszenia dobrego imienia,

e) naruszenia poufności danych chronionych tajemnicą zawodową,

f) nieuprawnionego odwrócenia pseudonimizacji,

g) utraty przysługujących osobom praw i wolności lub możliwości sprawowania kontroli nad swoimi danymi osobowymi,

h) ujawnienia danych szczególnych kategorii.

9. Administrator zgłasza fakt naruszenia ochrony danych organowi nadzorczemu bez zbędnej zwłoki, nie później niż w terminie 72 godzin po stwierdzeniu naruszenia.

10. Powiadomienie osób, o których mowa w ust. 7, nie będzie konieczne w przypadku, gdy Administrator wdrożył odpowiednie oraz skuteczne techniczne i organizacyjne środki ochrony oraz zastosował je do danych osobowych, których dotyczyło naruszenie. Powiadomienie, o którym mowa w ust. 7, może mieć formę publicznego komunikatu, o ile inne skuteczne środki będą wymagały od Administratora niewspółmiernie dużego kosztu, czasu lub wysiłku.

11. IOD, w imieniu i pod nadzorem Administratora, prowadzi Rejestr naruszeń ochrony danych, którego wzór określa **Załącznik nr 6** do Polityki.

Rozdział 9.
Nadzór w komórkach organizacyjnych

§ 20. 1. Bieżący nadzór nad przetwarzaniem danych osobowych w komórkach organizacyjnych spoczywa na kierujących komórkami organizacyjnymi.

2. W ramach nadzoru, o którym mowa w ust. 1, kierujący komórkami organizacyjnymi są zobowiązani do zapewnienia przestrzegania postanowień Polityki przez użytkowników przetwarzających dane osobowe w danej komórce organizacyjnej oraz do informowania IOD, a jeżeli jest to związane z przetwarzaniem danych osobowych w systemie informatycznym, również administratora systemu informatycznego o stwierdzonych nieprawidłowościach oraz naruszeniach ochrony danych osobowych, o których mowa w § 19 ust. 1.

3. W ramach nadzoru kierujący komórkami organizacyjnymi są zobowiązani do zgłaszania do IOD wszelkich zmian dokonywanych w czynnościach przetwarzania danych osobowych znajdujących się we właściwości danej komórki organizacyjnej, potrzeb w zakresie zgłoszenia nowych czynności przetwarzania lub usunięcia tych, dla których ustał cel przetwarzania.

Rozdział 10.
Audyty zgodności przetwarzania danych osobowych

§ 21. 1. IOD zawiadamia kierującego komórką organizacyjną objętą audytem o zakresie planowanych czynności w terminie co najmniej 7 dni przed dniem przeprowadzenia czynności.

2. IOD dokumentuje czynności przeprowadzone podczas audytu poprzez:

1) utrwalanie danych z systemu informatycznego służącego do przetwarzania danych lub zabezpieczenia danych osobowych na informatycznym nośniku danych lub dokonaniu wydruku tych danych;

2) sporządzanie notatki z czynności, w szczególności z zebranych wyjaśnień, przeprowadzonych oględzin oraz czynności związanych z dostępem do urządzeń, nośników oraz systemów informatycznych służących do przetwarzania danych osobowych;

3) odbieranie ustnych lub pisemnych wyjaśnień od osoby, której czynności objęto audytem;

4) sporządzanie kopii otrzymanego dokumentu, oraz obrazu wyświetlonego na ekranie urządzenia stanowiącego część systemu informatycznego służącego do przetwarzania lub zabezpieczania danych osobowych;

5) sporządzanie kopii zapisów rejestrów systemu informatycznego służącego do przetwarzania danych osobowych lub zapisów konfiguracji technicznych środków zabezpieczeń tego systemu.

3. Materiały dokumentujące czynności przeprowadzane podczas audytu są sporządzane w postaci papierowej lub w postaci elektronicznej, w tym w postaci fotografii cyfrowej.

4. Z przeprowadzonego audytu IOD sporządza sprawozdanie zawierające m.in. ocenę i rekomendacje w odniesieniu do zakresu objętego audytem.

5. Sprawozdanie, o którym mowa w ust. 4, przedkładane jest Administratorowi, nie później niż w terminie 15 dni od dnia zakończenia audytu oraz udostępniane kierującemu audytowanej komórki organizacyjnej – do wiadomości.

Rozdział 11.
Szkolenia

§ 22. 1. Administrator zapewnia szkolenia dla użytkowników w zakresie obowiązujących przepisów, procedur oraz podstawowych zagrożeń związanych z przetwarzaniem danych osobowych.

2. Szkolenia prowadzi IOD lub podmiot zewnętrzny posiadający wiedzę z zakresu ochrony danych osobowych.

Rozdział 12.
Uwzględnianie ochrony danych w fazie projektowania oraz domyślna ochrona danych

§ 23. Kierujący komórką organizacyjną, na etapie opracowania specyfikacji istotnych warunków zamówienia dotyczących usług lub narzędzi informatycznych, w ramach których będą przetwarzane dane osobowe, określa wymagania uwzględniające ochronę danych osobowych w porozumieniu z IOD. Kierujący komórką organizacyjną, w porozumieniu z IOD, na etapie opracowania specyfikacji istotnych warunków zamówienia dotyczących usług lub narzędzi informatycznych, w ramach których będą przetwarzane dane osobowe, wymaga od wykonawcy stosowania zasady domyślnej ochrony danych, tj. jak najdalej posuniętych zabezpieczeń prywatności w ustawieniach początkowych każdego systemu.

Rozdział 13.
Bezpieczeństwo przetwarzania, analiza ryzyka naruszenia praw i wolności podmiotów danych

§ 24. Dokumentacja opisująca sposób przetwarzania danych osobowych oraz sposoby ich zabezpieczenia, w tym w systemach informatycznych służących do przetwarzania danych osobowych w Ministerstwie, nie jest udostępniana podmiotom zewnętrznym.

§ 25. W doborze i stosowaniu środków ochrony przetwarzanych danych osobowych każdy użytkownik w zakresie swoich uprawnień na zajmowanym stanowisku pracy powinien zwracać szczególną uwagę na należyte ich zabezpieczenie przed udostępnieniem osobom nieuprawnionym, kradzieżą, uszkodzeniem, nieuprawnioną modyfikacją, utratą lub zniszczeniem, kierując się przy tym obowiązującymi w Ministerstwie regulacjami, o których mowa w szczególności w **Załączniku nr 5** do Polityki.

§ 26. 1. Administrator, w oparciu o analizę ryzyka naruszenia praw i wolności podmiotów danych, wdraża odpowiednie środki techniczne i organizacyjne, adekwatne do celu, jakim jest zapewnienie zgodności przetwarzania z rozporządzeniem.

2. Analiza ryzyka, o której mowa w ust. 1, dokonywana jest przez IOD we współpracy z Zespołem Systemu Zarządzania Bezpieczeństwem Informacji.

3. Wyniki analizy ryzyka Zespół Systemu Zarządzania Bezpieczeństwem Informacji przedkłada Administratorowi.

Rozdział 14.
Ocena skutków dla ochrony danych

§ 27. 1. Dokonanie oceny skutków dla ochrony danych wymagane jest dla następujących operacji przetwarzania:

1) systematycznej, kompleksowej oceny czynników osobowych odnoszących się do osób fizycznych, która opiera się na zautomatyzowanym przetwarzaniu, w tym profilowaniu, i jest podstawą decyzji wywołujących skutki prawne wobec osoby fizycznej lub w podobny sposób znacząco wpływających na osobę fizyczną;

2) przetwarzania na dużą skalę szczególnych kategorii danych osobowych, o których mowa w art. 9 ust. 1 i art. 10 rozporządzenia;

3) systematycznego monitorowania na dużą skalę miejsc dostępnych publicznie.

2. W przypadku wdrażania nowych operacji przetwarzania w komórce organizacyjnej, kierujący komórkami organizacyjnymi konsultują z IOD zasadność przeprowadzenia oceny, o której mowa w ust. 1.

3. W procesie legislacyjnym projektów rozporządzeń oraz ustaw, w ramach których regulowane będą kwestie przetwarzania danych osobowych, ocena skutków dla ochrony danych sporządzana jest na etapie dokonywania oceny skutków regulacji (OSR).

4. Ocena skutków dla ochrony danych konsultowana jest z IOD.

Rozdział 15.
Obszar przetwarzania

§ 28. 1. Obszarem przetwarzania danych osobowych są:

1) pomieszczenia, w którym przetwarzane są dane osobowe znajdujące się w lokalizacji budynków przy ul. Senatorskiej 14 i 12 w Warszawie, będących w użytkowaniu Ministerstwa;

2) pomieszczenia zlokalizowane poza siedzibą główną Ministerstwa, w których przetwarzane są dane, na podstawie odrębnych umów lub porozumień;

3) sprzęty elektroniczne, na których przetwarzane są dane osobowe.

2. Stosowane środki bezpieczeństwa oraz obowiązki pracowników w przypadku obszarów przetwarzania określają postanowienia Instrukcji.

Rozdział 16.
Postanowienia końcowe

§ 29. Polityka nie wyłącza stosowania innych instrukcji dotyczących zabezpieczenia systemu informatycznego lub zbiorów papierowych Ministerstwa.

Załącznik nr 1
do Polityki Ochrony Danych Osobowych w Ministerstwie Sportu

REJESTR CZYNNOŚCI PRZETWARZANIA W MINISTERSTWIE SPORTU

lp.	komórka organizacyjna	ID zbioru	kategoria danych osobowych	czynności przetwarzania	kategoria osób	podstawa prawna przetwarzania	cel przetwarzania	źródło pochodzenia danych[1]	kategorie odbiorców danych[2]	umowa powierzenia	przekazywanie danych[3]	termin usunięcia danych[4]	rodzaje technicznych i organizacyjnych środków bezpieczeństwa[5]	sposób przetwarzania danych osobowych[6]	ocena środków organizacyjnych i technicznych[7]	dane osobowe szczególnej kategorii[8]	czy dane osobowe są aktualne i prawidłowe?	koordynator[9]	utrzymywanie lub przetwarzanie zbioru przez podmiot zewnętrzny[10]

[1] zbierane przez Ministerstwo, czy otrzymane od innego podmiotu, jeśli tak to jakiego
[2] o ile są one przez Ministerstwo przekazywane lub ujawniane
[3] do państwa trzeciego lub organizacji międzynarodowej
[4] wynikający z przepisów prawa lub instrukcji archiwalnej
[5] art. 32 RODO lub odwołanie do istniejących procedur wewnętrznych
[6] przetwarzanie w postaci elektronicznej, w tym konkretne systemy informatyczne, przetwarzanie w postaci fizycznej
[7] czy stosowane środki bezpieczeństwa (organizacyjne i techniczne) są w ocenie kierującego komórką organizacyjną skuteczne
[8] art. 9 RODO
[9] imię nazwisko koordynatora do spraw ochrony danych osobowych
[10] Wskazać podstawę prawną (np. umowa)

Załącznik nr 2

do Polityki Ochrony Danych Osobowych w Ministerstwie Sportu

REJESTR KATEGORII PRZETWARZANIA W MINISTERSTWIE SPORTU

Rejestr kategorii przetwarzania

Nazwa i dane kontaktowe podmiotu przetwarzającego	
Nazwa	
Adres	
Email	
Telefon	

Inspektor Ochrony Danych (jeśli powołano)	
Nazwa	
Adres	
Email	
Telefon	

Administrator, w imieniu którego działa podmiot przetwarzający	
Nazwa	
Adres	
Email	
Telefon	

Lp.	Kategorie przetwarzań	Ogólny opis technicznych i organizacyjnych środków bezpieczeństwa (jeżeli jest to możliwe)	Administrator				Czas trwania przetwarzania	Nazwy państw trzecich lub organizacji międzynarodowych, do których dane są przekazywane	Dokumentacja odpowiednich zabezpieczeń danych osobowych przekazywanych na podstawie art. 49 ust. 1 akapit drugi	Podprzetwarzający (podwykonawca) - jeśli dotyczy	
			Nazwa i dane kontaktowe administratora	Nazwa i dane kontaktowe współadministratora (jeśli dotyczy)	Nazwa i dane kontaktowe przedstawiciela administratora (jeśli wyznaczono)	Inspektor ochrony danych administratora (jeśli powołano)				Nazwa i dane kontaktowe podprzetwarzającego (podwykonawcy)	Kategorie podpowierzonych przetwarzań
1.											
2.											
3.											
4.											
5.											
6.											

Załącznik nr 3
do Polityki Ochrony Danych Osobowych w Ministerstwie Sportu

.....
Minister Sportu

Warszawa, dnia …….

UPOWAŻNIENIE

Działając na podstawie udzielonego mi upoważnienia/pełnomocnictwa z dnia nr….. .oraz zgodnie z art. 29 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 (Dz. Urz. UE L 119 z 04.05.2016, str.1), zwanego dalej rozporządzeniem upoważniam Pana/Panią:

……..…
(imię i nazwisko)

do wykonywania niżej wymienionych czynności przetwarzania danych osobowych w Ministerstwie Sportu/*do przetwarzania danych osobowych w zakresie zbioru danych:
- [_____],
- [_____],

w ramach zakresu zadań realizowanych w ……..……..……
(nazwa departamentu, biura)

na stanowisku pracy, na którym dane osobowe są przetwarzane/*wynikających z umowy……..…

Niniejsze upoważnienie wygasa z dniem…../ z chwilą ustania stosunku pracy Pana/Pani w Departamencie/Biurze w Ministerstwie Sportu zmiany zakresu obowiązków powodującej zaprzestanie przetwarzania danych osobowych w ramach ww. czynności przetwarzania danych osobowych/zbiorze/-ach danych /* zaprzestania wykonywania zadań w ramach umowy cywilnoprawnej /*

……..……..……..

……...
(pieczątka i podpis osoby upoważnionej do wydania upoważnienia)

Oświadczam, że zapoznałem/am się z przepisami rozporządzenia, ustawą**, a także z obowiązującą w Ministerstwie Sportu Polityką Ochrony Danych Osobowych oraz Instrukcją zarządzania systemem teleinformatycznym i zobowiązuję się do przestrzegania zasad przetwarzania danych osobowych określonych w tych dokumentach.
Zobowiązuję się do zachowania w tajemnicy przetwarzanych danych osobowych, z którymi zapoznałem/am się oraz sposobów ich zabezpieczania, zarówno w okresie zatrudnienia w Ministerstwie Sportu, jak też po jego ustaniu/*wykonywania zadań wynikających z łączących mnie z Ministerstwem Sportu stosunków prawnych.

……
(czytelny podpis osoby upoważnionej)

Upoważnienie otrzymałem/am

……
(miejscowość, data, podpis)

*niepotrzebne skreślić
** ustawa z dnia 10 maja 2018 r. o ochronie danych osobowych (Dz. U. z 2019 r. poz. 1781)

Załącznik nr 4
do Polityki Ochrony Danych Osobowych w Ministerstwie Sportu

Ewidencja osób upoważnionych do przetwarzania danych osobowych w Ministerstwie Sportu

Lp.	Imię i nazwisko	Komórka organizacyjna/ Inny podmiot	Czynność przetwarzania/ zbiór	Nazwa systemu informatycznego, w którym dane osobowe są przetwarzane	Identyfikator użytkownika w systemie informatycznym	Zakres przydzielonych uprawnień (system/rola)	Data wydania upoważnienia	Data wygaśnięcia upoważnienia

Załącznik nr 5
do Polityki Ochrony Danych Osobowych w Ministerstwie Sportu

Środki techniczne i organizacyjne niezbędne dla zapewnienia poufności, integralności i rozliczalności przetwarzania danych osobowych w Ministerstwie Sportu

Zastosowane środki ochrony fizycznej danych osobowych:
- całodobowa ochrona fizyczna,
- bramki obrotowe współpracujące z informatycznym systemem kontroli dostępu umożliwiające wstęp na teren budynku (otwierane za pomocą kart zbliżeniowych),
- wydawanie i zdawanie kluczy do pomieszczeń Ministerstwa podlegających szczególnej ochronie odbywa się za pokwitowaniem i jest odnotowywane w księgach ewidencji kluczy, lub ewidencjonowane elektroniczne przez oprogramowanie współpracujące z depozytorem kluczy,
- system telewizji przemysłowej,
- osoby nieposiadające stałych kart zbliżeniowych przebywają na terenie budynku pod opieką pracownika, po uprzednim zarejestrowaniu w recepcji,
- dokumenty papierowe oraz płyty (CD, DVD) zawierające dane osobowe po ustaniu przydatności są niszczone w sposób mechaniczny za pomocą niszczarek.

Zastosowane środki sprzętowe, informatyczne i telekomunikacyjne:
- system IDS/IPS chroniący dostęp do sieci komputerowej Ministerstwa,
- firewall-e chroniące zasoby Ministerstwa przed zagrożeniami pochodzącymi z sieci publicznej,
- możliwość zarządzania urządzeniami tylko z wydzielonych podsieci, do których nieuprawnieni pracownicy Ministerstwa nie posiadają dostępu,
- generator prądu (w lokalizacji przy ul. Senatorskiej 12), urządzenia UPS i wydzielona sieć elektroenergetyczna chronią system służący do przetwarzania danych osobowych przed skutkami awarii zasilania,
- system antywirusowy zabezpieczający wewnętrzne systemy Ministerstwa przed złośliwym oprogramowaniem,
- autentykacja użytkownika za pomocą identyfikatora i hasła,
- środki ochrony kryptograficznej (np. szyfrowanie, pseudonimizacja)

Zastosowane środki ochrony w ramach narzędzi programowych i baz danych:
- rozliczalność operacji wykonywanych w systemie przez użytkowników na podstawie przyznanych im identyfikatorów,
- autentykacja użytkowników z pomocą identyfikatorów i haseł,
- mechanizm wymuszający okresową zmianę hasła (w przypadku braku w/w mechanizmu użytkownik zobowiązany jest do zmiany hasła zgodnie z wytycznymi zawartymi w Instrukcji zarządzania systemem informatycznym służącym do przetwarzania danych osobowych),
- zainstalowano wygaszacze ekranu na stacjach roboczych,
- mechanizm automatycznej blokady dostępu systemu operacyjnego w przypadku dłuższej nieaktywności pracy użytkownika.

Zastosowane środki ochrony w ramach systemu operacyjnego:
- scentralizowane uwierzytelnianie użytkowników domenowych na podstawie identyfikatorów i haseł,
- mechanizm wymuszający okresową zmianę hasła domenowego,
- kontrola uprawnień użytkownika wymuszana odpowiednimi polisami grupowymi,
- rozliczalność operacji wykonywanych w systemie przez użytkowników na podstawie przyznanych im identyfikatorów.

Zastosowane środki organizacyjne:
- Regulamin organizacyjny Ministerstwa,
- Regulamin pracy w Ministerstwie,
- Procedura postępowania z incydentami związanymi z bezpieczeństwem informacji,
- Polityka bezpieczeństwa Informacji,
- wewnętrzne uregulowania Ministerstwa związane z bezpieczeństwem informacji przetwarzanych w systemach informatycznych, w tym Instrukcja zarządzania systemem teleinformatycznym,
- zasada privacy by design,
- zasada privacy by default.

Załącznik nr 6
do Polityki Ochrony Danych Osobowych w Ministerstwie Sportu

REJESTR NARUSZEŃ OCHRONY DANYCH OSOBOWYCH W MINISTERSTWIE SPORTU

Lp.	Miejsce wystąpienia naruszenia	Data i godz. wystąpienia naruszenia	Data i godz. stwierdzenia naruszenia	Osoba zgłaszająca naruszenie/nazwa KO/Podmiot przetwarzający	Okoliczności wystąpienia naruszenia	Skutki i konsekwencje wywołane naruszeniem	Podjęte środki zaradcze	Decyzja o zgłoszeniu do organu nadzorczego lub uzasadnienie niezgłoszenia naruszenia	Data zgłoszenia do organu nadzorczego (godz. wysłania)	Uwagi
1.										
2.										
3.										
4.										
5.										

Załącznik nr 7
do Polityki Ochrony Danych Osobowych w Ministerstwie Sportu

Sposób przepływu danych osobowych pomiędzy poszczególnymi systemami informatycznymi w Ministerstwie Sportu

Lp.	Nazwa systemu, w którym są przetwarzane dane osobowe	Nazwa innego systemu, w którym są przetwarzane dane osobowe	Sposób przepływu danych pomiędzy poszczególnymi systemami informatycznymi