Warszawa, dnia 11 września 2017 r.

Poz. 71

ZARZĄDZENIE NR 24
MINISTRA SPORTU I TURYSTYKI[1)]

z dnia 11 września 2017 r.

w sprawie wprowadzenia Polityki ochrony danych osobowych w Ministerstwie Sportu i Turystyki

Na podstawie art. 36 ust. 2 ustawy z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (Dz. U. z 2016 r. poz. 922) oraz § 3 ust. 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. poz. 1024) zarządza się, co następuje:

§ 1. W Ministerstwie Sportu i Turystyki wprowadza się Politykę ochrony danych osobowych w Ministerstwie Sportu i Turystyki, stanowiącą załącznik do zarządzenia.

§ 2. Traci moc zarządzenie nr 20 Ministra Sportu i Turystyki z dnia 9 lipca 2013 r. w sprawie ustalenia zasad bezpieczeństwa informacji w Ministerstwie Sportu i Turystyki (Dz. Urz. Min. Spor. poz. 21).

§ 3. Zarządzenie wchodzi w życie z dniem 15 września 2017 r.

Minister Sportu i Turystyki

Witold Bańka

[1)] Minister Sportu i Turystyki kieruje działami administracji rządowej – kultura fizyczna oraz turystyka, na podstawie § 1 ust. 2 rozporządzenia Prezesa Rady Ministrów z dnia 17 listopada 2015 r. w sprawie szczegółowego zakresu działania Ministra Sportu i Turystyki (Dz. U. poz. 1911).

Załącznik do Zarządzenia Nr .....

Ministra Sportu i Turystyki

z dnia.....2017 r.

POLITYKA OCHRONY DANYCH OSOBOWYCH

W MINISTERSTWIE SPORTU I TURYSTYKI

Rozdział 1.
POSTANOWIENIA OGÓLNE

§ 1. 1. Polityka ochrony danych osobowych, zwana dalej „Polityką”, stanowi zestaw praw i reguł określających sposób zarządzania, ochrony i przetwarzania tych danych w Ministerstwie.

2. Polityka jest dokumentem określającym zasady i tryb postępowania przy przetwarzaniu danych osobowych w zbiorach danych:

1) w systemach informatycznych;

2) w kartotekach, księgach, wykazach, skorowidzach i innych zbiorach ewidencyjnych.

3. Ochrona danych osobowych obowiązuje wszystkie osoby, które mają dostęp do informacji przetwarzanych w Ministerstwie.

4. Osoby mające dostęp do danych osobowych są zobligowane do stosowania niezbędnych środków zapobiegających ujawnieniu tych danych osobom nieupoważnionym.

5. Administrator Danych jest odpowiedzialny za wdrożenie i interpretację Polityki oraz opracowanie procedur w zakresie przetwarzania danych osobowych w Ministerstwie.

6. Polecenia osób delegowanych w zakresie ochrony danych osobowych, wyznaczonych przez Administratora Danych, do działań w zakresie ochrony danych osobowych w Ministerstwie muszą być bezwzględnie wykonywane.

7. Gromadzenie i przetwarzanie danych osobowych w Ministerstwie jest dopuszczalne wyłącznie w zakresie niezbędnym do wykonywania zadań Ministra Sportu i Turystyki.

8. Wszyscy pracownicy Ministerstwa, pod groźbą sankcji dyscyplinarnych, mają obowiązek zachowania tajemnicy o przetwarzanych w Ministerstwie danych osobowych oraz o stosowanych sposobach zabezpieczeń danych osobowych. Zachowanie tajemnicy obowiązuje zarówno podczas trwania stosunku pracy, jak i po jego ustaniu.

§ 2. Użyte w Polityce określenia oznaczają:

1) **Ministerstwo** - Ministerstwo Sportu i Turystyki;

2) **Komórka organizacyjna** - właściwy rzeczowo departament lub biuro, którego zadania określone zostały w Regulaminie organizacyjnym Ministerstwa Sportu i Turystyki, stanowiącym załącznik do zarządzenia nr 6 Ministra Sportu i Turystyki z dnia 31 marca 2016 r. w sprawie ustalenia Regulaminu organizacyjnego Ministerstwa Sportu i Turystyki (Dz. Urz. Min. Spor. poz. 6 i 18 oraz z 2017 r. poz. 51);

3) **Ustawa -** ustawa z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (Dz. U. z 2016 r. poz. 922);

4) **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. poz. 1024);

5) **Administrator Danych** - Minister Sportu i Turystyki;

6) **Administrator Bezpieczeństwa Informacji** - pracownik Ministerstwa wyznaczony przez Administratora Danych, nadzorujący i kontrolujący przestrzeganie zasad ochrony danych osobowych w Ministerstwie;

7) **Administrator Systemu Informatycznego** - pracownik Ministerstwa wyznaczony przez Administratora Danych, nadzorujący i kontrolujący funkcjonowanie całości systemu informatycznego Ministerstwa, w szczególności części systemu, w których przetwarzane są dane osobowe;

8) **Lokalny Administrator Systemu Informatycznego** - specjalista informatyk, realizujący zadania techniczne w celu zapewnienia bezpiecznej eksploatacji wybranych urządzeń i aplikacji wykorzystywanych do przetwarzania danych;

9) **Koordynator Zbiorów Danych** - pracownik Ministerstwa wyznaczony przez dyrektora komórki organizacyjnej w Ministerstwie do prowadzenia ogółu spraw z zakresu ochrony danych osobowych w komórce organizacyjnej;

10) **System informatyczny** - zestaw urządzeń (w tym komputerów), programów i narzędzi programowych oraz metod postępowania i procedur, stosowanych w celu przetwarzania danych;

11) **Dane osobowe** - wszelkie informacje dotyczące zidentyfikowanej lub możliwej do zidentyfikowania osoby fizycznej; osobą możliwą do zidentyfikowania jest osoba, której tożsamość można określić bezpośrednio lub pośrednio, w szczególności poprzez powołanie się na numer identyfikacyjny albo jeden lub kilka specyficznych czynników określających jej cechy fizyczne, fizjologiczne, umysłowe, ekonomiczne, kulturowe lub społeczne;

12) **Naruszenie bezpieczeństwa** - jakiekolwiek naruszenie **zabezpieczenia** niezawodności, integralności lub poufności informacji;

13) **Nośnik -** dyskietki, płyty CD lub DVD, pamięć flash, dyski twarde, taśmy magnetyczne lub inne urządzenia lub materiały służące do przechowywania plików z danymi;

14) **Generalny Inspektor Ochrony Danych Osobowych -** organ do spraw ochrony danych osobowych działający na podstawie ustawy;

15) **Użytkownik -** pracownik przetwarzający dane, w tym dane osobowe, w systemie informatycznym, w ramach wykonywanych zadań, lub osoba przetwarzająca takie dane w ramach wykonywania czynności na podstawie umowy cywilnoprawnej, praktykant, wolontariusz lub stażysta.

Rozdział 2.
CEL I ZAKRES STOSOWANIA

§ 3. 1. Celem Polityki jest określenie postępowania gwarantującego bezpieczeństwo przetwarzanych danych osobowych w Ministerstwie, poprzez podejmowanie działań zapewniających ich poufność, integralność, dostępność i rozliczalność.

2. Zakres przedmiotowy stosowania niniejszej Polityki obejmuje wszystkie zbiory danych osobowych, przetwarzanych w Ministerstwie, zarówno w formie elektronicznej jak i papierowej.

§ 4. 1. Obszar, w ramach którego przetwarzane są informacje, w tym dane osobowe, obejmuje budynki Ministerstwa.

2. Obszar, o którym mowa w ust. 1, obejmuje również budynki i pomieszczenia podmiotów zewnętrznych, którym na podstawie zawartych umów powierzono przetwarzanie danych osobowych, w zakresie niezbędnym do wykonywania zadań Ministra Sportu i Turystyki.

Rozdział 3.
SYSTEM OCHRONY DANYCH OSOBOWYCH

§ 5. Politykę stosuje się do zbiorów danych przetwarzanych w Ministerstwie.

§ 6. 1. Administrator Bezpieczeństwa Informacji (ABI) prowadzi Wykaz zbiorów danych osobowych przetwarzanych w Ministerstwie, zawierający wykaz budynków, tworzących obszar, w którym przetwarzane są dane osobowe wraz z programami zastosowanymi do ich przetwarzania, według wzoru stanowiącego załącznik nr 6 do Polityki.

2. Opis struktury zbiorów danych, wskazujący na zawartość poszczególnych pól informacyjnych i powiązania między nimi, jest udostępniany przez Administratora Systemu Informatycznego (ASI).

§ 7. O celach i środkach przetwarzania danych osobowych w Ministerstwie decyduje Administrator Danych (AD).

§ 8. 1. W celu nadzoru nad przestrzeganiem zasad ochrony danych osobowych w Ministerstwie, Administrator Danych wyznacza Administratora Bezpieczeństwa Informacji.

2. W celu nadzoru nad systemem informatycznym Ministerstwa, Administrator Danych wyznacza Administratora Systemu Informatycznego.

§ 9. Nadzór nad zbiorami danych osobowych w komórkach organizacyjnych sprawują dyrektorzy tych komórek.

Rozdział 4.
PRZETWARZANIE DANYCH OSOBOWYCH

§ 10. Dane osobowe przetwarzane w Ministerstwie podlegają ochronie zgodnie z przepisami ustawy.

§ 11. Przetwarzanie danych osobowych w Ministerstwie jest dopuszczalne wyłącznie w zakresie określonym w upoważnieniu do przetwarzania danych osobowych.

§ 12. Przetwarzanie danych osobowych nie może naruszać praw i wolności osób, których dane osobowe dotyczą. W szczególności zabrania się przetwarzania danych osobowych ujawniających pochodzenie rasowe lub etniczne, poglądy polityczne, przekonania religijne lub filozoficzne, przynależność wyznaniową, partyjną lub związkową, jak również danych o stanie zdrowia, kodzie genetycznym, nałogach lub życiu seksualnym oraz danych dotyczących skazań, orzeczeń o ukaraniu i mandatów karnych, a także innych orzeczeń wydanych w postępowaniu sądowym lub administracyjnym.

§ 13. W przypadku zbierania jakichkolwiek danych osobowych na potrzeby Ministerstwa bezpośrednio od osoby, której dane dotyczą, pracownik zbierający dane osobowe jest zobowiązany do przekazania tej osobie informacji o przysługujących jej prawach, w szczególności o:

1) pełnej nazwie i adresie siedziby Administratora Danych;

2) celu zbierania danych osobowych;

3) prawie dostępu do treści swoich danych osobowych oraz ich poprawiania;

4) dobrowolności podania danych osobowych lub obowiązku podania danych, a jeśli taki obowiązek istnieje, o jego podstawie prawnej.

§ 14. Każdej osobie, której dane osobowe są przetwarzane w Ministerstwie przysługuje prawo do kontroli przetwarzania jej danych osobowych, a w szczególności prawo do:

1) uzyskania wyczerpującej informacji, czy jej dane osobowe są przetwarzane oraz do otrzymania informacji o pełnej nazwie i adresie siedziby Administratora Danych;

2) uzyskania informacji o celu, zakresie i sposobie przetwarzania danych osobowych;

3) uzyskania informacji, od kiedy są przetwarzane jej dane osobowe, oraz podania w powszechnie zrozumiałej formie treści tych danych;

4) uzyskania informacji o źródle, z którego pochodzą dane osobowe jej dotyczące;

5) uzyskania informacji o sposobie udostępniania danych osobowych, a w szczególności informacji o odbiorcach lub kategoriach odbiorców, którym te dane osobowe są udostępniane;

6) żądania uzupełnienia, uaktualnienia, sprostowania danych osobowych, czasowego lub stałego wstrzymania ich przetwarzania lub ich usunięcia, jeżeli są one niekompletne, nieaktualne, nieprawdziwe lub zostały zebrane z naruszeniem ustawy albo są już zbędne do realizacji celu, dla którego zostały zebrane.

§ 15. Na wniosek osoby, której dane osobowe dotyczą, Administrator Bezpieczeństwa Informacji jest zobowiązany, w terminie do 30 dni od dnia wpłynięcia wniosku, wskazać w powszechnie zrozumiałej formie:

1) zakres przetwarzanych danych osobowych wnioskodawcy;

2) sposób pozyskania danych;

3) cel przetwarzania danych;

4) termin rozpoczęcia przetwarzania danych;

5) odbiorców oraz zakres udostępnienia danych.

§ 16. W razie wykazania przez osobę, której dane dotyczą, że jej dane osobowe, przetwarzane w Ministerstwie są niekompletne, nieaktualne, nieprawdziwe lub zostały zebrane z naruszeniem ustawy, Administrator Bezpieczeństwa Informacji jest zobowiązany do uzupełnienia, uaktualnienia, sprostowania danych osobowych lub ich usunięcia, zgodnie z żądaniem osoby, której dane osobowe dotyczą.

§ 17. 1. Do przetwarzania danych osobowych w Ministerstwie mogą być dopuszczeni jedynie pracownicy posiadający pisemne upoważnienie wydane przez Administratora Danych.

2. Pracownik Ministerstwa, przed dopuszczeniem go do przetwarzania danych osobowych, jest obowiązany do zapoznania się z przepisami i procedurami dotyczącymi ochrony danych osobowych.

§ 18. Dostęp do danych osobowych, przetwarzanych w Ministerstwie, osoby niebędącej pracownikiem Ministerstwa, jest możliwy po uzyskaniu pozytywnej opinii Administratora Bezpieczeństwa Informacji, na podstawie pisemnego upoważnienia wydanego przez Administratora Danych oraz podpisaniu przez taką osobę oświadczenia o poufności. Wzór oświadczenia stanowi załącznik nr 4 do Polityki.

Rozdział 5.
DOSTĘP PODMIOTÓW ZEWNĘTRZNYCH

§ 19. Celem procedury jest zapewnienie ochrony informacji, w szczególności danych osobowych, udostępnionych lub powierzonych do przetwarzania przez Ministerstwo podmiotom zewnętrznym.

§ 20. 1. Przetwarzanie danych osobowych zgromadzonych w Ministerstwie może zostać powierzone podmiotowi zewnętrznemu, wyłącznie w zakresie określonym w § 1 ust. 7, pod warunkiem zawarcia z tym podmiotem pisemnej umowy, w pełni uwzględniającej przepisy ustawy, rozporządzenia oraz wewnętrzne procedury Ministerstwa.

2. Zawarcie umowy, o której mowa w ust. 1, wymaga uzyskania pozytywnej opinii Administratora Bezpieczeństwa Informacji oraz zgody Administratora Danych.

3. Postanowienia umowy, o której mowa w ust. 1, zobowiązują podmiot zewnętrzny, któremu powierzono przetwarzanie danych osobowych m.in. do:

1) przetwarzania danych zgodnie z celem i zakresem określonym w umowie;

2) zastosowania, przed rozpoczęciem przetwarzania danych, zabezpieczeń określonych w rozporządzeniu.

§ 21. 1. Udostępnianie podmiotom zewnętrznym danych osobowych przetwarzanych w Ministerstwie może się odbywać wyłącznie w trybie określonym w ustawie i procedurach wewnętrznych.

2. Każdorazowe udostępnienie podmiotowi zewnętrznemu danych osobowych przetwarzanych w Ministerstwie wymaga pozytywnej opinii Administratora Bezpieczeństwa Informacji oraz zgody Administratora Danych.

3. Dane osobowe przetwarzane w Ministerstwie udostępnia się na pisemny umotywowany wniosek, chyba że przepisy odrębne stanowią inaczej.

§ 22. Dane udostępniane Ministerstwu przez podmiot zewnętrzny wykorzystywane są zgodnie z przeznaczeniem, dla którego zostały udostępnione.

Rozdział 6.
OBOWIĄZKI I UPRAWNIENIA W SYSTEMIE OCHRONY DANYCH OSOBOWYCH

§ 23. 1. ADMINISTRATOR DANYCH jest obowiązany zastosować środki techniczne i organizacyjne zapewniające odpowiednią do zagrożeń oraz kategorii danych ochronę przetwarzanych danych osobowych, a w szczególności powinien zabezpieczyć dane przed ich udostępnieniem osobom nieupoważnionym, zabraniem przez osobę nieuprawnioną, przetwarzaniem z naruszeniem ustawy oraz zmianą, utratą, uszkodzeniem lub zniszczeniem.

2. Do zadań Administratora Danych należy:

1) zatwierdzanie Polityki ochrony danych osobowych w Ministerstwie;

2) udzielanie upoważnień do przetwarzania danych osobowych w zakresie, o którym mowa w § 1 ust. 7;

3) wyznaczenie Administratora Bezpieczeństwa Informacji;

4) wyznaczenie Administratora Systemu Informatycznego;

5) współpraca z Generalnym Inspektorem Ochrony Danych Osobowych, w tym zgłaszanie Generalnemu Inspektorowi Ochrony Danych Osobowych zbiorów danych osobowych Ministerstwa podlegających rejestracji;

6) podejmowanie odpowiednich działań w przypadku naruszenia lub podejrzenia naruszenia zabezpieczenia danych osobowych.

§ 24. 1. ADMINISTRATOR BEZPIECZEŃSTWA INFORMACJI wdraża i nadzoruje przestrzeganie zasad ochrony danych osobowych w Ministerstwie.

2. Do zadań Administratora Bezpieczeństwa Informacji należy:

1) współdziałanie z Administratorem Danych w zakresie zapewniającym wypełnianie obowiązków wynikających z ustawy i rozporządzenia oraz przepisów wewnętrznych Ministerstwa;

2) sprawowanie nadzoru nad wdrożeniem stosownych środków organizacyjno-technicznych w celu zapewnienia bezpieczeństwa danych osobowych przetwarzanych w Ministerstwie;

3) aktualizacja i dostosowanie Polityki do wymogów wynikających z przepisów prawa;

4) prowadzenie i aktualizacja ewidencji osób upoważnionych do przetwarzania danych osobowych w Ministerstwie;

5) przygotowywanie projektów upoważnień do przetwarzania danych osobowych w Ministerstwie i przedkładanie ich Administratorowi Danych do zatwierdzenia;

6) prowadzenie i aktualizacja Wykazu zbiorów danych osobowych przetwarzanych w Ministerstwie, zawierającego wykaz budynków tworzących obszar w którym przetwarzane są dane osobowe wraz z programami zastosowanymi do ich przetwarzania.

7) prowadzenie rejestru zbiorów danych przetwarzanych przez Administratora Danych, z wyjątkiem zbiorów, o których mowa w art. 43 ust. 1 ustawy, zawierającego nazwę zbioru oraz informacje, o których mowa w art. 41 ust. 1 pkt 2-4a i 7 ustawy;

8) sprawdzania zgodności przetwarzania danych osobowych z przepisami o ochronie danych osobowych oraz opracowanie w tym zakresie sprawozdania dla Administratora Danych;

9) zapewnienie zapoznania osób upoważnionych do przetwarzania danych osobowych z przepisami o ochronie danych osobowych;

10) wykrywanie naruszeń i właściwe reagowanie w sytuacji naruszenia lub podejrzenia naruszenia zasad ochrony danych osobowych;

11) współpraca z Koordynatorami Zbiorów Danych (KZD);

12) informowanie osób uprawnionych o przysługujących im prawach oraz udzielanie informacji w zakresie ochrony danych osobowych.

§ 25. 1. ADMINISTRATOR SYSTEMU INFORMATYCZNEGO nadzoruje i kontroluje systemy informatyczne służące do przetwarzania danych osobowych oraz pełni nadzór nad ich zabezpieczeniem w oparciu o akty prawa powszechnie obowiązujące oraz procedury wewnętrzne Ministerstwa.

2. Do zadań Administratora Systemu Informatycznego należy:

1) prowadzenie bieżącej kontroli oraz dokonywanie oceny stanu bezpieczeństwa systemu informatycznego Ministerstwa oraz podejmowanie odpowiednich działań w przypadku wykrycia naruszeń w systemie zabezpieczeń;

2) prowadzenie dokumentacji dotyczącej naruszeń zabezpieczeń systemu informatycznego Ministerstwa;

3) nadzór nad wykorzystywanym w Ministerstwie oprogramowaniem pod względem jego legalności;

4) aktualizacja wykorzystywanego w Ministerstwie oprogramowania;

5) nadzór nad naprawami, konserwacją oraz likwidacją urządzeń komputerowych zawierających dane osobowe;

6) wykonywanie kopii zapasowych, ich przechowywanie oraz ich okresowe sprawdzanie pod kątem dalszej przydatności;

7) koordynowanie pracy Lokalnych Administratorów Systemu Informatycznego;

8) inicjowanie i podejmowanie przedsięwzięć w zakresie poprawy bezpieczeństwa ochrony danych osobowych w systemie informatycznym;

9) prowadzenie następujących rejestrów, związanych z funkcjonowaniem systemu informatycznego Ministerstwa:

a) rejestru kontroli stanowisk użytkowników,

b) rejestru kopii zapasowych systemów informatycznych.

§ 26. 1. DYREKTOR komórki organizacyjnej nadzoruje przestrzeganie zasad bezpieczeństwa przy przetwarzaniu danych osobowych w zbiorach danych w podległej sobie komórce organizacyjnej.

2. Dyrektor komórki organizacyjnej, na podstawie pisemnego upoważnienia do przetwarzania danych osobowych w zakresie zarządzania danymi w podległej mu komórce organizacyjnej, jest obowiązany do:

1) określania obowiązków i uprawnień pracowników w zakresie przetwarzania danych osobowych;

2) wnioskowania do Administratora Bezpieczeństwa Informacji o udzielenie, zmianę lub odwołanie upoważnienia do przetwarzania danych osobowych podległym pracownikom. Wzór wniosku o udzielenie upoważnienia stanowi załącznik nr 1 do Polityki;

3) wnioskowania do Administratora Systemu Informatycznego, (po uzyskaniu pozytywnej opinii ABI i akceptacji Dyrektora Biura Dyrektora Generalnego), o przydzielenie nowemu pracownikowi komórki organizacyjnej dostępu do obszarów roboczych i systemu informatycznego Ministerstwa, zgodnie z wzorem formularza Wniosku o nadanie/zmianę/odebranie uprawnień, stanowiącego załącznik nr 5 do Polityki;

4) informowania Administratora Systemu Informatycznego o wszelkich zmianach w zakresie danych personalnych, danych o zatrudnieniu oraz danych o dostępie do obszarów roboczych i systemu informatycznego Ministerstwa. Aktualizacji dokonuje się za pomocą formularza Wniosku o nadanie/zmianę/odebranie uprawnień, o którym mowa w pkt 3;

5) stosowania środków organizacyjnych zalecanych przez Administratora Danych w celu zapewnienia ochrony przetwarzanych danych osobowych;

6) wykonywania zaleceń Administratora Bezpieczeństwa Informacji w zakresie ochrony danych osobowych;

7) wyznaczenia spośród podległych pracowników Koordynatora Zbiorów Danych oraz nadzorowanie wykonywania przez niego zadań;

8) realizacji zadań Koordynatora Zbiorów Danych, w przypadku jego niewyznaczenia;

9) informowania Administratora Bezpieczeństwa Informacji o wyznaczeniu lub zmianie Koordynatora Zbiorów Danych w komórce;

10) sprawowania nadzoru nad obiegiem oraz przechowywaniem dokumentów i nośników, zawierających dane osobowe;

11) zgłaszania Administratorowi Bezpieczeństwa Informacji zbiorów danych osobowych przetwarzanych w komórce organizacyjnej w celu ich rejestracji przez Generalnego Inspektora Ochrony Danych Osobowych;

12) zgłaszania Administratorowi Bezpieczeństwa Informacji potrzeb szkoleniowych dla pracowników z przepisów obowiązujących w zakresie ochrony danych osobowych;

13) zgłaszania Administratorowi Bezpieczeństwa Informacji wszelkich zmian dokonywanych w przetwarzanych w komórce organizacyjnej zbiorach danych osobowych, w szczególności obejmujących rozszerzenie zakresu przetwarzanych danych;

14) zgłaszania Administratorowi Bezpieczeństwa Informacji wszelkich przypadków świadczących o naruszeniu lub możliwości naruszenia postanowień Polityki.

§ 27. KOORDYNATORZY ZBIORÓW DANYCH są obowiązani do:

1) bieżącej współpracy z Administratorem Bezpieczeństwa Informacji oraz zgłaszania potencjalnych zagrożeń w zakresie ochrony przetwarzania danych osobowych w komórce organizacyjnej;

2) prowadzenia wykazu osób upoważnionych do przetwarzania danych osobowych w komórce organizacyjnej Ministerstwa;

3) monitorowania aktualności i zakresu wydanych pracownikom Ministerstwa upoważnień do przetwarzania danych osobowych;

4) przygotowywania do podpisu dyrektora komórki organizacyjnej wniosków o wydanie lub zmianę upoważnień dla pracowników komórki do przetwarzania danych osobowych oraz przekazywania podpisanych wniosków do Administratora Bezpieczeństwa Informacji;

5) prowadzenia i aktualizacji wykazu zbiorów danych osobowych przetwarzanych w komórce organizacyjnej;

6) informowania dyrektora komórki organizacyjnej o konieczności zgłoszenia bądź aktualizacji zbiorów danych osobowych przetwarzanych w komórce organizacyjnej Generalnemu Inspektorowi Ochrony Danych Osobowych oraz wstępnego przygotowania formularza zgłoszenia.

§ 28. PRACOWNICY Ministerstwa, upoważnieni do przetwarzania danych osobowych, są obowiązani do zachowania w tajemnicy tych danych oraz sposobów ich zabezpieczenia, a także do:

1) zapoznania się oraz stosowania procedur obowiązujących w Ministerstwie w zakresie ochrony danych osobowych, w tym Polityki;

2) przetwarzania danych osobowych wyłącznie w zakresie wskazanym w upoważnieniu do przetwarzania danych osobowych i w wyznaczonych do tego celu pomieszczeniach służbowych;

3) zabezpieczania danych osobowych przed ich udostępnieniem osobom nieupoważnionym, zabraniem przez osoby nieuprawnione, przetwarzaniem z naruszeniem ustawy oraz zmianą, utratą, uszkodzeniem lub zniszczeniem;

4) udzielania informacji związanych z przetwarzaniem oraz ochroną danych osobowych Administratorowi Bezpieczeństwa Informacji;

5) bezzwłocznego zawiadamiania Administratora Bezpieczeństwa Informacji oraz dyrektora komórki organizacyjnej o wszelkich przypadkach naruszenia bezpieczeństwa danych osobowych w Ministerstwie.

§ 29. W celu uzyskania dostępu do danych osobowych przetwarzanych w Ministerstwie pracownik jest obowiązany do złożenia pisemnego oświadczenia o poufności, którego wzór stanowi załącznik nr 3 do Polityki. Oświadczenie dołącza się do akt osobowych pracownika.

Rozdział 7.
UPOWAŻNIENIA DO PRZETWARZANIA DANYCH OSOBOWYCH

§ 30. 1. Przed otrzymaniem dostępu do danych osobowych oraz rozpoczęciem ich przetwarzania należy uzyskać upoważnienie udzielone przez Administratora Danych. Wzór upoważnienia do przetwarzania danych osobowych stanowi załącznik nr 2 do Polityki.

2. W upoważnieniu zawarty jest okres jego obowiązywania oraz zakres uprawnień dostępowych.

§ 31. 1. Administrator Danych, w drodze pisemnego upoważnienia, ustanawia dyrektorów komórek organizacyjnych odpowiedzialnymi za nadzór nad prawidłowym przetwarzaniem danych osobowych w zakresie właściwych rzeczowo zbiorów danych.

2. Dyrektor komórki organizacyjnej składa do Administratora Bezpieczeństwa Informacji wniosek o udzielenie, zmianę lub odwołanie upoważnienia do przetwarzania danych osobowych.

3. Na podstawie wniosku, o którym mowa w ust. 2, Administrator Danych udziela osobie wskazanej we wniosku upoważnienia do przetwarzania danych osobowych.

§ 32. 1. Administrator Bezpieczeństwa Informacji prowadzi ewidencję upoważnień do przetwarzania danych osobowych w Ministerstwie.

2. Ewidencja upoważnień, o której mowa w ust. 1, zawiera w szczególności:

1) imię i nazwisko osoby upoważnionej;

2) stanowisko;

3) identyfikator użytkownika w systemie informatycznym;

4) datę nadania uprawnień;

5) datę ustania uprawnień;

6) zakres przydzielonych uprawnień.

3. Upoważnienia, o których mowa w ust. 1, sporządza się w dwóch egzemplarzach, z których po jednym egzemplarzu otrzymują:

1) Administrator Bezpieczeństwa Informacji;

2) osoba upoważniona.

Rozdział 8.
TECHNICZNE I ORGANIZACYJNE ŚRODKI OCHRONY DANYCH OSOBOWYCH

§ 33. Administrator Danych jest obowiązany do zastosowania środków organizacyjnych i technicznych, zapewniających bezpieczeństwo i ochronę przetwarzanych danych osobowych, bez względu na formę ich przetwarzania.

§ 34. W Ministerstwie stosuje się następujące systemy zabezpieczeń przed nieuprawnionym dostępem do danych osobowych:

1) zabezpieczenia pomieszczeń, składających się na obszar przetwarzania danych osobowych:

   a) w przypadku opuszczenia pomieszczenia, w którym przetwarza się dane osobowe, przez ostatnią osobę, pomieszczenie zamykane jest na klucz, także w godzinach pracy,

   b) po godzinach pracy klucze do pomieszczeń, w których przetwarzane są dane osobowe, przechowywane są w recepcji danego budynku,

   c) dane osobowe przechowywane w formie papierowej lub elektronicznej na nośnikach po zakończeniu pracy przechowywane są w zamykanych na klucz szafach biurowych, a tam gdzie jest to możliwe - w szafach metalowych lub pancernych. Klucze od szaf są zabezpieczane przed nieuprawnionym dostępem,

   d) nieaktualne lub błędne wydruki zawierające dane osobowe niszczone są niezwłocznie w niszczarkach,

e) budynki Ministerstwa są nadzorowane przez pracowników ochrony przez całą dobę oraz wyposażone w system alarmowy przeciwwłamaniowy,

f) uzyskanie dostępu do obszarów roboczych Ministerstwa możliwe jest jedynie za pomocą indywidualnej identyfikacyjnej karty magnetycznej,

g) dostęp do wyznaczonych pomieszczeń kontrolowany jest przez system monitoringu z zastosowaniem kamer przemysłowych;

2) zabezpieczenia zbiorów danych osobowych w formie elektronicznej przed nieautoryzowanym dostępem:

a) identyfikacja użytkownika w systemie informatycznym wymaga zastosowania uwierzytelnienia,

b) niepowtarzalne indywidualne identyfikatory dla użytkowników systemu informatycznego,

c) udostępnianie użytkownikowi programów i baz danych, zawierających dane osobowe następuje na podstawie upoważnienia do przetwarzania danych osobowych, wydanego przez Administratora Danych,

d) podłączenie urządzenia końcowego do sieci komputerowej Ministerstwa dokonywane jest przez Administratora Systemu Informatycznego lub Lokalnego Administratora Systemu Informatycznego,

e) odseparowanie wewnętrznej sieci komputerowej Ministerstwa od sieci publicznej za pomocą urządzeń typu Firewall,

f) wyposażenie wszystkich stanowisk komputerowych w indywidualną ochronę antywirusową,

g) zabezpieczenie hasłami kont na komputerach oraz używanie kont z ograniczonymi uprawnieniami do ciągłej pracy,

h) automatyczne wygaszanie ekranu i blokowanie nieużywanego komputera po upływie określonego czasu,

i) wymuszanie okresowej zmiany hasła użytkownika co 30 dni,

j) ustawienie monitorów stanowisk komputerowych używanych do przetwarzania danych osobowych w sposób uniemożliwiający wgląd w dane osobom nieupoważnionym,

k) udostępnianie kluczy i kart dostępu do serwerowni wyłącznie osobom do tego upoważnionym;

3) zabezpieczenia danych osobowych przed utratą w wyniku awarii:

a) zastosowanie zasilaczy zapasowych UPS w celu ochrony stanowisk komputerowych oraz serwerów przed skutkami zaniku zasilania,

b) cykliczne wykonywanie kopii zapasowych zgromadzonych danych, z których w przypadku awarii, odtwarzane są dane i system operacyjny,

c) zastosowanie klimatyzatorów w celu zapewnienia właściwej temperatury i wilgotności powietrza w serwerowniach,

d) rozmieszczenie gaśnic w serwerowniach;

4) stały nadzór nad systemem stosowanych zabezpieczeń:

a) pracownicy Ministerstwa są obowiązani do zwracania uwagi na prawidłowość pracy systemów informatycznych, przestrzegania wewnętrznych procedur bezpieczeństwa, informowania Administratora Bezpieczeństwa Informacji oraz przełożonych o zauważonych lub potencjalnych nieprawidłowościach,

b) przetwarzanie danych osobowych dopuszczalne jest wyłącznie na zarejestrowanych:

- stacjach roboczych,

- komputerach przenośnych,

- nośnikach.

§ 35. 1. Uszkodzone lub wycofywane elektroniczne nośniki zawierające dane osobowe podlegają fizycznemu zniszczeniu. Każdorazowo sporządzany jest protokół zniszczenia.

2. Komputery podlegające naprawie przekazywane są do punktów serwisowych po wymontowaniu dysków twardych. Każdorazowo sporządzany jest protokół naprawy.

Rozdział 9.
KONTROLA NAD PRZESTRZEGANIEM OCHRONY DANYCH OSOBOWYCH

§ 36. Schemat organizacyjny w zakresie ochrony danych osobowych w Ministerstwie stanowi załącznik nr 7 do Polityki.

§ 37. Ogólny nadzór nad przetwarzaniem danych osobowych w Ministerstwie sprawuje Administrator Danych.

§ 38. Administrator Bezpieczeństwa Informacji wykonuje bieżącą kontrolę nad przestrzeganiem wdrożonych w Ministerstwie środków bezpieczeństwa oraz postanowień wewnętrznych procedur w zakresie zasad przetwarzania danych osobowych.

§ 39. Administrator Systemu Informatycznego wykonuje bieżącą kontrolę w celu zapewnienia sprawnego działania i bezpieczeństwa systemów informatycznych Ministerstwa.

§ 40. Przy realizacji kontroli, o których mowa w § 38 i 39, Administratorowi Bezpieczeństwa Informacji oraz Administratorowi Systemu Informatycznego przysługują uprawnienia do przeprowadzania czynności kontrolnych, w szczególności do:

1) wstępu do pomieszczeń, w których zlokalizowane są zbiory danych lub przetwarzane są dane osobowe poza zbiorem danych;
2) prawo do przeprowadzenia inspekcji, oględzin urządzeń, nośników i systemów informatycznych;
3) prawo wglądu do dokumentów mających bezpośredni związek z przedmiotem kontroli i sporządzania ich kopii;
4) prawo do żądania wyjaśnień.

§ 41. 1. Administrator Bezpieczeństwa Informacji dokonuje sprawdzeń zgodności przetwarzania danych osobowych oraz opracowuje w tym zakresie sprawozdanie dla Administratora Danych.

2. Sprawozdanie, o którym mowa w ust. 1, zawiera również:

1) wnioski bieżących kontroli, o których mowa w § 38 i 39;
2) analizę zagrożeń i ryzyka w odniesieniu do procesu przetwarzania danych osobowych w Ministerstwie;
3) wnioski i zalecenia dotyczące funkcjonowania systemu ochrony danych osobowych w Ministerstwie.

Rozdział 10.
NARUSZENIA ZASAD OCHRONY DANYCH OSOBOWYCH

§ 42. Poprzez naruszenie bezpieczeństwa danych osobowych należy rozumieć każdy stwierdzony przypadek nieuprawnionego dostępu lub ujawnienia danych osobowych nieupoważnionym do tego osobom.

§ 43. Określa się następujący sposób postępowania w przypadku naruszenia zasad ochrony danych osobowych:

1) w momencie stwierdzenia naruszenia lub próby naruszenia zasad ochrony danych osobowych, należy niezwłocznie powiadomić o tym fakcie Administratora Bezpieczeństwa Informacji oraz Dyrektora komórki organizacyjnej;
2) jeśli taka możliwość istnieje, należy podjąć czynności zmierzające do zmniejszenia skutków zaistniałego naruszenia zasad ochrony danych osobowych;
3) jeśli mogłoby to przyczynić się do utrudnienia wyjaśnienia okoliczności zdarzenia, należy powstrzymać się od bieżącej pracy, w celu zabezpieczenia miejsca zdarzenia;
4) nie opuszczać, bez uzasadnionej potrzeby, miejsca zdarzenia do czasu przybycia Administratora Bezpieczeństwa Informacji;

5) w przypadku braku możliwości zawiadomienia Administratora Bezpieczeństwa Informacji lub Dyrektora komórki organizacyjnej, należy wstępnie udokumentować zaistniałe naruszenie zasad ochrony danych osobowych;

6) jeśli naruszeniu lub próbie naruszenia uległy dane w systemie informatycznym, dodatkowo powiadamiany jest Administrator Systemu Informatycznego;

7) Administrator Bezpieczeństwa Informacji oraz, w przypadku naruszenia danych osobowych w systemie informatycznym, Administrator Systemu Informatycznego, po przyjęciu zawiadomienia dokumentują zaistniały przypadek naruszenia zasad ochrony danych osobowych oraz podejmują działania w celu wyjaśnienia sytuacji oraz usunięcia naruszenia, w szczególności:

   a) dokonują szczegółowej analizy zaistniałej sytuacji, w celu potwierdzenia lub wykluczenia faktu naruszenia zasad ochrony danych osobowych,

   b) podejmują odpowiednie kroki w celu powstrzymania lub ograniczenia dostępu osoby nieupoważnionej, zminimalizowania szkód i zabezpieczenia przed usunięciem śladów naruszenia zasad ochrony danych,

   c) podejmują decyzję o celowości i potrzebie powiadomienia o naruszeniu zasad ochrony danych osobowych Administratora Danych,

   d) w przypadku potwierdzenia naruszenia zasad ochrony danych osobowych, dokonują identyfikacji rodzaju zaistniałego zdarzenia,

   e) podejmują działania w celu przywrócenia prawidłowego stanu, przy czym, jeżeli nastąpiło uszkodzenie bazy danych, odtworzenia jej z ostatniej kopii awaryjnej z zachowaniem wszelkich środków ostrożności mających na celu uniknięcie ponownego uzyskania dostępu przez osobę nieupoważnioną;

8) przy wyjaśnianiu okoliczności naruszania zasad ochrony danych osobowych Administrator Bezpieczeństwa Informacji oraz Administrator Systemu Informatycznego mają prawo do:

   a) żądania wyjaśnień,

   b) nakazania przerwy w pracy w zakresie przetwarzania danych osobowych,

   c) czasowego zablokowania uprawnień wskazanym użytkownikom lub wszystkim użytkownikom;

9) odmowa wyjaśnień lub współpracy z Administratorem Bezpieczeństwa Informacji oraz z Administratorem Systemu Informatycznego, przy wyjaśnianiu okoliczności naruszenia zasad ochrony danych osobowych, będzie traktowana jako naruszenie obowiązków pracowniczych.

§ 44. 1. Z przeprowadzonego postępowania Administrator Bezpieczeństwa Informacji, przy udziale Administratora Systemu Informatycznego w przypadku naruszenia zabezpieczenia danych osobowych w systemie informatycznym, sporządza raport dla Administratora Danych.

2. Raport powinien zawierać w szczególności: wskazanie osoby lub osób powiadamiających o naruszeniu lub możliwości naruszenia bezpieczeństwa oraz innych osób związanych ze zdarzeniem, okoliczności zdarzenia, rodzaj naruszenia, opis podjętych działań oraz ocenę przyczyn wystąpienia naruszenia, a także propozycje przedsięwzięć mających na celu naprawę powstałych szkód i zapobiegnięcie podobnym zdarzeniom w przyszłości.

3. Wobec pracowników, którzy dopuścili się naruszenia zasad ochrony danych osobowych lub zabezpieczeń systemu informatycznego stosuje się odpowiednie przepisy ustawy oraz Regulaminu pracy Ministerstwa, w zakresie odpowiedzialności dyscyplinarnej i porządkowej pracowników.

Rozdział 11.
POSTANOWIENIA KOŃCOWE

§ 45. Do spraw nieuregulowanych w Polityce, w zakresie ochrony danych osobowych stosuje się przepisy ustawy, rozporządzeń oraz innych regulacji wewnętrznych.

§ 46. Wszystkie rejestry, ewidencje, wykazy, o których mowa w Polityce objęte są nakazem zachowania w tajemnicy.

Załącznik nr 1
do Polityki Ochrony Danych Osobowych
w Ministerstwie Sportu i Turystyki

Warszawa, dnia ……r.

……
(pieczątka/nagłówek komórki organizacyjnej)

W N I O S E K

o udzielenie/zmianę/odwołanie upoważnienia do przetwarzania danych osobowych

Na podstawie art. 37 ustawy z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (Dz. U. z 2016 r. poz. 922) oraz § 31 ust. 2 Polityki Ochrony Danych Osobowych w Ministerstwie Sportu i Turystyki stanowiącej załącznik do zarządzenia nr … Ministra Sportu i Turystyki z dnia …….. w sprawie wprowadzenia Polityki ochrony danych osobowych w Ministerstwie Sportu i Turystyki, proszę o:

☐ - udzielenie ☐ - zmianę ☐ - odwołanie

upoważnienia

dla **Pani/Pana** ……
(imię i nazwisko)

……
(stanowisko, komórka organizacyjna)

do wykonywania czynności związanych z przetwarzaniem danych osobowych w następujący sposób:

☐ - w kartotekach, skorowidzach, księgach, wykazach i innych zbiorach ewidencyjnych (wymienić):
……
……

☐ - w systemie informatycznym:
……
(pełna nazwa systemu/ów informatycznym/ych lub zbioru/ów danych)

w zakresie:
……
……
……
(wymienić rodzaj danych osobowych)

na okres:

☐ - od dnia……..…… do dnia……..…… ☐ - bezterminowo

……
(podpis i pieczątka Dyrektora komórki organizacyjnej)

Załącznik nr 2
do Polityki Ochrony Danych Osobowych
w Ministerstwie Sportu i Turystyki

Warszawa, dnia r.

MINISTER
SPORTU I TURYSTYKI

UPOWAŻNIENIE NR...

Na podstawie art. 37 ustawy z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (Dz. U. z 2016 r. poz. 922), upoważniam

Panią/Pana ..... ……
(imię i nazwisko)

……
(stanowisko, komórka organizacyjna**)**

do przetwarzania danych osobowych w następujących zbiorach danych*:
……
……
w zakresie
……
……
(wymienić rodzaj danych osobowych)

na okres.....

Upoważnienie niniejsze nie upoważnia do udzielania dalszych upoważnień i wygasa z dniem ustania Pani/Pana stosunku pracy, a ponadto może być w każdym czasie zmienione lub odwołane.

……
(podpis i pieczęć Administratora Danych)

Zgodnie z art. 39 ust. 2 ustawy o ochronie danych osobowych zobowiązuję się do zachowania w tajemnicy treści przetwarzanych danych osobowych oraz sposobów ich zabezpieczania w okresie trwania stosunku pracy, jak i po jego ustaniu.

Przyjmuję do realizacji
powierzone mi obowiązki i uprawnienia

……..
(data i podpis upoważnionego)

*podać sposób przetwarzania danych np. w systemie informatycznym lub/także w kartotekach, skorowidzach, księgach, wykazach i innych zbiorach ewidencyjnych (wymienić)

Załącznik nr 3
do Polityki Ochrony Danych Osobowych
w Ministerstwie Sportu i Turystyki

……..
Imię i Nazwisko

……..
Stanowisko

…….
Nazwa komórki organizacyjnej

Oświadczenie o poufności

Ja, niżej podpisana/y, oświadczam, że **zobowiązuję** się do:

1. zachowania w tajemnicy danych osobowych, w tym wiedzy w zakresie sposobów ich zabezpieczenia w Ministerstwie Sportu i Turystyki, w okresie trwania stosunku pracy, jak i po jego ustaniu,
2. przestrzegania zasad zabezpieczania i ochrony danych osobowych przetwarzanych przeze mnie w Ministerstwie Sportu i Turystyki, w tym do ochrony danych osobowych przed dostępem osób nieupoważnionych, zabraniem, uszkodzeniem oraz nieuzasadnioną modyfikacją lub zniszczeniem,
3. przetwarzania danych osobowych w Ministerstwie Sportu i Turystyki wyłącznie w zakresie wskazanym w udzielonym mi upoważnieniu do przetwarzania danych,
4. zgłaszania dyrektorowi komórki organizacyjnej i Administratorowi Bezpieczeństwa Informacji w Ministerstwie Sportu i Turystyki wszelkich podejrzeń lub faktycznych prób naruszenia bezpieczeństwa danych osobowych przetwarzanych w systemach informatycznych lub każdej innej formie.

Jednocześnie **oświadczam**, że zapoznałam/em się z treścią obowiązujących przepisów prawa w zakresie przetwarzania oraz ochrony danych osobowych, w szczególności z postanowieniami ustawy z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (Dz. U. z 2016 r. poz. 922) i zasadami ochrony danych osobowych określonych w zarządzeniu nr … Ministra Sportu i Turystyki z dnia …….. w sprawie wprowadzenia Polityki ochrony danych osobowych w Ministerstwie Sportu i Turystyki i **zobowiązuję** się do ich przestrzegania.

Oświadczam, że znana jest mi odpowiedzialność za naruszenie podstawowych obowiązków pracowniczych w zakresie wskazanym powyżej oraz mam świadomość, iż postępowanie sprzeczne z powyższymi zobowiązaniami, może być uznane za naruszenie przepisów określonych w ustawie o ochronie danych osobowych oraz stanowi naruszenie obowiązków pracowniczych.

…….....
podpis pracownika

……
miejscowość i data

Załącznik nr 4
do Polityki Ochrony Danych Osobowych
w Ministerstwie Sportu i Turystyki

……..
Imię i Nazwisko

Umowa Nr……z dnia……

Oświadczenie o poufności

Ja, niżej podpisana/y, oświadczam, że **zobowiązuję** się do:

1. zachowania w tajemnicy danych osobowych, w tym wiedzy w zakresie sposobów ich zabezpieczenia w Ministerstwie Sportu i Turystyki, w trakcie współpracy z Ministerstwem Sportu i Turystyki, jak i po jej ustaniu,
2. przestrzegania zasad zabezpieczania i ochrony danych osobowych przetwarzanych przeze mnie w trakcie współpracy z Ministerstwem Sportu i Turystyki, w tym do ochrony danych osobowych przed dostępem osób nieupoważnionych, zabraniem, uszkodzeniem oraz nieuzasadnioną modyfikacją lub zniszczeniem,
3. przetwarzania danych osobowych w trakcie współpracy z Ministerstwem Sportu i Turystyki wyłącznie w zakresie wskazanym w udzielonym mi upoważnieniu do przetwarzania danych,
4. zgłaszania osobie nadzorującej wykonanie umowy i Administratorowi Bezpieczeństwa Informacji w Ministerstwie Sportu i Turystyki wszelkich podejrzeń lub faktycznych prób naruszenia bezpieczeństwa danych osobowych przetwarzanych w systemach informatycznych lub każdej innej formie.

Jednocześnie **oświadczam**, że zapoznałam/em się z treścią obowiązujących przepisów prawa w zakresie przetwarzania oraz ochrony danych osobowych, w szczególności z postanowieniami ustawy z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (Dz. U. z 2016 r. poz. 922) i zasadami ochrony danych osobowych określonych w zarządzeniu nr … Ministra Sportu i Turystyki z dnia …….. w sprawie wprowadzenia Polityki ochrony danych osobowych w Ministerstwie Sportu i Turystyki i **zobowiązuję** się do ich przestrzegania.

Oświadczam, że znana jest mi odpowiedzialność za naruszenie obowiązków w zakresie wskazanym powyżej oraz mam świadomość, iż postępowanie sprzeczne z powyższymi zobowiązaniami, może być uznane za naruszenie przepisów określonych w ustawie o ochronie danych osobowych oraz stanowi naruszenie wewnętrznych regulacji Administratora Danych.

…….....
podpis składającego oświadczenie

……
miejscowość i data

Załącznik nr 5
do Polityki Ochrony Danych Osobowych
w Ministerstwie Sportu i Turystyki

Warszawa, dnia ……r.

Wniosek o nadanie/zmianę/odebranie uprawnień

☐ nadanie uprawnień ☐ modyfikacja uprawnień (wypełnić części A,B,C,D) ☐ odebranie uprawnień (wypełnić części A,B,E)

CZĘŚĆ A: DANE PERSONALNE

Jeżeli zmianie uległo nazwisko osoby, należy wpisać dotychczasowe (pole 2a) i nowe (pole 2b)

1	Imię				
2	Nazwisko	a		b	

CZĘŚĆ B: DANE O ZATRUDNIENIU (innej podstawie wykonywania zadań)

1	Stanowisko			
2	Budynek/Pokój/nr tel.			
3	Departament/Biuro		Wydział/Zespół:	

☐ dane o zatrudnieniu bez zmian (w przypadku zaznaczenia, nie należy uzupełniać danych poniżej)

4. Podstawa wykonywania zadań:	☐ stosunek pracy	☐ umowa cywilnoprawna	☐ praktyka/staż/wolontariat
5. Rodzaj umowy:	☐ na czas określony	☐ na czas nieokreślony	
6. Okres zatrudnienia/czas trwania umowy cywilnoprawnej, praktyki, stażu, wolontariatu:			
Od:		Do:	

CZĘŚĆ C: DANE O SYSTEMACH KONTROLI DOSTĘPU

☐ dane o zatrudnieniu bez zmian (w przypadku zaznaczenia, nie należy uzupełniać danych poniżej)

1. Lokalizacja:	☐ ul. Senatorska 12	☐ ul. Senatorska 14	
2. Zakres dostępu:	☐ pełny	☐ z wył. sekretariatu ministra	☐ niestandardowy
3. Czas dostępu:	☐ pn-pt: 7.00-19.00	☐ pn-nd: 7.00-19.00	☐ pn-nd: 24 godziny

4. Opis/uzasadnienie nadania dostępu:

CZĘŚĆ D: DANE O DOSTĘPIE DO SYSTEMU INFORMATYCZNEGO

☐ dane o zatrudnieniu bez zmian (w przypadku zaznaczenia, nie należy uzupełniać danych poniżej)

1. komputer:	☐ konto osobiste	☐ EIK
2. ESOD:	☐ konto osobiste ☐ zastępstwo pomiędzy komórkami – za: …… na okres: ……	
3. Poczta e-mail:	☐ osobista ☐ przypisanie do grupy: ……	
4. Dostęp do aplikacji (wypisać niezbędne aplikacje): ……		

Część E: Odebranie Uprawnień

W przypadku odebrania uprawnień wniosek podpisuje tylko osoba w pkt. 1 i 4

	odebrania uprawnień	☐ wszystkie ☐ wybrane (wpisać jakie):……..

1. Wnioskuję

……
Podpis Dyrektora komórki wnioskującej

2. Oświadczam, iż ww. osoba posiada upoważnienie do przetwarzania danych osobowych w zakresie wnioskowanych uprawnień dostępowych

……
Podpis Administratora Bezpieczeństwa Informacji

3. Wyrażam zgodę / Nie wyrażam zgody

……
Akceptacja Dyrektora Biura Dyrektora Generalnego

4. Potwierdzam

……
Podpis ASI/LASI

Wzór

Załącznik nr 6
do Polityki Ochrony Danych Osobowych
w Ministerstwie Sportu i Turystyki

Warszawa, dnia ……..

Wykaz zbiorów danych osobowych przetwarzanych w MSiT, zawierający wykaz budynków, tworzących obszar w którym przetwarzane są dane osobowe wraz z programami zastosowanymi do ich przetwarzania

prowadzony na podstawie ustawy z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (Dz. U. z 2016 r. poz. 922)
zgodnie z § 4 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. poz. 1024)

Lp.	Nazwa zbioru/ podzbioru	Przesłanka	Podstawa prawna	Cel przetwarzania danych	Opis kategorii osób, których dane dotyczą	Zakres przetwarzania danych	Przepływ danych	Forma zbioru System/program	Miejsce przetwarzania danych (komórka organizacyjna)	Adresy budynków
(1)	(2)	(3)	(4)	(5)	(6)	(7)	(8)	(9)	(10)	(11)
1.										
2.										
3.										

Załącznik nr 7
do Polityki Ochrony Danych Osobowych
w Ministerstwie Sportu i Turystyki

SCHEMAT ORGANIZACYJNY W ZAKRESIE OCHRONY DANYCH OSOBOWYCH W MSIT