Warszawa, dnia 9 lipca 2013 r.

Poz. 21

ZARZĄDZENIE NR 20
MINISTRA SPORTU I TURYSTYKI[1)]

z dnia 9 lipca 2013 r.

w sprawie ustalenia zasad bezpieczeństwa informacji 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 2002 r. Nr 101, poz. 926, z późn. zm.[2)]) 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. Nr 100, poz. 1024) zarządza się, co następuje:

§ 1. Ustala się zasady ochrony danych osobowych przetwarzanych w Ministerstwie Sportu i Turystyki, obejmujące:

1) Politykę bezpieczeństwa informacji – stanowiącą załącznik nr 1 do zarządzenia;

2) Instrukcję zarządzania systemem informatycznym – stanowiącą załącznik nr 2 do zarządzenia.

§ 2. Traci moc zarządzenie nr 9 Ministra Sportu i Turystyki z dnia 27 stycznia 2009 r. w sprawie wprowadzenia Instrukcji ochrony danych osobowych, zmienione zarządzeniem nr 28 Ministra Sportu i Turystyki z dnia 25 sierpnia 2009 r. oraz zarządzeniem nr 8 Ministra Sportu i Turystyki z dnia 16 lipca 2012 r.

§ 3. Zarządzenie wchodzi w życie z dniem podpisania.

Minister Sportu i Turystyki

Joanna Mucha

[1)] Minister Sportu i Turystyki kieruje działami administracji rządowej - kultura fizyczna i turystyka na podstawie § 1 ust. 2 rozporządzenia Prezesa Rady Ministrów z dnia 18 listopada 2011 r. w sprawie szczegółowego zakresu działania Ministra Sportu i Turystyki (Dz. U. Nr 248, poz. 1489, oraz z 2013 r. poz. 606).

[2)] Zmiany tekstu jednolitego wymienionej ustawy zostały ogłoszone w Dz. U. z 2002 r. Nr 153, poz. 1271, z 2004 r. Nr 25, poz. 219 i Nr 33, poz. 285, z 2006 r. Nr 104, poz. 708 i 711, z 2007 r. Nr 165, poz. 1170 i Nr 176, poz. 1238, z 2010 r. Nr 41, poz. 233, Nr 182, poz. 1228 i Nr 229, poz. 1497 oraz z 2011 r. Nr 230, poz. 1371.

Załącznik Nr 1 do Zarządzenia Nr 20

Ministra Sportu i Turystyki

z dnia 9 lipca 2013 r.

POLITYKA BEZPIECZEŃSTWA INFORMACJI

Rozdział 1. POSTANOWIENIA OGÓLNE

§ 1. 1. Polityka bezpieczeństwa informacji stanowi zestaw praw i reguł określających sposób zarządzania, ochrony i przetwarzania informacji w Ministerstwie.

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

1) w systemach informatycznych, także w przypadku przetwarzania danych poza zbiorem danych osobowych;

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

3. Ochrona danych osobowych obowiązuje wszystkich pracowników Ministerstwa, którzy mają dostęp do informacji przetwarzanych w Ministerstwie, bez względu na zajmowane stanowisko, miejsce wykonywania pracy, jak również rodzaj stosunku pracy.

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 bezpieczeństwa informacji Ministerstwa 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 przez wszystkich pracowników.

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/biuro, którego zadania określone zostały w Regulaminie organizacyjnym Ministerstwa Sportu i Turystyki, stanowiącym załącznik do zarządzenia nr 3 Ministra Sportu i Turystyki z dnia 11 lutego 2013 r. w sprawie ustalenia Regulaminu organizacyjnego Ministerstwa Sportu i Turystyki (Dz. Urz. Min. Spor. poz. 3);

3) **Regulamin organizacyjny** – regulamin, o którym mowa w pkt 2;

4) **Regulamin pracy** – Regulamin pracy Ministerstwa Sportu i Turystyki, stanowiący załącznik do zarządzenia nr 5 Dyrektora Generalnego z dnia 26 lipca 2012 r. w sprawie ustalenia Regulaminu pracy w Ministerstwie Sportu i Turystyki;

5) **Polityka** – Polityka bezpieczeństwa informacji obowiązująca w Ministerstwie;

6) **Instrukcja –** Instrukcja zarządzania systemem informatycznym Ministerstwa;

7) **ustawa –** ustawa z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (Dz. U. z 2002 r. Nr 101, poz. 926, z późn. zm.);

8) **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. Nr 100, poz. 1024);

9) **Administrator Danych (AD)** – Minister Sportu i Turystyki;

10) **Pełnomocnik ds. ochrony danych osobowych –** pracownik Ministerstwa, któremu Administrator Danych na podstawie pisemnego upoważnienia może powierzyć realizację zadań wynikających z ustawy o ochronie danych osobowych;

11) **Administrator Bezpieczeństwa Informacji (ABI)** – pracownik Ministerstwa wyznaczony przez Administratora Danych, nadzorujący i kontrolujący przestrzeganie zasad ochrony danych osobowych w Ministerstwie;

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

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

14) **Koordynator Zbiorów Danych (KZD)** – pracownik wyznaczony przez dyrektora komórki organizacyjnej w Ministerstwie do prowadzenia ogółu spraw z zakresu ochrony danych osobowych w komórce organizacyjnej;

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

16) **dane osobowe** – wszelkie informacje dotyczące zidentyfikowanej lub możliwej do zidentyfikowania osoby fizycznej; 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;

17) **naruszenie zabezpieczenia** – jakiekolwiek naruszenie bezpieczeństwa, niezawodności, integralności lub poufności informacji;

18) **dostępność informacji** – zapewnienie, że podmioty uprawnione uzyskują dostęp do informacji tylko w uzasadnionych przypadkach;

19) **nośnik –** dyskietki, płyty CD lub DVD, pamięć flash, dyski twarde, taśmy magnetyczne lub inne urządzenia/materiały służące do przechowywania plików z danymi;

20) **zniszczenie nośnika** – trwałe i nieodwracalne fizyczne zniszczenie nośnika uniemożliwiające rekonstrukcję i odzyskanie danych;

21) **Generalny Inspektor Ochrony Danych Osobowych (GIODO) –** organ do spraw ochrony danych osobowych działający na podstawie ustawy;

22) **pracownik –** osoba, która świadczy pracę na rzecz Ministerstwa, bez względu na jakiej podstawie (w tym umowa zlecenia, staż, praktyki);

23) **użytkownik –** osoba przetwarzająca dane, w tym dane osobowe, w systemie informatycznym, w ramach wykonywanych zadań, niezależnie od charakteru zatrudnienia lub wykonywanych prac zleconych.

Rozdział 2.
CEL I ZAKRES STOSOWANIA

§ 3. 1. Celem Polityki jest określenie postępowania gwarantującego bezpieczeństwo informacji przetwarzanych w Ministerstwie, w tym zabezpieczenie przetwarzanych przez Ministerstwo danych osobowych, poprzez podejmowanie działań mających na celu zapewnienie ich poufności, integralności, dostępności i rozliczalności.

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 położone w Warszawie przy ul. Senatorskiej 12 i 14.

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. Szczegółowy wykaz budynków, tworzących obszar, w którym przetwarzane są dane osobowe wraz z programami zastosowanymi do ich przetwarzania zawarte są w dokumencie *Wykaz zbiorów danych osobowych przetwarzanych w Ministerstwie Sportu i Turystyki*, stworzonym według wzoru stanowiącego załącznik nr 7 do Polityki.

2. Wykaz o którym mowa w ust. 1 znajduje się u Administratora Bezpieczeństwa Informacji (ABI).

3. 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. Czynności Administratora Danych (AD) wynikające z ustawy może pełnić upoważniony przez Administratora Danych, Pełnomocnik ds. Ochrony Danych Osobowych.

2. W celu nadzoru nad przestrzeganiem zasad ochrony danych osobowych w Ministerstwie, Administrator Danych (AD) wyznacza Administratora Bezpieczeństwa Informacji (ABI).

3. W celu nadzoru nad systemem informatycznym Ministerstwa, Administrator Danych (AD) wyznacza Administratora Systemu Informatycznego (ASI).

§ 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 (AD);

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 (AD);

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 (ABI) 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 (ABI) 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 (AD).

2. Pracownik Ministerstwa, przed dopuszczeniem go do przetwarzania danych osobowych, jest zobowiązany 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 (ABI), na podstawie pisemnego upoważnienia wydanego przez Administratora Danych (AD) oraz podpisaniu przez taką osobę oświadczenia o poufności. Wzór oświadczenia stanowi załącznik nr 6 do Polityki.

Rozdział 5.
DOSTĘP PODMIOTÓW ZEWNĘTRZNYCH

§ 19. Celem procedury jest zapewnienie bezpieczeństwa 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 (ABI) oraz zgody Administratora Danych (AD).

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 (ABI) oraz zgody Administratora Danych (AD).

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

§ 22. 1. Administrator Bezpieczeństwa Informacji (ABI) prowadzi Rejestr podmiotów zewnętrznych , którym powierzono przetwarzanie danych osobowych.

2. Administrator Bezpieczeństwa Informacji (ABI) prowadzi Rejestr podmiotów zewnętrznych, którym udostępniono dane osobowe.

§ 23. 1. Rejestry, o których mowa w § 22 zawierają:

1) datę powierzenia/udostępnienia informacji;

2) adresata powierzonych/udostępnionych danych;

3) zakres powierzonych/udostępnionych danych.

2. Ewidencjonowanie następuje bezpośrednio po powierzeniu lub udostępnieniu danych osobowych.

§ 24. 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

§ 25. 1. ADMINISTRATOR DANYCH (AD) jest zobowiązany 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 (AD) należy:

1) zatwierdzanie procedur regulujących postępowanie przy przetwarzaniu danych osobowych w Ministerstwie;

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

3) wyznaczenie Administratora Bezpieczeństwa Informacji (ABI);

4) wyznaczenie Administratora Systemu Informatycznego (ASI);

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

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

7) parafowaniu projektów umów w zakresie powierzania przetwarzania danych osobowych podmiotom zewnętrznym;

8) inicjowaniu szkoleń pracowników Ministerstwa z obowiązujących przepisów w zakresie ochrony danych osobowych.

3. Zadania, o których mowa w ust. 2, może wykonywać, na podstawie pisemnego upoważnienia, Pełnomocnik ds. ochrony danych osobowych. Wzór upoważnienia stanowi załącznik nr 1 do Polityki.

§ 26. 1. ADMINISTRATOR BEZPIECZEŃSTWA INFORMACJI (ABI) wdraża i nadzoruje przestrzeganie zasad ochrony danych osobowych w Ministerstwie.

2. Do zadań Administratora Bezpieczeństwa Informacji (ABI) należy:

1) współdziałanie z Administratorem Danych (AD) 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 i Instrukcji 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 (AD) do zatwierdzenia;

6) prowadzenie i aktualizacja wykazu zbiorów danych osobowych Ministerstwa, oprogramowania używanego do ich przetwarzania oraz budynków, tworzących obszar, w obrębie którego przetwarzane są dane osobowe, zawartych w *Wykazie zbiorów danych osobowych przetwarzanych w Ministerstwie Sportu i Turystyki*;

7) prowadzenie rejestrów, o których mowa w § 22 Polityki;

8) prowadzenie rejestru stwierdzonych naruszeń, którego wzór stanowi załącznik nr 8 do Polityki;

9) identyfikacja zagrożeń i analiza ryzyka, w odniesieniu do procesu przetwarzania danych osobowych w Ministerstwie oraz informowanie o wynikach analizy Administratora Danych (AD);

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;

13) przeprowadzanie audytu systemu ochrony danych osobowych oraz informowanie o wynikach audytu Administratora Danych (AD) oraz Dyrektora Generalnego Ministerstwa, w formie pisemnego sprawozdania.

§ 27. 1. ADMINISTRATOR SYSTEMU INFORMATYCZNEGO (ASI) zarządza systemami informatycznymi służącymi do przetwarzania danych osobowych oraz pełni nadzór nad ich zabezpieczeniem;

2. Do zadań Administratora Systemu Informatycznego (ASI) 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 Administratorów Systemu;

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,

   c) rejestru kontroli stanu zabezpieczenia systemów informatycznych, rejestru zmiany haseł administracyjnych.

§ 28. 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 zobowiązany do:

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

2) wnioskowania do Administratora Bezpieczeństwa Informacji (ABI) o udzielenie, nadanie, zmianę lub odwołanie upoważnienia do przetwarzania danych osobowych podległym pracownikom. Wzór wniosku o udzielenie upoważnienia stanowi załącznik nr 4 do Polityki;

3) wnioskowania do Administratora Systemu Informatycznego (ASI), po akceptacji Dyrektora Biura Administracyjnego, o przydzielenie nowemu pracownikowi komórki organizacyjnej dostępu do obszarów roboczych i systemu informatycznego Ministerstwa. Zgłoszenia dokonuje się za pomocą formularza informacyjnego, którego wzór stanowi załącznik nr 9 do Polityki;

4) informowania Administratora Systemu Informatycznego (ASI) 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 informacyjnego, o którym mowa w pkt 3;

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

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

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

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

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

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

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

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

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

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

§ 29. KOORDYNATORZY ZBIORÓW DANYCH (KZD) są zobowiązani do:

1) bieżącej współpracy z Administratorem Bezpieczeństwa Informacji (ABI) 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;

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

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

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 (GIODO) oraz wstępnego przygotowania formularza zgłoszenia;

§ 30. PRACOWNICY Ministerstwa, upoważnieni do przetwarzania danych osobowych, są zobowiązani 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 i Instrukcji;

2) przetwarzania danych osobowych wyłącznie w zakresie wskazanym w upoważnieniu do przetwarzania danych 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 (ABI);

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

§ 31. W celu uzyskania dostępu do danych osobowych przetwarzanych w Ministerstwie pracownik jest zobowiązany do złożenia pisemnego oświadczenia o poufności, którego wzór stanowi załącznik nr 6 do Polityki. Oświadczenie dołącza się do akt osobowych pracownika.

Rozdział 7.
UPOWAŻNIENIA DO PRZETWARZANIA DANYCH OSOBOWYCH

§ 32. 1. Przed otrzymaniem dostępu do danych osobowych oraz rozpoczęciem ich przetwarzania należy uzyskać stosowne upoważnienie wydane przez Administratora Danych (AD).

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

§ 33. 1. Administrator Danych (AD) 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 (ABI) wniosek o nadanie, zmianę lub cofnięcie upoważnienia do przetwarzania danych osobowych.

3. Na podstawie wniosku, o którym mowa w ust. 2, Administrator Danych (AD) nadaje osobie upoważnienie do przetwarzania danych osobowych.

§ 34. 1. Administrator Bezpieczeństwa Informacji (ABI) prowadzi ewidencję pracowników posiadających upoważnienia do przetwarzania danych osobowych w Ministerstwie.

2. Rejestr upoważnień, o którym mowa w ust. 1, zawiera:

1) imię i nazwisko pracownika;

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 (ABI);

2) upoważniony pracownik.

4. Potwierdzone za zgodność z oryginałem kopie upoważnień, o których mowa w ust. 1, przekazywane są przez Administratora Bezpieczeństwa Informacji (ABI) do komórki kadrowej Ministerstwa, celem dołączenia do akt osobowych pracowników.

Rozdział 8.
TECHNICZNE I ORGANIZACYJNE ŚRODKI OCHRONY DANYCH OSOBOWYCH

§ 35. Administrator Danych (AD) jest zobowiązany do zastosowania środków organizacyjnych i technicznych, zapewniających bezpieczeństwo i ochronę przetwarzanych danych osobowych, bez względu na formę ich przetwarzania.

§ 36. 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 pojemnikach deponowanych we właściwej recepcji;

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, o których mowa w § 4, nadzorowane są przez pracowników ochrony przez całą dobę; budynki wyposażone są 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 (AD);

d) podłączenie urządzenia końcowego do sieci komputerowej Ministerstwa dokonywane jest przez Administratora Systemu Informatycznego (ASI) lub Administratora Systemu;

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 zobowiązani do zwracania uwagi na prawidłowość pracy systemów informatycznych, przestrzegania wewnętrznych procedur bezpieczeństwa, informowania Administratora Bezpieczeństwa Informacji (ABI) oraz przełożonych o zauważonych lub potencjalnych nieprawidłowościach;

b) przetwarzanie danych dopuszczalne jest wyłącznie na zarejestrowanych stacjach roboczych, komputerach przenośnych oraz innych nośnikach informacji;

c) Administrator Bezpieczeństwa Informacji (ABI) przeprowadza audyt, o którym mowa w § 26 ust. 2 pkt 13.

§ 37. 1. Uszkodzone lub wycofywane elektroniczne nośniki danych 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

§ 38. Schemat organizacyjny w zakresie ochrony danych osobowych w Ministerstwie stanowi załącznik nr 10 do Polityki.

§ 39. Ogólny nadzór nad przetwarzaniem danych osobowych w Ministerstwie sprawuje Administrator Danych (AD).

§ 40. Administrator Bezpieczeństwa Informacji (ABI) wykonuje bieżącą kontrolę nad przestrzeganiem przez pracowników, wdrożonych w Ministerstwie środków bezpieczeństwa oraz postanowień wewnętrznych procedur w zakresie zasad przetwarzania danych osobowych.

§ 41. Administrator Systemu Informatycznego (ASI) wykonuje bieżącą kontrolę w celu zapewnienia sprawnego działania i bezpieczeństwa systemów informatycznych Ministerstwa.

§ 42. Przy realizacji kontroli, o których mowa w § 40 i 41 Administratorowi Bezpieczeństwa Informacji (ABI) oraz Administratorowi Systemu Informatycznego (ASI) 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.

§ 43. 1. Audyt w zakresie przestrzegania ochrony danych osobowych w Ministerstwie, o którym mowa w § 26 ust. 2 pkt 13 sporządzany jest za poprzedni rok kalendarzowy.

2. Administrator Bezpieczeństwa Informacji (ABI) do końca pierwszego kwartału każdego roku, sporządza sprawozdanie z audytu o którym mowa w ust 1.

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

1) wnioski bieżących kontroli, o których mowa w § 40 i 41;

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.

4. Sprawozdanie, o którym mowa w ust. 2, Administrator Bezpieczeństwa Informacji (ABI) przedkłada Administratorowi Danych (AD).

Rozdział 10.
NARUSZENIA ZASAD OCHRONY DANYCH OSOBOWYCH

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

2. Określa się tryb postępowania w przypadku:

1) naruszeń bezpieczeństwa danych osobowych.

2) naruszeń zabezpieczenia systemu informatycznego, w tym: stanu urządzeń, zawartości zbioru danych osobowych, ujawnienia sposobu działania programu lub jakości komunikacji w sieci teleinformatycznej, mogących wskazywać na naruszenie zabezpieczeń tych danych.

3. Każdy pracownik Ministerstwa, posiadający upoważnienie do przetwarzania danych osobowych, jest odpowiedzialny za bezpieczeństwo tych danych.

4. Nadzór nad przestrzeganiem instrukcji postępowania w sytuacji naruszenia zasad ochrony danych osobowych sprawuje Administrator Bezpieczeństwa Informacji (ABI).

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

1) każdy pracownik w momencie stwierdzenia naruszenia lub próby naruszenia bezpieczeństwa danych, obowiązany jest do niezwłocznego zawiadomienia o tym fakcie Administratora Bezpieczeństwa Informacji (ABI) oraz Dyrektora komórki organizacyjnej;

2) w przypadku braku możliwości zawiadomienia Administratora Bezpieczeństwa Informacji (ABI)) lub Dyrektora komórki organizacyjnej, należy:

   a) jeśli taka możliwość istnieje, podjąć czynności zmierzające do zmniejszenia skutków zaistniałego naruszenia bezpieczeństwa,

   b) jeśli mogłoby to przyczynić się do utrudnienia wyjaśnienia okoliczności zdarzenia, powstrzymać się od bieżącej pracy, w celu zabezpieczenia miejsca zdarzenia,

   c) wstępnie udokumentować zaistniałe naruszenie bezpieczeństwa,

   d) nie opuszczać, bez uzasadnionej potrzeby, miejsca zdarzenia do czasu przybycia Administratora Bezpieczeństwa Informacji (ABI);

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

4) Administrator Bezpieczeństwa Informacji (ABI) oraz, w przypadku naruszenia danych w systemie informatycznym, Administrator Systemu Informatycznego (ASI), po przyjęciu zawiadomienia dokumentują zaistniały przypadek naruszenia bezpieczeństwa danych 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 ochrony danych osobowych,

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

   c) podejmują decyzję o celowości i potrzebie powiadomienia o naruszeniu bezpieczeństwa danych osobowych Administratora Danych (AD),

   d) w przypadku potwierdzenia naruszenia bezpieczeństwa 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;

5) W ramach przyznanych uprawnień Administrator Bezpieczeństwa Informacji (ABI) oraz Administrator Systemu Informatycznego (ASI) mają prawo do:

   a) żądania wyjaśnień od pracowników Ministerstwa,

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

   c) czasowego zablokowania uprawnień wskazanym użytkownikom lub wszystkim użytkownikom systemu informatycznego Ministerstwa;

6) Odmowa wyjaśnień lub współpracy z Administratorem Bezpieczeństwa Informacji (ABI) oraz z Administratorem Systemu Informatycznego (ASI), przy wyjaśnianiu okoliczności naruszenia zasad ochrony danych osobowych, będzie traktowana jako naruszenie obowiązków pracowniczych.

§ 46. 1. Z przeprowadzonego postępowania Administrator Bezpieczeństwa Informacji (ABI), przy udziale Administratora Systemu Informatycznego (ASI) w przypadku naruszenia zabezpieczenia danych w systemie informatycznym, sporządza raport dla Administratora Danych (AD).

2. Raport powinien zawierać w szczególności: wskazanie osoby/osób powiadamiającej 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 bezpieczeństwa danych osobowych lub zabezpieczeń systemu informatycznego stosuje się odpowiednie przepisy ustawy oraz postanowienia § 52 Regulaminu pracy, w zakresie odpowiedzialności dyscyplinarnej i porządkowej pracowników.

Rozdział 11.
POSTANOWIENIA KOŃCOWE

§ 47. 1. Polityka jest dokumentem wewnętrznym i może być udostępniana uprawnionym podmiotom zewnętrznym w celu zapoznania się i postepowania w zgodzie z postanowieniami niniejszego dokumentu.

2. Do spraw nieuregulowanych w Polityce, w zakresie ochrony danych osobowych stosuje się przepisy ustawy, rozporządzenia oraz Instrukcji.

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

§ 49. Integralną część niniejszej Polityki stanowią następujące załączniki:

1) Załącznik nr 1 – Wzór upoważnienia Ministra Sportu i Turystyki do pełnienia obowiązków Pełnomocnika ds. Ochrony Danych Osobowych w Ministerstwie Sportu i Turystyki;

2) Załącznik nr 2 – Wzór wyznaczania Administratora Bezpieczeństwa Informacji w Ministerstwie;

3) Załącznik nr 3 – Wzór wyznaczania Administratora Systemu Informatycznego w Ministerstwie;

4) Załącznik nr 4 – Wzór wniosku o nadanie, zmianę, odwołanie upoważnienia do przetwarzania danych osobowych;

5) Załącznik nr 5 – Wzór upoważnienia do przetwarzania danych osobowych;

6) Załącznik nr 6 – Wzór oświadczenia o poufności;

7) Załącznik nr 7 – Wzór Wykazu zbiorów danych osobowych przetwarzanych w Ministerstwie Sportu i Turystyki

8) Załącznik nr 8 – Wzór rejestru stwierdzonych naruszeń;

9) Załącznik nr 9 – Wzór formularza informacyjnego;

10) Załącznik nr 10 – Schemat organizacyjny w zakresie ochrony danych osobowych w Ministerstwie.

Załącznik nr 1 do Polityki Bezpieczeństwa
Informacji Ministerstwa Sportu i Turystyki

WZÓR

**MINISTER
SPORTU I TURYSTYKI**

Warszawa, dnia r.

UPOWAŻNIENIE NR …

Na podstawie art. 37 ustawy z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (Dz. U. z 2002 r. Nr 101, poz. 926, z późn. zm.) wyznaczam

Panią/Pana……
(imię i nazwisko, stanowisko, komórka organizacyjna)

na

PEŁNOMOCNIKA DS. OCHRONY DANYCH OSOBOWYCH W MINISTERSTWIE SPORTU I TURYSTYKI

oraz upoważniam

do wykonywania w imieniu Administratora Danych czynności wynikających z ustawy z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (Dz. U. z 2002 r. Nr 101, poz. 926, z późn. zm.) oraz Polityki Bezpieczeństwa Informacji stanowiącej załącznik nr 1 do zarządzenia nr … Ministra Sportu i Turystyki z dnia … 2013 r. w sprawie ustalenia zasad bezpieczeństwa informacji w Ministerstwie Sportu i Turystyki.

Niniejsze upoważnienie uprawnia Pełnomocnika ds. Ochrony Danych Osobowych w Ministerstwie Sportu i Turystyki do udzielania dalszych upoważnień w zakresie wskazanym powyżej.

Niniejsze upoważnienie obowiązuje na czas pełnienia funkcji Pełnomocnika ds. Ochrony Danych Osobowych w Ministerstwie Sportu i Turystyki albo do odwołania.

W czasie usprawiedliwionej nieobecności Pełnomocnika ds. Ochrony Danych Osobowych w Ministerstwie Sportu i Turystyki, do wykonywania czynności, o których mowa powyżej, upoważniam Panią/Pana …… pełniącego funkcję Administratora Bezpieczeństwa Informacji w Ministerstwie Sportu i Turystyki.

……
(podpis i pieczęć Ministra Sportu i Turystyki)

Zgodnie z art. 39 ust. 2 ustawy o ochronie danych osobowych zobowiązuje się do zachowania w tajemnicy treści przetwarzanych danych osobowych oraz sposobów ich zabezpieczania w okresie wykonywania obowiązków związanych z przetwarzaniem danych, zmiany, odwołania a także po ustaniu stosunku pracy.

Przyjmuję do realizacji
powierzone mi obowiązki i uprawnienia

……
(data i podpis upoważnionego)

Załącznik nr 2 do Polityki Bezpieczeństwa
Informacji Ministerstwa Sportu i Turystyki

WZÓR

Warszawa, dnia r.

MINISTER
SPORTU I TURYSTYKI

Na podstawie art. 36 ust. 3 ustawy z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (Dz. U. z 2002 r. Nr 101, poz. 926, z późn. zm.) oraz § 8 ust. 2 Polityki Bezpieczeństwa Informacji stanowiącej załącznik nr 1 do zarządzenia nr … Ministra Sportu i Turystyki z dnia … w sprawie ustalenia zasad bezpieczeństwa informacji w Ministerstwie Sportu i Turystyki, wyznaczam

Panią/Pana……
(imię i nazwisko)

……
(stanowisko, komórka organizacyjna)

na

ADMINISTRATORA BEZPIECZEŃSTWA INFORMACJI
W MINISTERSTWIE SPORTU I TURYSTYKI

Administrator Bezpieczeństwa Informacji zobowiązany jest do wdrażania i nadzoru nad prawidłową realizacją czynności dotyczących przetwarzania danych osobowych w Ministerstwie Sportu i Turystyki poprzez zastosowanie środków technicznych i organizacyjnych zapewniających ochronę przetwarzanych danych osobowych, odpowiednio do zagrożeń oraz kategorii danych objętych ochroną, zgodnie z § 26 Polityki Bezpieczeństwa Informacji stanowiącej załącznik nr 1 do zarządzenia nr … Ministra Sportu i Turystyki z dnia … w sprawie ustalenia zasad bezpieczeństwa informacji w Ministerstwie Sportu i Turystyki.

……..…
(podpis i pieczęć Administratora Danych/
Pełnomocnika ds. ochrony danych osobowych)

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)

Załącznik nr 3 do Polityki Bezpieczeństwa
Informacji Ministerstwa Sportu i Turystyki

WZÓR

Warszawa, dnia r.

MINISTER
SPORTU I TURYSTYKI

Na podstawie § 8 ust. 3 Polityki Bezpieczeństwa Informacji stanowiącej załącznik nr 1 do zarządzenia nr … Ministra Sportu i Turystyki z dnia … 2013 r. w sprawie ustalenia zasad bezpieczeństwa informacji w Ministerstwie Sportu i Turystyki, wyznaczam

Panią/Pana……..
(imię i nazwisko, stanowisko, departament)

na

ADMINISTRATORA SYSTEMU INFORMATYCZNEGO
W MINISTERSTWIE SPORTU I TURYSTYKI

Administrator Systemu Informatycznego zobowiązany jest do zastosowania środków technicznych i organizacyjnych zapewniających ochronę przetwarzanych danych osobowych w systemach informatycznych Ministerstwa Sportu i Turystyki oraz realizacji zadań określonych w § 27 Polityki Bezpieczeństwa Informacji stanowiącej załącznik nr 1 do zarządzenia nr … Ministra Sportu i Turystyki z dnia … 2013 r. w sprawie ustalenia zasad bezpieczeństwa informacji w Ministerstwie Sportu i Turystyki.

……
(podpis i pieczęć Administratora Danych/
Pełnomocnika ds. ochrony danych osobowych)

Zgodnie z art. 39 ust. 2 ustawy o ochronie danych osobowych zobowiązuje się do zachowania w tajemnicy treści przetwarzanych danych osobowych oraz sposobów ich zabezpieczania w okresie wykonywania obowiązków związanych z przetwarzaniem danych, zmiany, odwołania a także po ustaniu stosunku pracy.

Przyjmuję do realizacji
powierzone mi obowiązki i uprawnienia

……
(data i podpis upoważnionego)

Załącznik nr 4 do Polityki Bezpieczeństwa
Informacji Ministerstwa Sportu i Turystyki

WZÓR

Warszawa, dnia ……r.

……
(pieczęć/nagłówek komórki organizacyjnej)

W N I O S E K

o nadanie/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 2002 r. Nr 101, poz. 926, z późn. zm.) oraz § 33 ust. 2 Polityki Bezpieczeństwa Informacji stanowiącej załącznik nr 1 do zarządzenia nr … Ministra Sportu i Turystyki z dnia … w sprawie ustalenia zasad bezpieczeństwa informacji w Ministerstwie Sportu i Turystyki, proszę o

☐ - nadanie ☐ - zmianę ☐ - odwołanie

upoważnienia

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

……
(stanowisko, komórka organizacyjna)

do wykonywania czynności związanych z przetwarzaniem danych osobowych w następujący w 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 pieczęć Dyrektora komórki organizacyjnej)

Załącznik nr 5 do Polityki Bezpieczeństwa
Informacji Ministerstwa Sportu i Turystyki

WZÓR

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 2002 r. Nr 101, poz. 926, z późn. zm.) oraz § 33 ust. 3 Polityki Bezpieczeństwa Informacji stanowiącej załącznik nr 1 do zarządzenia nr … Ministra Sportu i Turystyki z dnia … w sprawie ustalenia zasad bezpieczeństwa informacji w Ministerstwie Sportu i Turystyki, 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/
Pełnomocnika ds. ochrony danych osobowych)

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 6 do Polityki Bezpieczeństwa
Informacji Ministerstwa 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 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 bezpośredniemu przełożonemu i Administratorowi Bezpieczeństwa Informacji w Ministerstwie Sportu i Turystyki wszelkich faktycznych prób lub podejrzeń 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 2002 r. Nr 101, poz. 926, z późn. zm.) i zasadami bezpieczeństwa przetwarzania danych osobowych określonych w Zarządzeniu nr … Ministra Sportu i Turystyki z dnia … w sprawie ustalenia zasad bezpieczeństwa informacji 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 7 do Polityki Bezpieczeństwa
Informacji Ministerstwa Sportu i Turystyki

WZÓR

Wykaz zbiorów danych osobowych przetwarzanych w MSiT

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)
(1)	(2)	(3)	(4)	(5)	(6)	(7)	(8)	(9)	(10)
1.									
2.									
3.									

Załącznik nr 8 do Polityki Bezpieczeństwa
Informacji Ministerstwa Sportu i Turystyki

Rejestr stwierdzonych naruszeń w Ministerstwie Sportu i Turystyki

Lp.	Rodzaj stwierdzonego naruszenia	Rodzaj podjętych czynności	Data zgłoszenia naruszenia	Podpis osoby zgłaszającej	Podpis ABI/ASI	Podpis Administratora Danych
1						
2						
3						

Załącznik nr 9 do Polityki Bezpieczeństwa
Informacji Ministerstwa Sportu i Turystyki

WZÓR

Warszawa, dnia ……..

FORMULARZ INFORMACYJNY

☐ nowy pracownik ☐ **zmiana danych pracownika** ☐ zakończenie pracy w MSiT

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

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

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

4. Forma zatrudnienia: ☐ stosunek pracy ☐ umowa cywilno-prawna ☐ praktyka/staż/wolontariat

5. Rodzaj umowy: ☐ na czas określony ☐ na czas nieokreślony

6. Okres zatrudnienia: *(należy uzupełnić w przypadku zatrudnienia na czas określony)*

Od:		Do:	

CZĘŚĆ C: DANE O SYSTEMACH KONTROLI DOSTĘPU

☐ **dane o dostępie bez zmian**

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 dostępie do systemów informatycznych bez zmian**

1. Domena: ☐ utworzenie konta osobistego

2. ESOD: ☐ utworzenie konta osobistego
☐ ustanowienie zastępstwa – za: …… na okres: ……...….

3. Poczta e-mail: ☐ osobista ☐ przypisanie do grupy: …….

4. Dostęp do aplikacji (wypisać niezbędne aplikacje): …….

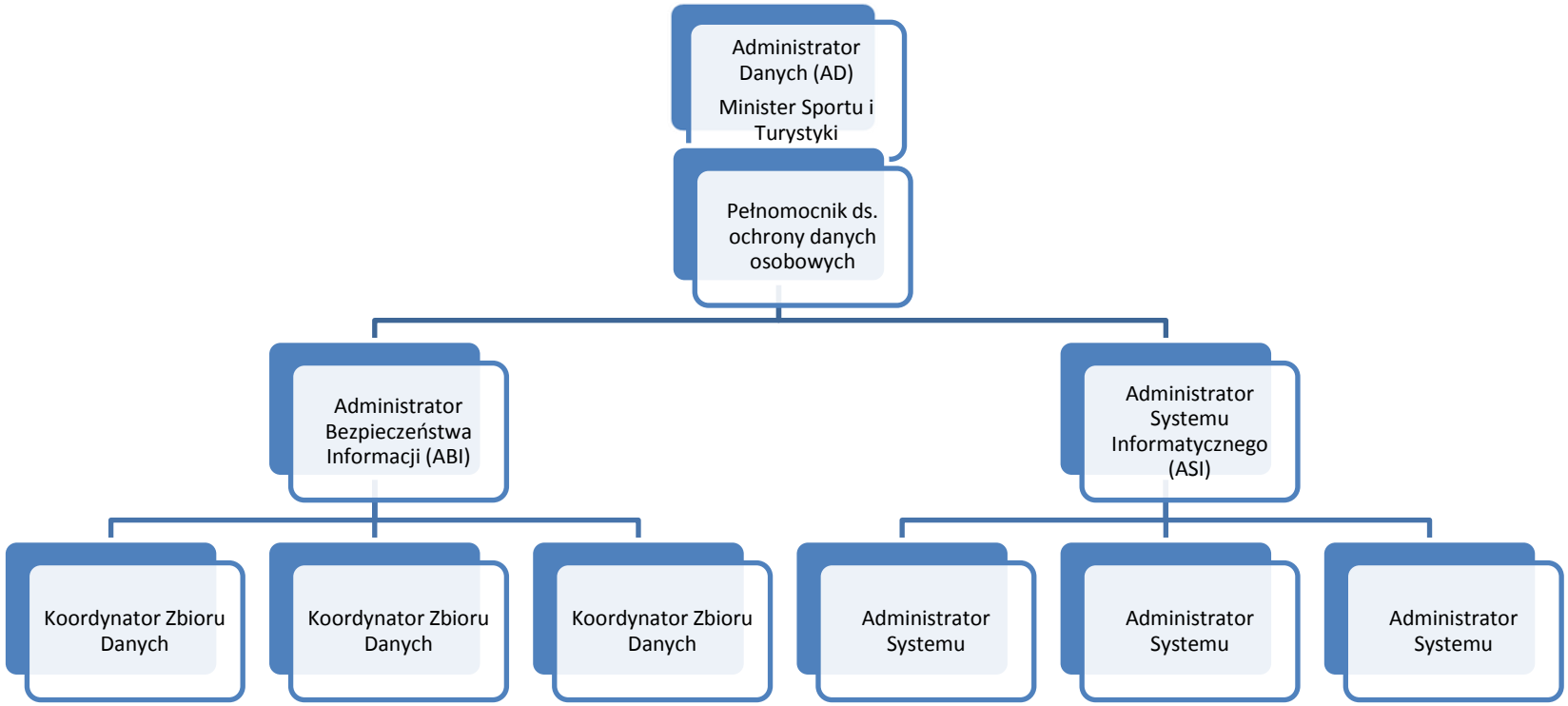
☐ Oświadczam, iż ww. pracownik posiada upoważnienie do przetwarzania danych osobowych w zakresie wnioskowanych uprawnień dostępowych

…… ……..…….

akceptacja Dyrektora Biura Administracyjnego *Podpis Dyrektora komórki organizacyjnej*

Załącznik nr 10 do Polityki Bezpieczeństwa Informacji
Ministerstwa Sportu i Turystyki

SCHEMAT ORGANIZACYJNY W ZAKRESIE OCHRONY DANYCH OSOBOWYCH W MSIT



Załącznik Nr 2 do Zarządzenia Nr 20

Ministra Sportu i Turystyki

z dnia 9 lipca 2013 r.

INSTRUKCJA ZARZĄDZANIA SYSTEMEM INFORMATYCZNYM

Rozdział 1. POSTANOWIENIA OGÓLNE

§ 1. Instrukcja Zarządzania Systemem Informatycznym określa procedury i zasady postępowania przy przetwarzaniu danych, w szczególności danych osobowych, w zbiorach danych systemu informatycznego Ministerstwa Sportu i Turystyki.

§ 2. Użyte w Instrukcji określenia oznaczają:

1) **Ministerstwo** – Ministerstwo Sportu i Turystyki;
2) **komórka organizacyjna** – właściwy rzeczowo departament/biuro, którego zadania określone zostały w regulaminie organizacyjnym Ministerstwa;
3) **użytkownik** – osoba przetwarzająca dane, w tym dane osobowe, w systemie informatycznym, w ramach wykonywanych zadań, niezależnie od charakteru zatrudnienia lub wykonywanych prac zleconych;
4) **Instrukcja –** Instrukcja zarządzania systemem informatycznym Ministerstwa;
5) **Polityka** – Polityka bezpieczeństwa informacji obowiązująca w Ministerstwie;
6) **ustawa –** ustawa z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (Dz. U. z 2002 r. Nr 101, poz. 926, z późn. zm.);
7) **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. Nr 100, poz. 1024);
8) **Administrator Danych (AD) –** Minister Sportu i Turystyki;
9) **Pełnomocnik ds. ochrony danych osobowych –** pracownik Ministerstwa, któremu Administrator Danych, na podstawie pisemnego upoważnienia, może powierzyć realizację zadań wynikających z ustawy;
10) **Administrator Systemu Informatycznego (ASI)** – pracownik Ministerstwa wyznaczony przez Administratora Danych nadzorujący i kontrolujący funkcjonowanie całości systemu informatycznego Ministerstwa, w szczególności części systemu, w których przetwarzane są dane osobowe;
11) **Administrator Bezpieczeństwa Informacji (ABI)** – pracownik Ministerstwa wyznaczony przez Administratora Danych, nadzorujący i kontrolujący przestrzeganie zasad ochrony danych osobowych w Ministerstwie;
12) **Administrator Systemu** – specjalista informatyk, realizujący zadania techniczne w celu zapewnienia bezpiecznej eksploatacji wybranych urządzeń i aplikacji wykorzystywanych do przetwarzania danych;
13) **dane osobowe** – wszelkie informacje dotyczące zidentyfikowanej lub możliwej do zidentyfikowania osoby fizycznej; 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;

14) **zabezpieczenie danych osobowych –** środki administracyjne, techniczne i fizyczne wdrożone w celu zabezpieczenia zasobów technicznych oraz ochrony przed zniszczeniem, nieuprawnionym dostępem i modyfikacją, ujawnieniem lub pozyskaniem danych osobowych bądź ich utratą;

15) **naruszenie zabezpieczenia –** jakiekolwiek naruszenie bezpieczeństwa, niezawodności, integralności lub poufności;

16) **dostępność informacji** – zapewnienie, że podmioty uprawnione mają dostęp do informacji tylko w uzasadnionych przypadkach;

17) **nośnik –** dyskietki, płyty CD lub DVD, pamięć flash, dyski twarde, taśmy magnetyczne lub inne urządzenia/materiały służące do przechowywania plików z danymi;

18) **zniszczenie nośnika –** trwałe i nieodwracalne fizyczne zniszczenie nośnika uniemożliwiające rekonstrukcje i odzyskanie danych;

19) **identyfikator użytkownika –** ciąg znaków literowych, cyfrowych i/lub innych jednoznacznie identyfikujący osobę upoważnioną do przetwarzania danych osobowych w systemie informatycznym;

20) **konto „Root”/Administrator –** konto administracyjne, które umożliwia pełne zarządzanie systemem informatycznym.

Rozdział 2.
ZARZĄDZANIE UPRAWNIENIAMI UŻYTKOWNIKÓW

§ 3. 1. Zarządzanie uprawnieniami dostępu do systemu informatycznego, w tym do zbiorów danych osobowych obejmuje przyznanie, cofnięcie lub zmianę zakresu uprawnień użytkowników.

2. Czynności przyznania, cofnięcia lub zmiany zakresu uprawnień dla użytkowników systemu informatycznego Ministerstwa realizuje Administrator Systemu Informatycznego (ASI), na podstawie wniosku dyrektora właściwej komórki organizacyjnej, przesłanego za pomocą elektronicznego systemu obiegu dokumentów.

3. Wzór wniosku o którym mowa w ust. 2 określa załacznik nr 9 do Polityki.

4. Po realizacji czynności, o których mowa w ust. 2, Administrator Systemu Informatycznego (ASI) przekazuje kopię wniosku Administratorowi Bezpieczeństwa Informacji (ABI).

§ 4. 1. Rejestracja użytkownika w systemie informatycznym Ministerstwa polega na przydziale identyfikatora i hasła dostępu.

2. Wyrejestrowanie użytkownika z systemu informatycznego Ministerstwa polega na cofnięciu uprawnień dostępu.

3. Osoby uprawnione do wykonywania prac administracyjnych w systemie informatycznym Ministerstwa posiadają własne konta administracyjne oraz hasła.

4. Użytkownik jest wyrejestrowywany z systemu informatycznego Ministerstwa w każdym przypadku utraty przez niego uprawnień, szczególnie w sytuacji:

1) ustania zatrudnienia użytkownika w Ministerstwie;

2) zmiany zakresu obowiązków użytkownika.

5. Dyrektorzy komórek organizacyjnych zobowiązani są informować Administratora Systemu Informatycznego (ASI) o każdej zmianie dotyczącej podległych im pracowników, mającej wpływ na zakres posiadanych przez nich uprawnień. Informacje należy przesyłać za pomocą elektronicznego systemu obiegu dokumentów.

§ 5. 1. Administratorzy Systemu zobowiązani są do wykonywania bieżącej pracy na koncie roboczym.

2. Użycie konta „Root”/Administrator dopuszczalne jest jedynie w sytuacji awarii lub podczas poważnych zmian wprowadzanych w systemie informatycznym Ministerstwa.

3. Hasło do konta „Root”/Administrator znane jest tylko Administratorowi Systemu Informatycznego (ASI) oraz Administratorom Systemu.

Rozdział 3.
METODY I ŚRODKI UWIERZYTELNIANIA UŻYTKOWNIKÓW

§ 6. 1. Dostęp do części systemu informatycznego Ministerstwa, w którym przetwarzane są dane osobowe, mają wyłącznie osoby do tego upoważnione.

2. Dostęp do systemu informatycznego Ministerstwa, w tym do zbiorów danych osobowych, możliwy jest jedynie po dokonaniu uwierzytelnienia użytkownika, poprzez podanie identyfikatora i hasła.

3. Dla każdego użytkownika jest ustalany indywidualny identyfikator i hasło dostępu do systemu informatycznego Ministerstwa.

4. Użytkownik jest odpowiedzialny za wszystkie czynności wykonane przy użyciu identyfikatora, który został mu przyznany. Użytkownik nie może udostępniać identyfikatora osobom nieuprawnionym.

5. Użytkownik jest zobowiązany utrzymywać hasło, którym się posługuje lub posługiwał, w ścisłej tajemnicy, w szczególności dołożyć wszelkich starań w celu uniemożliwienia zapoznania się z hasłem przez osoby nieuprawnione, nawet po ustaniu jego ważności.

6. Przypadki, w których konieczne jest udostępnienie identyfikatora i hasła Użytkownika innej osobie rozpatrywane są indywidualnie przez Administratora Danych (AD) na wniosek Dyrektora właściwej komórki organizacyjnej.

7. Po uwierzytelnieniu w systemie informatycznym Ministerstwa użytkownik nie może udostępniać osobom nieuprawnionym swojego stanowiska pracy.

§ 7. 1. W celu zapewnienia jednoznacznej identyfikacji użytkowników systemu przyjmuje się następującą metodologię nadawania nazw kont: pierwsza litera imienia + nazwisko.

2. W nazwie identyfikatora stosuje się małe litery, z wyłączeniem polskich znaków. Nie stosuje się spacji ani znaków interpunkcyjnych.

3. Zasady opisane w ust. 1 i 2 nie dotyczą oprogramowania, w którym nazwa użytkownika generowana jest automatycznie.

4. Identyfikator użytkownika jest niepowtarzalny, a po wyrejestrowaniu użytkownika z systemu informatycznego Ministerstwa nie jest przydzielany innej osobie.

§ 8. 1. Administrator Systemu Informatycznego (ASI) ustala jednorazowe hasło dla nowego użytkownika systemu informatycznego Ministerstwa. Hasło przekazywane jest użytkownikowi wraz z zestawem komputerowym.

2. Przy pierwszym logowaniu system informatyczny Ministerstwa wymusza na użytkowniku zmianę hasła na znany tylko jemu ciąg znaków. W przypadku oprogramowania, nieposiadającego mechanizmów hasła jednorazowego, hasło tworzone jest zgodnie z zasadami funkcjonowania danego programu.

3. Hasło użytkownika:

1) przydzielane jest indywidualnie dla każdego użytkownika;

2) nie jest zapisane w systemie informatycznym Ministerstwa w postaci jawnej;

3) zmieniane jest co najmniej raz na 30 dni;

4) nie może być zapisane w miejscu dostępnym dla osób nieuprawnionych;

5) utrzymywane jest w tajemnicy, również po upływie jego ważności.

4. Utworzenie hasła dokonywane jest w następujący sposób:

1) hasło powinno składać się z co najmniej 8 znaków i musi zawierać małe i wielkie litery oraz cyfry lub znaki specjalne;

2) hasła nie powinny składać się z kombinacji znaków mogących ułatwić ich odgadnięcie lub odszyfrowanie przez osoby nieuprawnione (np.: imię, nazwisko użytkownika).

5. Zmiany hasła dokonuje użytkownik. W przypadku, gdy użytkownik zapomniał hasła, Administrator Systemu Informatycznego (ASI) ustala hasło tymczasowe, z wymuszeniem jego zmiany podczas kolejnego logowania użytkownika.

§ 9. 1. Dane autoryzacyjne przesyłane przez sieć komputerową są automatycznie szyfrowane.

2. Hasła użytkowników systemu informatycznego Ministerstwa w domenie przechowywane są w formie elektronicznej na serwerze w zaszyfrowanej postaci.

3. Hasła Administratora Systemu Informatycznego (ASI) oraz Administratorów Systemu przechowywane są w jawnej postaci w formie papierowej w zapieczętowanej kopercie i umieszczone w sejfie.

4. Każdorazowo, po dokonaniu zmiany haseł administracyjnych, o których mowa w ust. 3, nowoutworzone hasła, Administrator Systemu Informatycznego (ASI) umieszcza w sejfie, w formie określonej w ust. 3.

5. Rejestr zmian haseł administracyjnych, o którym mowa w § 27 ust. 2 pkt 9 lit. d Polityki zawiera informację o programie, użytkowniku oraz o dacie ostatniej zmiany hasła.

6. System przechowuje historię 5 ostatnich haseł użytkownika Systemu.

§ 10. 1. W celu zabezpieczenia kont użytkowników przed próbą złamania hasła, system informatyczny Ministerstwa automatycznie blokuje konto użytkownika po 3 nieudanych próbach zalogowania.

2. Blokada konta, o której mowa w ust. 1, zdejmowana jest automatycznie po 30 minutach.

3. Wcześniejsze odblokowanie konta możliwe jest wyłącznie przez Administratora Systemu.

Rozdział 4.
ZABEZPIECZENIA SYSTEMU INFORMATYCZNEGO

§ 11. W celu zabezpieczenia systemu informatycznego Ministerstwa zastosowano następujące środki bezpieczeństwa:

1) mechanizm wymuszający okresową zmianę haseł dostępu;

2) mechanizm uwierzytelnienia z wykorzystaniem identyfikatora użytkownika oraz hasła;

3) mechanizm umożliwiający automatyczną rejestrację identyfikatora użytkownika i datę pierwszego wprowadzenia danych osobowych;

4) mechanizmy pozwalające na określenie odpowiednich praw dostępu do zasobów informatycznych, w tym zbiorów danych osobowych dla poszczególnych użytkowników systemu informatycznego;

5) kryptograficzne środki ochrony danych osobowych (szyfrowanie baz danych);

6) automatyczne wygaszanie ekranów na stanowiskach;

7) mechanizm automatycznej blokady dostępu do systemu informatycznego Ministerstwa w przypadku okresu dłuższej nieaktywności użytkownika;

8) system antywirusowy;

9) oprogramowanie zainstalowane na stacjach roboczych posiada niezbędne licencje i jest użytkowane z zachowaniem praw autorskich.

10) stacje robocze są monitorowane pod kątem zapewnienia bezpieczeństwa danych, nadzoru wykorzystania sprzętu służbowego, zgodności działań użytkownika z Polityką oraz Instrukcją.

§ 12. W celu zabezpieczenia infrastruktury informatycznej i telekomunikacyjnej w Ministerstwie zastosowano:

1) środki bezpieczeństwa przed skutkami awarii zasiania (UPS-y podtrzymujące zasilanie serwera i pozostałych kluczowych elementów systemu IT, wydzielona sieć elektroenergetyczna, listwy przeciw-przepięciowe);

2) zabezpieczenia trwałych elementów infrastruktury (serwery, macierze, urządzenia aktywne) – kontrola dostępu do pomieszczeń z ww. elementami;

3) zabezpieczenia przed szkodliwym oprogramowaniem i nieuprawnionym dostępem do przetwarzanych danych (Firewall, system IDS/IPS);

4) mechanizmy monitorujące aktywność użytkowników w Internecie;

5) blokowanie stron internetowych określonego typu oraz analiza przesyłanych informacji pod kątem niebezpiecznego oprogramowania, w tym przeglądanie zasobów internetowych;

6) umieszczenie klimatyzatorów w serwerowniach w celu zapewnienia właściwych warunków pracy infrastruktury informatycznej i telekomunikacyjnej;

7) kontrole dostępu do portów USB i nośników danych;

8) cykliczne wykonywanie kopii zgromadzonych danych.

Rozdział 5.
ROZPOCZĘCIE, ZAWIESZENIE I ZAKOŃCZENIE PRACY W SYSTEMIE

§ 13. 1. W celu rozpoczęcia pracy użytkownik systemu loguje się do systemu operacyjnego używając indywidualnego identyfikatora i hasła. Praca w systemie informatycznym możliwa jest wyłącznie na podstawie autoryzacji, poprzez podanie prawidłowego identyfikatora oraz powiązanego z nim hasła.

2. W przypadku stwierdzenia, że logowanie jest niemożliwe z użyciem aktualnie obowiązującego hasła należy zawiadomić Administratora Systemu Informatycznego (ASI).

3. Podczas logowania należy zwracać szczególną uwagę na systemowe komunikaty informujące o konieczności zmiany hasła i stosować się do ich treści, a w razie wątpliwości poinformować Administratora Systemu Informatycznego (ASI).

4. Praca jednego użytkownika na kilku komputerach równocześnie, z wykorzystaniem tego samego identyfikatora, jest dozwolona w uzasadnionych przypadkach wynikających z zakresu wykonywanych obowiązków.

§ 14. 1. Przed uruchomieniem komputera użytkownik powinien sprawdzić:

1) stanowisko komputerowe, z którego korzysta – szczególną uwagę powinien zwrócić na fizyczne ślady prób otwarcia komputera;

2) ustawienie monitora – w przypadku stanowisk dostępu do danych osobowych należy ustawić ekrany monitorów w taki sposób, aby uniemożliwić wgląd w dane przebywającym w pomieszczeniu osobom nieupoważnionym.

2. Po uruchomieniu komputera użytkownik powinien:

1) sprawdzić, czy nie ma oznak modyfikacji danych (brak plików, odmienny wygląd systemu po uruchomieniu, nietypowe komunikaty systemowe);

2) zweryfikować stan programu antywirusowego, a w szczególności, sprawdzić czy jest uruchomiony i posiada aktualne bazy sygnatur.

3. Każdy użytkownik, który stwierdzi lub podejrzewa naruszenie ochrony danych osobowych w systemie informatycznym Ministerstwa, zobowiązany jest niezwłocznie poinformować o tym fakcie Administratora Bezpieczeństwa Informacji (ABI) oraz Administratora Systemu Informatycznego (ASI).

4. W sytuacji stwierdzenia naruszenia lub podejrzenia naruszenia zasad ochrony danych osobowych w systemie obowiązuje tryb postępowania określony w § 44-46 Polityki.

§ 15. 1. Użytkownik, opuszczający czasowo stanowisko pracy, jest zobowiązany do zablokowania konta.

2. W przypadku, gdy użytkownik planuje przerwać pracę na dłuższy okres lub zakończyć pracę, zobowiązany jest do wylogowania się z systemu informatycznego Ministerstwa oraz sprawdzenia, czy nie zostały pozostawione bez zamknięcia nośniki zawierające dane osobowe.

§ 16. 1. Użytkownik kończący pracę, przed wylogowaniem z systemu informatycznego Ministerstwa, powinien zamknąć wszystkie używane programy.

2. Po prawidłowym zamknięciu programów użytkownik powinien wylogować się lub zamknąć system operacyjny.

3. Jeżeli komputer nie wyłącza się automatycznie, z uwagi na nieprawidłowo działające oprogramowanie, należy wyłączyć go odpowiednim przyciskiem na obudowie.

§ 17. 1. Użytkownik zobowiązany jest do korzystania z sieci Internet wyłącznie w celach służbowych.

2. Zabrania się zgrywania na dysk twardy komputera oraz uruchamiania programów nielegalnych oraz plików pobranych z niewiadomego źródła.

3. Użytkownik ponosi odpowiedzialność za szkody spowodowane przez oprogramowanie pobrane z Internetu i zainstalowane bez wiedzy Administratora Systemu Informatycznego (ASI).

4. Zabrania się wchodzenia na strony, na których prezentowane są informacje o charakterze przestępczym, hakerskim, pornograficznym lub innym zakazanym przez prawo.

5. Nie należy w opcjach przeglądarki internetowej włączać opcji autouzupełniania formularzy i zapamiętywania haseł.

6. W przypadku korzystania z szyfrowanego połączenia przez przeglądarkę internetową, należy zwrócić uwagę na nazwę protokołu (https) oraz obecność odpowiedniej ikony (zamknięta kłódka) w pasku adresu przeglądarki. Kliknięcie ikony powoduje wyświetlenie certyfikatu, na podstawie którego można sprawdzić zabezpieczenie witryny internetowej.

§ 18. 1. Korzystanie ze służbowej poczty elektronicznej dopuszczalne jest wyłącznie w celach służbowych.

2. Korzystając ze służbowej poczty elektronicznej użytkownik powinien zwracać szczególną uwagę na poprawność adresu odbiorcy dokumentu.

3. Zaleca się, aby użytkownik podczas przesyłania danych osobowych mailem, zawarł w treści prośbę o potwierdzenie otrzymania i zapoznania się z informacją przez adresata. Przed wysłaniem, dane osobowe należy zaszyfrować.

4. Nie należy otwierać plików załączonych do korespondencji elektronicznej nadesłanej przez nieznanego nadawcę lub podejrzanych załączników nadanych przez znanego nadawcę.

5. Zabrania się wysyłania za pośrednictwem poczty elektronicznej informacji o zagrożeniach dla systemu informatycznego, „łańcuszków szczęścia” itp.

6. Zabrania się rozsyłania wiadomości zawierających załączniki o dużym rozmiarze dla większej liczby adresatów. W celu określenia krytycznych rozmiarów przesyłek i dopuszczalnej liczby adresatów należy skontaktować się z Administratorem Systemu Informatycznego (ASI).

7. Zaleca się okresowe archiwizowanie wiadomości pocztowych.

8. Zaleca się okresowe kasowanie niepotrzebnych wiadomości pocztowych.

§ 19. 1. W celu zapobieżenia naruszeniu zasad ochrony danych osobowych, pracownicy Ministerstwa korzystający ze służbowych komputerów przenośnych (lub innych nośników do przetwarzania danych osobowych), zobowiązani są zachować szczególną ostrożność podczas transportu i korzystania z nich, poza wskazanym w Polityce obszarem przetwarzania danych osobowych.

2. Osoby wskazane w ust. 1 mają obowiązek zabezpieczyć dostęp do komputera hasłem oraz nie udostępniać komputerów osobom nieupoważnionym.

Rozdział 6.
KOPIE ZAPASOWE ORAZ NOŚNIKI ELEKTRONICZNE

§ 20. Procedura określa zasady postępowania z nośnikami elektronicznymi, na których znajdują się dane osobowe oraz procedury tworzenia zapasowych kopii danych, celem zabezpieczenia ich przez zniszczeniem, kradzieżą oraz dostępem osób nieupoważnionych.

§ 21. 1. Dane przetwarzane w systemie informatycznym Ministerstwa, w tym dane osobowe, podlegają zabezpieczeniu poprzez tworzenie kopii zapasowych.

2. Za wszelkie czynności związane z tworzeniem kopii zapasowych, ich testowaniem, przechowywaniem odpowiedzialny jest Administrator Systemu Informatycznego (ASI).

3. Kopie zapasowe mogą być tworzone również przez Administratorów Systemu.

4. Za likwidację nośników zawierających zbiory danych osobowych odpowiedzialny jest Administrator Systemu Informatycznego (ASI).

§ 22. 1. Przez tworzenie kopii danych rozumie się przegrywanie zbiorów danych na specjalnie wydzielony do tego celu obszar dysku na serwerze.

2. Kopie zapasowe przechowuje się na serwerze odrębnym od tego, na którym zbiór danych eksploatowany jest na bieżąco.

3. Kopie zapasowe przechowywane są w sposób uniemożliwiający nieuprawnione przejęcie, modyfikację, uszkodzenie lub zniszczenie, m. in.:

1) w sejfie, w pomieszczeniu Biura Administracyjnego;

2) w serwerowni.

4. Dostęp do nośników z kopiami zapasowymi systemu informatycznego Ministerstwa oraz kopiami danych osobowych mają:

1) Administrator Systemu Informatycznego (ASI);

2) Administratorzy Systemu;

3) Administrator Bezpieczeństwa Informacji (ABI).

5. Administrator Systemu Informatycznego (ASI) zobowiązany jest do prowadzenia rejestru kopii zapasowych wszystkich części systemu informatycznego Ministerstwa, o którym mowa w § 27 ust. 2 pkt 9 lit. b Polityki.

§ 23. 1. Kopie zapasowe zbiorów danych są okresowo sprawdzane pod kątem ich przydatności do odtworzenia przez Administratora Systemu Informatycznego (ASI) lub wyznaczonego przez niego Administratora Systemu.

2. Po ustaniu ich użyteczności, kopie zapasowe danych przetwarzanych w systemie informatycznym Ministerstwa, w tym danych osobowych, są niezwłocznie usuwane.

3. Kopie zapasowe danych przetwarzanych w systemie informatycznym Ministerstwa, w tym danych osobowych, które uległy uszkodzeniu, podlegają natychmiastowemu zniszczeniu.

§ 24. 1. Ze względu na różnorodność danych podlegających zabezpieczeniu stosuje się, właściwą dla poszczególnych części systemu informatycznego Ministerstwa, metodologię i harmonogram tworzenia kopii zapasowych.

2. Kopie zapasowe wykonywane są zgodnie z następującymi zasadami:

1) kopia zapasowa danego oprogramowania – pełna kopia wykonywana jest po wprowadzeniu zmian do oprogramowania i zapisywana na serwerze;

2) kopia zapasowa zbiorów danych przetwarzanych w systemie informatycznym Ministerstwa, w tym danych osobowych – pełna kopia wykonywana jest raz w tygodniu, a w przypadku wprowadzenia znacznych zmian danych, może być wykonywana nawet raz dziennie;

3) kopia zapasowa danych konfiguracyjnych systemu informatycznego Ministerstwa, w tym uprawnień użytkowników – pełna kopia wykonywana jest co najmniej raz w tygodniu.

§ 25. 1. Nośniki danych przechowywane są w sposób uniemożliwiający dostęp do nich osobom nieupoważnionym, jak również zabezpieczający je przed zagrożeniami środowiskowymi.

2. Zabrania się wynoszenia poza obszar Ministerstwa wymiennych nośników informacji, a w szczególności twardych dysków z zapisanymi danymi osobowymi bez zgody Administratora Danych (AD).

3. W sytuacji przekazywania nośników z danymi osobowymi poza obszar Ministerstwa należy stosować następujące zasady bezpieczeństwa:

1) adresat powinien zostać powiadomiony o przesyłce;

2) nadawca powinien sporządzić kopię przesyłanych danych;

3) dane przed wysłaniem powinny zostać zaszyfrowane, a hasło podane adresatowi inną drogą;

4) przesyłka powinna być zabezpieczona przed uszkodzeniem;

5) nadawca powinien potwierdzić u adresata otrzymanie przesyłki.

4. Użytkownicy są zobowiązani do niezwłocznego i trwałego usuwania danych z nośników informacji po ustaniu konieczności ich przechowywania.

5. Podlegające likwidacji uszkodzone lub przestarzałe nośniki, a w szczególności twarde dyski z danymi osobowymi są komisyjnie niszczone w sposób fizyczny.

6. Nośniki informacji zamontowane jako elementy stacji roboczej lub innej infrastruktury informatycznej, w szczególności twarde dyski z danymi osobowymi, przed ich przekazaniem poza obszar Ministerstwa, powinny być wymontowane lub wyczyszczone z danych za pomocą specjalistycznego oprogramowania.

§ 26. Procedura przekazywania nośników do naprawy została określona w rozdziale VIII Instrukcji.

Rozdział 7.
OCHRONA SYSTEMU PRZED SZKODLIWYM OPROGRAMOWANIEM

§ 27. Procedura określa metody i środki zabezpieczenia zbiorów danych systemu informatycznego Ministerstwa, w tym zbiorów danych osobowych, przed szkodliwym oprogramowaniem oraz nieautoryzowanym dostępem.

§ 28. W celu zabezpieczenia systemu informatycznego Ministerstwa Administrator Systemu Informatycznego (ASI) zobowiązany jest do:

1) wdrożenia ochrony antywirusowej;

2) poprawnej konfiguracji i aktywowania oprogramowania monitorującego wymianę danych na styku poszczególnych warstw systemu informatycznego Ministerstwa;

3) poprawnej konfiguracji i zastosowania oprogramowania antywirusowego na stacjach roboczych użytkowników Ministerstwa. Ustawienie poziomu bezpieczeństwa i wysyłanie aktualizacji bazy sygnatur wirusów zarządzane jest centralnie;

4) podejmowania decyzji o ewentualnej instalacji na stacjach roboczych użytkowników dodatkowego, poza standardowego, oprogramowania systemowego lub użytkowego;

5) zapewnienia odpowiedniej ilości licencji oprogramowania w zakresie ochrony antywirusowej.

§ 29. 1. Program antywirusowy jest uaktywniony przez pełny czas pracy każdej stacji roboczej w systemie informatycznym Ministerstwa.

2. Wszystkie pliki, wprowadzane z zewnątrz do systemu informatycznego Ministerstwa, podlegają automatycznemu sprawdzeniu przez program antywirusowy pod kątem szkodliwego oprogramowania, z zastosowaniem najnowszej dostępnej wersji programu antywirusowego.

3. Niedozwolone jest wyłączanie, blokowanie i odinstalowywanie programów zabezpieczających stację roboczą przed szkodliwym oprogramowaniem oraz nieautoryzowanym dostępem.

§ 30. 1. W przypadku wykrycia szkodliwego oprogramowania, użytkownik zobowiązany jest zaprzestać pracy w systemie informatycznym Ministerstwa oraz natychmiast powiadomić o tym fakcie Administratora Systemu Informatycznego (ASI).

2. Po usunięciu szkodliwego oprogramowania Administrator Systemu Informatycznego (ASI) sprawdza działanie systemu informatycznego Ministerstwa pod kątem jego pełnej funkcjonalności i sprawności.

Rozdział 8.
PRZEGLĄDY, KONSERWACJA, NAPRAWY I UTYLIZACJA

§ 31. 1. Celem procedury jest zapewnienie ciągłości działania systemu informatycznego Ministerstwa.

2. Administrator Systemu Informatycznego (ASI) odpowiada za bezawaryjną pracę systemu informatycznego Ministerstwa.

§ 32. Nośniki zawierające dane osobowe, które uległy uszkodzeniu, można przekazać do naprawy pod warunkiem, że firma posiada autoryzację i wystawi stosowne oświadczenie o zapewnieniu poufności informacji, w przypadku ich pozyskania w trakcie naprawy.

§ 33. 1. Przeglądy i konserwacje sprzętu komputerowego dokonywane są przez Administratora Systemu Informatycznego (ASI) lub wyznaczonego przez niego Administratora Systemu.

2. Wszelkie prace związane z naprawami systemu informatycznego Ministerstwa są wykonywane przez Administratora Systemu Informatycznego (ASI) lub wyznaczonego przez niego Administratora Systemu.

3. Przeglądy i konserwacja systemu informatycznego Ministerstwa powinny być wykonywane w terminach określonych przez producentów lub zgodnie z harmonogramem przyjętym przez Administratora Systemu Informatycznego (ASI), jednak nie rzadziej, niż raz w roku.

4. Administrator Systemu Informatycznego (ASI) odpowiada za:

1) terminowość przeprowadzania przeglądów, konserwacji, napraw oraz ich prawidłowy przebieg,

2) optymalizację zasobów serwerowych, wielkość pamięci i dysków;

3) monitorowanie poprawności działania systemu informatycznego Ministerstwa;

4) identyfikację i przyjmowanie zgłoszeń o nieprawidłowościach w działaniu całości lub części systemu informatycznego Ministerstwa celem ich niezwłocznego usunięcia;

5) aktualizację oprogramowania zgodnie z zaleceniami producentów oraz opinią rynkową co do bezpieczeństwa i stabilności nowych wersji;

6) zapewnienie licencjonowanego oprogramowania do przetwarzania danych osobowych;

7) monitorowanie stanu istniejącej infrastruktury i zgłaszanie potrzeb jej modernizacji.

5. Wszelkie prace konserwacyjne i naprawcze sprzętu komputerowego oraz uaktualnienia całości lub części systemu informatycznego Ministerstwa, wykonywane przez podmiot zewnętrzny, powinny odbywać się na zasadach szczegółowo określonych w odrębnej umowie, z uwzględnieniem klauzuli dotyczącej ochrony danych osobowych.

6. Czynności konserwacyjne i naprawcze wykonywane doraźnie przez osoby nieposiadające upoważnień do przetwarzania danych, m.in. przez specjalistów z firm zewnętrznych, muszą być wykonywane pod nadzorem osób upoważnionych.

7. Przed przekazaniem do naprawy poza teren Ministerstwa uszkodzonego sprzętu komputerowego zawierającego dyski lub inne informatyczne nośniki informacji z danymi osobowymi, należy:

1) wymontować nośniki z danymi osobowymi;

2) trwale usunąć dane osobowe z użyciem specjalistycznego oprogramowania.

8. W przypadku braku możliwości usunięcia nośnika lub pozbawienia go zapisu danych osobowych naprawy dokonuje się pod nadzorem Administratora Systemu Informatycznego (ASI) lub wyznaczonego przez niego Administratora Systemu.

9. Przed przekazaniem do utylizacji sprzętu komputerowego należy wymontować, a następnie przekazać Administratorowi Systemu Informatycznego (ASI) dyski lub inne informatyczne nośniki informacji z danymi osobowymi.

10. Wymontowane dyski lub inne informatyczne nośniki informacji z danymi osobowymi przekazuje się firmie, która podpisała stosowne oświadczenie o zapewnieniu poufności informacji.

11. Proces utylizacji dysków lub innych informatycznych nośników informacji z danymi osobowymi należy przeprowadzić na podstawie odrębnego protokołu, podpisanego przez firmę wykonującą utylizację, zawierającego oświadczenie o nieodwracalnym zniszczeniu danych.

§ 34. Nieprawidłowości w działaniu całości lub części systemu informatycznego Ministerstwa są niezwłocznie usuwane przez Administratora Systemu Informatycznego (ASI), a ich przyczyny analizowane. Procedury postępowania w przypadku awarii lub innych nieprawidłowości w funkcjonowaniu systemu informatycznego Ministerstwa opisane są w § 44-46 Polityki.

§ 35. Zmiana konfiguracji sprzętu komputerowego, na którym znajdują się dane osobowe lub zmiana jego lokalizacji, może być dokonana wyłącznie za wiedzą Administratora Bezpieczeństwa Informacji (ABI).

§ 36. Zakres wykonywanych przeglądów i konserwacji sprzętu informatycznego obejmuje:

1) całość systemu informatycznego Ministerstwa, z wyjątkiem części objętych wyłączną obsługą serwisową producenta;
2) oprogramowanie systemowe, a także oprogramowanie biurowe w ogólnym zakresie;
3) wszystkie stacje robocze z wyjątkiem tych, objętych wyłączną gwarancją producenta, w których konserwacja ograniczona jest warunkami technicznymi;
4) sprzęt peryferyjny w zakresie ogólnego przeglądu, przy czym wszelkie czynności serwisowe wykonywane są poprzez specjalistyczne punkty serwisowe.

Rozdział 9.
POSTANOWIENIA KOŃCOWE

§ 37. 1. Do spraw nieuregulowanych w Instrukcji stosuje się przepisy o ochronie danych osobowych.

2. Instrukcja nie wyłącza stosowania innych procedur wewnętrznych dotyczących systemu informatycznego Ministerstwa.

§ 38. Integralną część Instrukcji stanowią następujące załączniki:

1) Załącznik nr 1 – Wzór rejestru kontroli stanowisk użytkowników;
2) Załącznik nr 2 – Wzór rejestru kopii zapasowych systemów informatycznych;
3) Załącznik nr 3 – Wzór rejestru kontroli stanu zabezpieczenia systemów informatycznych;
4) Załącznik nr 4 – Wzór rejestru zmiany haseł administracyjnych.

Załącznik nr 1do Instrukcji zarządzania
systemem informatycznym

WZÓR

Rejestr kontroli stanowisk użytkowników

Lp.	**Data przeprowadzenia kontroli**	**Nazwa kontrolowanego zbioru danych**	**Imię i nazwisko, stanowisko użytkownika, nazwa komputera**	**Stwierdzenie stanu zabezpieczenia systemu**	**Potwierdzenie kontroli (podpis użytkownika)**	**Potwierdzenie kontroli (podpis ASI)**	**Potwierdzenie kontroli (podpis ABI)**
1							
2							
3							

Załącznik nr 2 do Instrukcji zarządzania systemem informatycznym

WZÓR

Rejestr kopii zapasowych systemów informatycznych

Lp.	**Numer kopii**	**Nazwa rejestru**	**Data wykonania kopii**	**Podpis ASI**	**Podpis ABI**	**Uwagi**
1						
2						
3						

Załącznik nr 3 do Instrukcji zarządzania systemem informatycznym

WZÓR

Rejestr kontroli stanu zabezpieczenia systemów informatycznych

Lp.	**Nazwa urządzenia/systemu**	**Wykonane czynności**	**Stwierdzenie stanu zabezpieczenia (zabezpieczone/niezabezpieczone)**	**Zalecenia/wnioski**	**Podpis ASI**	**Podpis ABI**
1						
2						
3						

WZÓR

Rejestr zmiany haseł administracyjnych

Lp.	Informacja o systemie	Użytkownik	Data ostatniej zmiany hasła	Podpis ASI	Podpis ABI
1					
2					
3					