ZARZĄDZENIE Nr 76 MINISTRA ŚRODOWISKA[1)]

z dnia 13 grudnia 2010 r.

w sprawie dokumentacji przetwarzania danych osobowych w Ministerstwie Środowiska

Na podstawie art. 34 ust. 1 ustawy z dnia 8 sierpnia 1996 r. o Radzie Ministrów (Dz. U. z 2003 r. Nr 24, poz. 199, z późn. zm.[2)]), zarządza się, co następuje:

§ 1

W celu wykonania art. 36 ust. 1 ustawy z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (Dz. U. z 2002 r. Nr 101, poz. 926, z późn. zm.[3)]) oraz wdrożenia wymagań w zakresie przetwarzania danych osobowych określonych w rozporządzeniu 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), w Ministerstwie Środowiska wprowadza się do stosowania:

1) Politykę Bezpieczeństwa w zakresie przetwarzania danych osobowych w Ministerstwie Środowiska, stanowiącą załącznik nr 1 do zarządzenia;

2) Instrukcję zarządzania systemami informatycznymi służącymi do przetwarzania danych osobowych, stanowiącą załącznik nr 2 do zarządzenia.

§ 2

Traci moc zarządzenie Ministra Środowiska Nr 56 z dnia 7 maja 2008 r. w sprawie wprowadzenia zasad ochrony danych osobowych (Dz. Urz. MŚiGIOŚ Nr 4, poz. 79).

§ 3

Zarządzenie wchodzi w życie z dniem podpisania.

Minister Środowiska

Andrzej Kraszewski

[1)] Minister Środowiska kieruje działami administracji rządowej — środowisko i gospodarka wodna, na podstawie § 1 ust. 2 rozporządzenia Prezesa Rady Ministrów z dnia 16 listopada 2007 r. w sprawie szczegółowego zakresu działania Ministra Środowiska (Dz. U. Nr 216, poz. 1606).

[2)] Zmiany tekstu jednolitego wymienionej ustawy zostały ogłoszone w Dz. U. z 2003 r. Nr 80, poz. 717, z 2004 r. Nr 238, poz. 2390 i Nr 273, poz. 2703, z 2005 r. Nr 169, poz. 1414 i Nr 249, poz. 2104, z 2006 r. Nr 45, poz. 319, Nr 170, poz. 1217 i Nr 220, poz. 1600, z 2008 r. Nr 227, poz. 1505, z 2009 r. Nr 42, poz. 337, Nr 98, poz. 817, Nr 157, poz. 1241 i Nr 161, poz. 1277 oraz z 2010 r. Nr 57, poz. 354.

[3)] 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 oraz z 2010 r. Nr 41, poz. 233 i Nr 182, poz. 1228.

Załączniki do zarządzenia Nr 76 Ministra Środowiska z dnia 13 grudnia 2010 r. (poz. 81)

Załącznik nr 1

POLITYKA BEZPIECZEŃSTWA W ZAKRESIE PRZETWARZANIA DANYCH OSOBOWYCH W MINISTERSTWIE ŚRODOWISKA

I. POSTANOWIENIA OGÓLNE

§ 1

Celem wdrożenia Polityki Bezpieczeństwa w zakresie przetwarzania danych osobowych w Ministerstwie Środowiska, zwanej dalej „Polityką Bezpieczeństwa", jest uzyskanie optymalnego i zgodnego z wymogami obowiązujących aktów normatywnych, sposobu przetwarzania danych osobowych w Ministerstwie Środowiska.

§ 2

Obszar przetwarzania danych osobowych w Ministerstwie Środowiska stanowią wydzielone pomieszczenia budynku Ministerstwa usytuowanego w Warszawie przy ulicy Wawelskiej 52/54.

§ 3

Ilekroć w Polityce Bezpieczeństwa jest mowa o:

1) Ministerstwie — rozumie się przez to Ministerstwo Środowiska;

2) komórce organizacyjnej — rozumie się przez to odpowiednią komórkę organizacyjną, o której mowa w Statucie Ministerstwa Środowiska;

3) danych osobowych — rozumie się przez to wszelkie informacje dotyczące zidentyfikowanej lub możliwej do zidentyfikowania osoby fizycznej;

4) przetwarzaniu danych osobowych — rozumie się przez to jakiekolwiek operacje wykonywane na danych osobowych, takie jak: zbieranie, utrwalanie,

przechowywanie, opracowywanie, zmienianie, udostępnianie i usuwanie, zwłaszcza te, które wykonuje się w systemach informatycznych;

5) użytkowniku — rozumie się przez to osobę upoważnioną do przetwarzania danych osobowych;

6) Administratorze systemu informatycznego — rozumie się przez to osobę upoważnioną do zarządzania systemem informatycznym;

7) systemie informatycznym — rozumie się przez to zespół współpracujących ze sobą urządzeń, programów, procedur przetwarzania informacji i narzędzi programowych zastosowanych w celu przetwarzania danych osobowych;

8) zabezpieczeniu systemu informatycznego — rozumie się przez to wdrożenie i eksploatację stosowanych środków technicznych i organizacyjnych zapewniających ochronę danych osobowych przed modyfikacją, zniszczeniem, nieuprawnionym dostępem i ujawnieniem lub pozyskaniem danych, a także ich utratą;

9) poufności danych — rozumie się przez to właściwość zapewniającą, że dane osobowe nie są udostępnianie nieupoważnionym podmiotom;

10) integralności danych — rozumie się przez to właściwość zapewniającą, że dane osobowe nie zostały zmienione lub zniszczone w sposób nieautoryzowany;

11) dostępności danych — rozumie się przez to zapewnienie, że osoby upoważnione mają dostęp do danych osobowych i związanych z nimi zasobów wtedy, gdy jest to niezbędne;

12) zarządzaniu ryzykiem — rozumie się przez to proces identyfikowania, kontrolowania i minimalizowania lub eliminowania ryzyka dotyczącego bezpieczeństwa, które może dotyczyć systemów informacyjnych służących do przetwarzania danych osobowych.

II. DEFINICJA BEZPIECZEŃSTWA DANYCH

§ 4

1. Utrzymanie bezpieczeństwa danych osobowych przetwarzanych w Ministerstwie rozumiane jest jako zapewnienie ich poufności, integralności i dostępności na odpowiednim poziomie. Miarą bezpieczeństwa jest wielkość ryzyka związanego z ochroną danych osobowych.

2. Zarządzanie bezpieczeństwem danych osobowych wiąże się z zapewnieniem:

   1) niezaprzeczalności odbioru — rozumianej jako zdolność systemu do udowodnienia, że adresat informacji zawierającej dane osobowe otrzymał ją w określonym miejscu i czasie;

   2) niezaprzeczalności nadania — rozumianej jako zdolność systemu do udowodnienia, że nadawca informacji zawierającej dane osobowe faktycznie ją nadał lub wprowadził do systemu w określonym miejscu i czasie;

   3) rozliczalności działań — rozumianej, jako zapewnienie, że wszystkie działania istotne dla przetwarzania informacji zawierającej dane osobowe zostały zarejestrowane w systemie i możliwym jest zidentyfikowanie użytkownika, który działania dokonał.

III. ZAKRES STOSOWANIA

§ 5

1. W Ministerstwie przetwarzane są dane osobowe niezbędne do realizacji uprawnień lub spełnienia obowiązków wynikających z przepisów prawa.

2. Dane osobowe są przetwarzane zarówno w postaci dokumentacji tradycyjnej jak i elektronicznej.

§ 6

Politykę Bezpieczeństwa stosuje się do danych osobowych przetwarzanych w Ministerstwie, w tym w szczególności:

1) gromadzonych w związku z udzielaniem zamówień publicznych;

2) pracowników Ministerstwa;

3) kandydatów do pracy pozyskiwanych w procesie naboru;

4) sposobu ich zabezpieczenia, w tym nazw kont i haseł w systemach informatycznych służących do przetwarzania danych osobowych;

5) przetwarzanych w innych dokumentach zawierających dane osobowe.

§ 7

1. Zakres ochrony danych osobowych określony w Polityce Bezpieczeństwa ma zastosowanie do systemów informatycznych Ministerstwa, w których są przetwarzane dane osobowe, w szczególności do:

   1) istniejących, wdrażanych obecnie lub w przyszłości systemów informatycznych oraz papierowych, w których przetwarzane są dane osobowe;

   2) informacji będących własnością Ministerstwa lub osób występujących w realacjach prawnych z Ministerstwem;

   3) wszystkich lokalizacji — budynków i pomieszczeń, w których są lub będą przetwarzane dane osobowe;

   4) wszystkich pracowników w rozumieniu przepisów Kodeksu Pracy, konsultantów, stażystów i innych osób mających dostęp do danych osobowych.

2. Do stosowania zasad określonych w Polityce Bezpieczeństwa zobowiązani są wszyscy pracownicy w rozumieniu Kodeksu Pracy, konsultanci, stażyści oraz inne osoby mające dostęp do danych osobowych.

IV. DOSTĘP DO DANYCH

§ 8

1. Wszystkie osoby, których rodzaj wykonywanej pracy będzie wiązał się z dostępem do danych osobowych, przed przystąpieniem do pracy, podlegają przeszkoleniu w zakresie obowiązujących przepisów prawa dotyczących ochrony danych osobowych oraz obowiązujących w Ministerstwie zasad ochrony danych osobowych, po którym otrzymują upoważnienie do przetwarzania danych osobowych.

2. Upoważnienie do przetwarzania danych osobowych wydaje Administrator Bezpieczeństwa Informacji na wniosek dyrektora komórki organizacyjnej, zatrudniającej pracownika, któremu ma zostać wydane upoważnienie.

§ 9

Udostępnianie danych osobowych podmiotom upoważnionym do ich otrzymania na podstawie przepisów prawa powinno odbywać się według procedur postępowania określonych odrębnymi przepisami.

V. BEZPIECZEŃSTWO DANYCH

§ 10

W Ministerstwie stosuje się następujące środki techniczne i organizacyjne niezbędne do zapewnienia poufności, integralności i rozliczalności przetwarzanych danych osobowych:

1) zabezpieczenia fizyczne:
   a) całodobowy monitoring budynku Ministerstwa,
   b) system kart zbliżeniowych,
   c) pomieszczenia zamykane na klucz,
   d) szafy z zamkami,
   e) zabezpieczenie fizyczne przez pracowników ochrony;

2) zabezpieczenia procesów przetwarzania danych w dokumentacji papierowej:
   a) przetwarzanie danych osobowych następuje w wyznaczonych pomieszczeniach,
   b) przetwarzanie danych osobowych następuje przez wyznaczone do tego celu osoby,
   c) dokumenty zawierające dane osobowe zbędne do prowadzenia dalszych działań i które nie podlegają, archiwizacji są niezwłocznie niszczone w sposób uniemożliwiający ich odczytanie;

3) zabezpieczenia informatyczne określone w Instrukcji zarządzania systemami informatycznymi służącymi do przetwarzania danych osobowych w Ministerstwie;

4) zabezpieczenia organizacyjne:
   a) osobami bezpośrednio odpowiedzialnymi za bezpieczeństwo danych są: użytkownicy, lokalni administratorzy danych, Administrator systemu informatycznego, Administrator Bezpieczeństwa Informacji (ABI),
   b) Administrator Bezpieczeństwa Informacji, Administrator systemu informatycznego, lokalni administratorzy danych osobowych na bieżąco kontrolują z należytą starannością, zgodnie z aktualnie obowiązującą w tym zakresie wiedzą i z obowiązującymi procedurami, pracę pracowników odpowiedzialnych za przetwarzanie danych osobowych oraz systemów informatycznych służących do przetwarzania danych.

§ 11

Ochronę danych osobowych w Ministerstwie należy realizować z wykorzystaniem następujących minimalnych zabezpieczeń:

1) przyznawanie indywidualnych identyfikatorów;

2) zapewnienie stopniowania uprawnień;

3) zapewnienie wymuszania zmiany haseł;

4) odnotowanie daty pierwszego wprowadzenia danych w systemie;

5) odnotowanie identyfikatora użytkownika wprowadzającego dane;

6) odnotowanie sprzeciwu określonego w art. 32 ust. 1 pkt 8 ustawy z dnia 29 sierpnia 1997 r. o ochronie danych osobowych;

7) odnotowanie źródła danych, w przypadku zbierania danych nie od osoby, której dane dotyczą;

8) odnotowanie informacji o odbiorcach, którym dane zostały udostępnione, dacie i zakresie tego udostępnienia;

9) zapewnienie możliwości sporządzenia i wydrukowania raportu zawierającego dane osobowe wraz z informacjami o historii przetwarzania danych.

§ 12

1. W ramach zabezpieczenia danych osobowych, ochronie podlegają:
   1) sprzęt komputerowy — serwer, komputery osobiste, drukarki i inne urządzenia zewnętrzne;
   2) oprogramowanie — kody źródłowe, programy użytkowe, systemy operacyjne, narzędzia wspomagające i programy komunikacyjne;
   3) dane osobowe zapisane na dyskach oraz podlegające przetwarzaniu w systemach informatycznych;
   4) identyfikatory, hasła oraz inne elementy służące do uwierzytelniania użytkowników;
   5) pliki dziennych operacji systemowych i baz danych, kopie zapasowe i archiwa;
   6) dokumentacja — zawierająca dane systemu, opisująca w szczególności jego zastosowanie, przetwarzane informacje;

7) wydruki zawierające dane osobowe;

8) związana z przetwarzaniem danych osobowych dokumentacja papierowa, z której dane są wprowadzane do systemu informatycznego lub też funkcjonują niezależnie od niego.

VI. ZARZĄDZANIE DANYMI OSOBOWYMI

§ 13

Administratorem danych osobowych w Ministerstwie jest Minister Środowiska.

§ 14

1. Za bezpieczeństwo danych osobowych w Ministerstwie, odpowiadają:
   1) Administrator Danych Osobowych — Minister Środowiska;
   2) Administrator Bezpieczeństwa Informacji Ministerstwa Środowiska;
   3) lokalni administratorzy danych;
   4) Administrator systemu informatycznego;
   5) inne osoby zobowiązane do ochrony danych osobowych na podstawie odrębnych przepisów.
2. Administrator Bezpieczeństwa Informacji Ministerstwa realizując Politykę Bezpieczeństwa ma prawo wydawać zalecenia regulujące kwestie związane z ochroną danych osobowych w Ministerstwie.
3. W umowach zawieranych przez Ministerstwo winny znajdować się postanowienia zobowiązujące podmioty wchodzące w relacje prawne z Ministerstwem, do ochrony danych osobowych udostępnionych przez Ministerstwo w związku z realizacją powyższych umów.

§15

1. Obowiązki wynikające z przepisów o ochronie danych osobowych, o których mowa w § 19, Minister Środowiska powierza lokalnym administratorom danych — dyrektorom komórek organizacyjnych Ministerstwa — w zakresie podległych im pracowników, systemów informatycznych i posiadanych zbiorów danych osobowych.
2. Lokalny administrator danych odpowiada za realizację wymagań obowiązujących przepisów prawa o ochronie danych osobowych i jest zobowiązany do współdziałania z Administratorem Bezpieczeństwa Informacji w zakresie swojej właściwości.
3. Dyrektorzy komórek organizacyjnych Ministerstwa zobowiązani są do zapoznania podległych pracowników z treścią ustawy z dnia 29 sierpnia 1997 r. o ochronie danych osobowych, Polityką Bezpieczeństwa oraz Instrukcją zarządzania systemami informatycznymi służącymi do przetwarzania danych osobowych w Ministerstwie Środowiska.
4. Zapoznanie się z dokumentami określonymi w ust. 3 pracownicy Ministerstwa potwierdzają podpisem.
5. Przetwarzanie danych osobowych w Ministerstwie odbywa się z uwzględnieniem następujących reguł:
   1) ewidencja pracowników Ministerstwa upoważnionych do przetwarzania danych osobowych, jest prowadzona przez Administratora Bezpieczeństwa Informacji;
   2) do przetwarzania danych osobowych mogą zostać dopuszczeni wyłącznie:
      a) pracownicy, którzy zostali zapoznani z obowiązującymi zasadami ochrony danych osobowych, potwierdzili podpisem fakt przeszkolenia oraz posiadają upoważnienie przyznane przez Administratora Bezpieczeństwa Informacji,
      b) inne osoby, pod warunkiem zapoznania z obowiązującymi zasadami ochrony danych osobowych oraz posiadania upoważnienia przyznanego przez Administratora Bezpieczeństwa Informacji;
   3) w czasie przetwarzania danych osobowych, pracownik jest osobiście odpowiedzialny za bezpieczeństwo powierzonych mu danych osobowych;
   4) przed przystąpieniem do realizacji zadań związanych z przetwarzaniem danych osobowych, pracownik powinien sprawdzić, czy posiadane przez niego dane są należycie zabezpieczone;
   5) w czasie przetwarzania danych osobowych, pracownik powinien dbać o należyte ich zabezpieczenie przed możliwością wglądu, bądź zmiany przez osoby nieupoważnione;
   6) po zakończeniu przetwarzania danych osobowych pracownik powinien należycie zabezpieczyć dane osobowe przed możliwością dostępu do nich osób nieupoważnionych;
   7) pracownicy przetwarzający dane osobowe są nadzorowani przez lokalnych administratorów danych osobowych;
   8) przetwarzanie danych osobowych w Ministerstwie jest okresowo kontrolowane przez Administratora Bezpieczeństwa Informacji;
   9) zmiany oprogramowania, aktualizacja oprogramowania oraz jego zabezpieczenia antywirusowe i sieciowe dokonywane są przez Administratora systemu informatycznego.

VII. ZAKRESY ODPOWIEDZIALNOŚCI

§ 16

Za bezpieczeństwo danych osobowych odpowiedzialny jest każdy pracownik Ministerstwa w zakresie zajmowanego stanowiska i posiadanych danych.

§ 17

Administrator Bezpieczeństwa Informacji w Ministerstwie:

1) odpowiada za realizację zasad ochrony danych osobowych określonych postanowieniami ustawy z dnia 29 sierpnia 1997 r. o ochronie danych osobowych oraz Polityki Bezpieczeństwa;

2) wydaje, na podstawie umocowania Administratora Danych Osobowych, upoważnienia do przetwarzania danych osobowych w Ministerstwie (wzór upoważnienia stanowi załącznik do Polityki bezpieczeństwa);

3) prowadzi ewidencję osób upoważnionych do przetwarzania danych osobowych w Ministerstwie;

4) prowadzi wykaz zbiorów danych osobowych Ministerstwa Środowiska wraz ze wskazaniem programów zastosowanych do przetwarzania tych danych (przetwarzanych metodą tradycyjną lub w systemach informatycznych);

5) sprawuje nadzór nad fizycznym zabezpieczeniem pomieszczeń, w których dane są przetwarzane oraz kontrolą przebywających w nich osób;

6) identyfikuje i analizuje zagrożenia oraz ryzyko, na które narażone może być przetwarzanie danych osobowych w Ministerstwie;

7) określa, w porozumieniu z Administratorem systemu informatycznego, potrzeby w zakresie zabezpieczenia systemów informatycznych, w których przetwarzane są dane osobowe;

8) sprawuje nadzór nad obiegiem oraz przechowywaniem dokumentów i wydawnictw zawierających dane osobowe.

§ 18

1. Dyrektor komórki właściwej w sprawach kadr powiadamia Administratora Bezpieczeństwa Informacji o zamiarze wypowiedzenia umowy o pracę, lub ustaniu stosunku pracy z osobą zatrudnioną w Ministerstwie przy przetwarzaniu danych osobowych.

2. Administrator Bezpieczeństwa Informacji niezwłocznie powiadamia o okolicznościach określonych w ust. 1, osobę odpowiedzialną za nadawanie haseł i kodów dostępu do systemów informatycznych służących do przetwarzania danych osobowych. Kody dostępu i hasła są likwidowane w ciągu 24 godzin od ustania uprawnień lub zatrudnienia.

§ 19

1. Lokalni administratorzy danych osobowych zobowiązani są do przestrzegania przepisów o ochronie danych osobowych, w szczególności przez:

   1) określanie indywidualnych obowiązków i odpowiedzialności osób zatrudnionych przy przetwarzaniu danych osobowych;

   2) wykonywanie zaleceń Administratora Bezpieczeństwa Informacji w zakresie organizacyjnej i technicznej ochrony danych osobowych;

   3) wdrażanie i nadzorowanie przestrzegania postanowień Polityki Bezpieczeństwa oraz Instrukcji zarządzania systemami informatycznymi służącymi do przetwarzania danych osobowych w Ministerstwie;

   4) sprawowanie nadzoru nad naprawami, konserwacją oraz likwidacją urządzeń służących do przetwarzania danych osobowych;

   5) tworzenie warunków organizacyjnych i technicznych umożliwiających spełnienie wymogów wynikających z przepisów o ochronie danych osobowych;

   6) sprawowanie nadzoru nad poprawnością merytoryczną gromadzonych danych;

   7) przygotowanie projektów formularzy zgłoszenia do rejestracji zbiorów danych do Generalnego Inspektora Ochrony Danych Osobowych.

2. Lokalni administratorzy danych osobowych są nadzorowani pod względem stosowania zasad bezpieczeństwa przetwarzania danych osobowych przez Administratora Bezpieczeństwa Informacji.

§ 20

1. Administrator Systemu Informatycznego odpowiedzialny jest za:

   1) bieżący monitoring i zapewnienie ciągłości działania systemów informatycznych służących do przetwarzania danych osobowych;

   2) zapewnienie prowadzenia dla każdego systemu informatycznego służącego do przetwarzania danych osobowych dokumentacji zawierającej:

      a) opis struktury zbiorów danych osobowych przetwarzanych z użyciem tego systemu, wskazujący zawartość poszczególnych pól informacyjnych i powiązania między nimi,

      b) sposób przepływu danych osobowych pomiędzy poszczególnymi systemami informatycznymi służącymi do przetwarzania danych;

   3) konfigurację i administrowanie oprogramowaniem systemowym, sieciowym oraz bazodanowym zabezpieczającym dane osobowe przed nieupoważnionym dostępem;

   4) sprawowanie nadzoru nad zapewnieniem awaryjnego zasilania urządzeń służących do przechowywania danych osobowych;

   5) współpracę z dostawcami usług oraz sprzętu sieciowego i serwerowego oraz zapewnienie realizacji postanowień dotyczących ochrony danych osobowych;

   6) zarządzanie kopiami bezpieczeństwa zbiorów danych osobowych oraz zasobów umożliwiających ich przetwarzanie;

   7) przeciwdziałanie próbom naruszenia bezpieczeństwa danych osobowych przetwarzanych w systemach informatycznych;

   8) przyznawanie na wniosek lokalnego administratora danych, za zgodą Administratora Bezpieczeństwa Informacji określonych praw dostępu do danych osobowych przetwarzanych w danym systemie informatycznym (procedura przyznawania oraz wygaszania praw dostępu do danych osobowych przetwarzanych w systemie informatycznym oraz strategia zabezpieczania systemów informatycznych sporządzana jest przez Administratora systemu informatycznego);

   9) prowadzenie monitoringu działania zabezpieczeń wdrożonych w celu ochrony danych osobowych w systemach informatycznych;

10) sprawowanie nadzoru nad funkcjonowaniem mechanizmów uwierzytelniania użytkowników w systemach informatycznych służących do przetwarzania danych osobowych oraz kontrolą dostępu do danych;

11) wnioskowanie do Administratora Bezpieczeństwa Informacji w sprawie zmian lub usprawnienia procedur bezpieczeństwa i standardów zabezpieczeń;

12) prowadzenie ochrony antywirusowej.

2. Administrator systemu informatycznego jest nadzorowany pod względem przestrzegania przepisów o ochronie danych osobowych przez Administratora Bezpieczeństwa Informacji.

VIII. PRZETWARZANIE DANYCH OSOBOWYCH

§ 21

Systemy informatyczne służące do przetwarzania danych osobowych muszą spełniać wymogi obowiązujących aktów normatywnych regulujących zasady gromadzenia i przetwarzania danych osobowych.

§ 22

Kopie bezpieczeństwa oraz dokumenty papierowe zawierające dane osobowe przechowuje się w warunkach uniemożliwiających dostęp do nich osobom nieuprawnionym.

IX. ARCHIWIZOWANIE DOKUMENTÓW ZAWIERAJĄCYCH DANE OSOBOWE

§ 23

Archiwizację dokumentów zawierających dane osobowe prowadzi się w odpowiednio zabezpieczonych pomieszczeniach i na właściwie zabezpieczonych nośnikach informatycznych lub w postaci tradycyjnej. Dokumenty zawierające dane osobowe zbędne dla prowadzonych postępowań są natychmiast niszczone poprzez działania fizyczne i informatyczne uniemożliwiające ich odczytanie.

Załącznik nr 2

INSTRUKCJA ZARZĄDZANIA SYSTEMAMI INFORMATYCZNYMI SŁUŻĄCYMI DO PRZETWARZANIA DANYCH OSOBOWYCH W MINISTERSTWIE ŚRODOWISKA

I. POSTANOWIENIA OGÓLNE

§ 1

1. Instrukcja zarządzania systemami informatycznymi służącymi do przetwarzania danych osobowych w Ministerstwie Środowiska, zwana dalej „Instrukcją zarządzania", określa procedury zarządzania systemami informatycznymi Ministerstwa Środowiska zwanego dalej „Ministerstwem", służącymi do przetwarzania danych osobowych.

2. Instrukcja zarządzania pozwala stosować ujednolicone zasady ochrony danych osobowych w systemach i sieciach informatycznych Ministerstwa służących do przetwarzania danych osobowych.

3. Celem przyjęcia Instrukcji zarządzania jest podniesienie poziomu bezpieczeństwa systemów informatycznych, w których są przetwarzane dane osobowe oraz określenie odpowiedzialności pracowników Ministerstwa za prawidłowe działanie tych systemów i bezpieczeństwo przetwarzanych w nich danych osobowych.

§ 2

Instrukcja określa w szczególności:

1) procedury przydziału haseł dla użytkowników i częstotliwość ich zmiany, ze wskazaniem osoby odpowiedzialnej za te czynności;

2) procedury rejestrowania i wyrejestrowywania użytkowników oraz wskazanie osoby odpowiedzialnej za te czynności;

3) procedury rozpoczęcia i zakończenia pracy w systemach informatycznych;

4) opis metod oraz procedurę i harmonogram tworzenia kopii bezpieczeństwa;

5) opis metod i harmonogram sprawdzania obecności wirusów komputerowych;

6) procedurę i okres przechowywania elektronicznych nośników informacji i wydruków;

7) procedurę i harmonogram dokonywania przeglądów i konserwacji systemów informatycznych;

8) zasady wyposażania i eksploatacji stacji roboczych;

9) zasady wymiany danych osobowych w sieciach komputerowych.

§ 3

Ilekroć w Instrukcji zarządzania jest mowa o:

1) ustawie — rozumie się przez to ustawę z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (Dz. U. z 2002 r. Nr 101, poz. 926, z późn. zm.);

2) rozporządzeniu — rozumie się przez to rozporządzenie Ministra Spraw Wewnętrznych i Administracji z dnia 29 kwietnia 2004 r. w sprawie dokumentacji przetwarzania danych osobowych oraz warunków technicznych i organizacyjnych, jakim powinny odpowiadać urządzenia i systemy informatyczne służące do przetwarzania danych osobowych (Dz. U. z 2004 r. Nr 100, poz. 1024);

3) Ministerstwie — rozumie się przez to Ministerstwo Środowiska;

4) komórce organizacyjnej — rozumie się przez to odpowiednio komórki organizacyjne, o których mowa w Statucie Ministerstwa Środowiska;

5) naruszeniu bezpieczeństwa systemu informatycznego — rozumie się przez to jakiekolwiek naruszenie poufności, integralności, dostępności do systemu informatycznego spowodowane przez ludzi, jak też powstałe na skutek innych zdarzeń w szczególności oddziaływania sił przyrody;

6) Administratorze Danych Osobowych — rozumie się przez to Ministra Środowiska;

7) ABI — rozumie się przez to Administratora Bezpieczeństwa Informacji;

8) Administratorze systemu informatycznego — rozumie się przez to dyrektora komórki organizacyjnej Ministerstwa właściwej w sprawach informatyki lub jego zastępcę;

9) systemach informatycznych Ministerstwa Środowiska — rozumie się przez to zespół współpracujących ze sobą urządzeń, programów, procedur przetwarzania informacji i narzędzi programowych zastosowanych w celu przetwarzania danych osobowych;

10) przetwarzaniu danych — rozumie się przez to jakiekolwiek operacje wykonywane na danych, takie jak utrwalanie, przechowywanie, opracowywanie, zmienianie, udostępnianie, przekazywanie i usuwanie, a zwłaszcza te, które wykonuje się w systemach informatycznych;

11) obszarze przetwarzania danych — rozumie się przez to obiekty, pomieszczenia komórek organizacyjnych Ministerstwa, w których odbywa się przetwarzanie danych w układach elektronicznych na nośnikach magnetycznych, optycznych (również w postaci papierowej — kartoteki czy inne zbiory danych osobowych), urządzenia, elementy techniczne, z których charakteru pracy wynika przesyłanie danych na zewnątrz;

12) zabezpieczeniu danych osobowych w systemie Ministerstwa — rozumie się przez to wdrożenie i eksploatację stosownych środków technicznych i organizacyjnych zapewniających ochronę danych przed ich nieuprawnionym przetwarzaniem;

13) użytkowniku systemu — rozumie się przez to:

a) osobę zatrudnioną przy przetwarzaniu danych w Ministerstwie, która posiada upoważnienie do przetwarzania danych osobowych, a także osobę przetwarzającą dane osobowe w toku wykonywania umowy cywilnoprawnej zawartej z Ministerstwem (w szczególności umowy zlecenia, umowy o dzieło),

b) pracownika innego podmiotu, który świadczy usługi związane z dostępem do systemu informatycznego Ministerstwa, na podstawie odrębnych umów z tym podmiotem (w szczególności serwis, zlecenie przetwarzania danych).

§ 4

1. Ochrona danych osobowych przetwarzanych w Ministerstwie, przed ich nieuprawnionym użyciem lub zniszczeniem, jest obowiązkiem pracowników Ministerstwa.

2. Obowiązkiem pracowników Ministerstwa jest ponadto zachowanie tajemnicy służbowej, w tym ochrony danych osobowych przetwarzanych w Ministerstwie. Obowiązek ten istnieje również po ustaniu zatrudnienia.

3. Osoby zatrudnione przy przetwarzaniu danych osobowych (także poza systemami informatycznymi) są zobowiązane do szczególnej dbałości o zachowanie poufności, integralności i dostępności do danych osobowych gromadzonych w kartotekach, skorowidzach oraz infrastruktury sprzętowo — programowej systemu.

§ 5

Obowiązki wynikające z przepisów o ochronie danych osobowych Minister Środowiska powierza lokalnym administratorom danych osobowych — dyrektorom komórek organizacyjnych — w zakresie podległych im pracowników.

§ 6

1. Obszar przetwarzania danych osobowych w budynku Ministerstwa jest zorganizowany w sposób zapewniający dostęp do danych osobowych wyłącznie osobom uprawnionym.

2. Dopuszczalne odstępstwo stanowią pomieszczenia, w których przyjmowani są interesanci. Jeżeli pomieszczenia te wyposażone są jednocześnie w urządzenia z dostępem do systemów informatycznych służących do przetwarzania danych osobowych albo tradycyjne kartoteki, stosuje się w nich szczególne środki ostrożności, w tym:

1) interesanci powinni wchodzić pojedynczo i pozostawać w pomieszczeniu tylko w obecności użytkownika systemu;

2) kartoteki tradycyjne należy zabezpieczyć przed dostępem osób nieuprawnionych;

3) nie należy pozostawiać dokumentów papierowych i nośników elektronicznych w miejscach umożliwiających ich wykorzystanie przez osoby nieuprawnione;

4) monitory powinny być usytuowane tak, aby niemożliwy był wgląd w ekrany dla osób nieuprawnionych;

5) drukarki i urządzenia peryferyjne powinny być usytuowane tak, aby znajdowały się z dala od przestrzeni, po której poruszają się osoby nieuprawnione.

§ 7

Systemy informatyczne w Ministerstwie powinny być tak zaprojektowane, aby wymuszać autoryzację osoby przystępującej do pracy na zbiorach danych osobowych.

§ 8

Odpowiedzialność za ochronę danych osobowych przetwarzanych na urządzeniach przenośnych umożliwiających gromadzenie danych, spoczywa na dysponentach tych urządzeń. Minimalnym wymaganym zabezpieczeniem każdego komputera w Ministerstwie, jak również komputera przenośnego jest ograniczenie dostępu do tego komputera hasłem (hasło na BIOS, system operacyjny, wygaszasz ekranu).

§ 9

1. Dane osobowe przetwarzane na urządzeniach przenośnych mogą znajdować się na tych urządzeniach wyłącznie przez czas niezbędny do ich wykorzystania.

2. Po wykorzystaniu danych osobowych określonych w ust. 1 należy je niezwłocznie usunąć.

3. Danych osobowych określonych w ust. 1 nie można udostępniać osobom nieuprawnionym.

§ 10

1. Wszelkie informacje zawierające dane osobowe, udostępniane podmiotom zewnętrznym, mogą zostać przekazane tylko za pośrednictwem kancelarii ogólnej Ministerstwa.

2. W uzasadnionych przypadkach informacje zawierające dane osobowe mogą być przesyłane drogą elektroniczną w formie zaszyfrowanej.

§ 11

1. Zabrania się:
   1) notowania indywidualnych haseł dostępu;
   2) dokonywania przez osoby nieuprawnione napraw sprzętu informatycznego oraz modyfikowania oprogramowania;
   3) samodzielnego zakupu sprzętu komputerowego lub oprogramowania;
   4) autoryzacji w systemie informatycznym służącym do przetwarzania danych osobowych jako inny użytkownik;
   5) samodzielnego wgrywania oprogramowania;
   6) w celach innych niż służbowe, wynoszenia dokumentacji, w tym na nośnikach elektronicznych zawierającej dane osobowe, poza budynek Ministerstwa;
   7) instalowania na komputerach Ministerstwa prywatnych kont poczty elektronicznej;
   8) wykorzystywania Internetu do celów innych niż służbowe w szczególności przeglądania nielegalnych stron z kodami aktywacyjnymi do programów lub programami naruszającymi zabezpieczenia programów przed nielegalnym kopiowaniem.

2. Odwiedzanie stron internetowych jest nadzorowane przez pracowników komórki organizacyjnej Ministerstwa właściwej w sprawach informatyki.

3. Identyfikator i hasło osoby, która utraciła uprawnienia do korzystania z systemu podlegają bezzwłocznemu unieważnieniu.

4. Identyfikator osoby, która utraciła uprawnienia i została wyrejestrowana z systemu nie może być przydzielony innej osobie.

5. Dostęp do poszczególnych elementów systemów informatycznych służących do przetwarzania danych osobowych powinien być realizowany tylko w zakresie określonym nadanymi uprawnieniami, po wydaniu upoważnienia użytkownikowi.

II. PROCEDURY REJESTROWANIA I WYREJESTROWYWANIA UŻYTKOWNIKÓW

§ 12

1. Pracownika Ministerstwa korzystającego z systemu informatycznego służącego do przetwarzania danych osobowych i jego oprogramowania rejestruje się jako użytkownika.

2. Niedopuszczalna jest praca w systemie na koncie innego użytkownika.

§ 13

W celu zarejestrowania osoby jako użytkownika systemu informatycznego służącego do przetwarzania danych osobowych, dyrektor komórki organizacyjnej Ministerstwa, w której zatrudniona jest osoba, kieruje wniosek do Administratora sieci informatycznych, w którym określa:

1) konieczne uprawnienia (bądź zmianę, wycofanie uprawnień) ze szczególnym uwzględnieniem uprawnień do przetwarzania danych osobowych;

2) informację o przeszkoleniu użytkownika w zakresie ochrony danych osobowych.

§ 14

1. Administrator systemu informatycznego w porozumieniu z Administratorem Bezpieczeństwa Informacji nadaje, nadzoruje i wycofuje uprawnienia.

2. Nadawanie i rozszerzanie uprawnień użytkowników, w porozumieniu z lokalnym administratorem danych osobowych, koordynuje Administrator Bezpieczeństwa Informacji.

§ 15

1. Identyfikator użytkownika powinien spełniać następujące wymagania:
   1) długość minimum trzy znaki;
   2) niepowtarzalność w skali systemu.

2. Jednym identyfikatorem może posługiwać się tylko jeden użytkownik.

3. Identyfikator jest niezwłocznie blokowany przez administratora systemu po rozwiązaniu z pracownikiem umowy o pracę, po uzyskaniu takiej informacji od Administratora Bezpieczeństwa Informacji.

4. Identyfikator pracownika z którym rozwiązano umowę o pracę nie może zostać przydzielony innemu pracownikowi.

III. BUDOWA I PROCEDURA PRZYDZIAŁU HASEŁ DLA ADMINISTRATORÓW SYSTEMÓW I UŻYTKOWNIKÓW ORAZ CZĘSTOTLIWOŚĆ ICH ZMIANY

§ 16

1. Określa się następujące zasady tworzenia haseł:
   1) hasło składa się z nie mniej niż 6 znaków;

2) hasło powinno zawierać:

a) małe i duże litery,

b) cyfry,

c) znaki specjalne (! @ # $ % ^ & * () oraz znak kropki);

3) w haśle nie należy używać polskich znaków diakrytycznych lub innych znaków narodowych;

4) hasło nie powinno mieć charakteru słownikowego.

2. Hasło jest obowiązkowe dla każdego użytkownika posiadającego identyfikator w systemie.

3. Po przyznaniu hasła przez administratora użytkownik ma obowiązek zalogować się do systemu i zmienić hasło.

§ 17

Określa się następujące zasady korzystania z haseł:

1) hasło raz użyte może zostać wykorzystywane powtórnie po pięciu zmianach hasła;

2) hasło znane jest tylko użytkownikowi;

3) przy wpisywaniu hasła nie jest ono wyświetlane na ekranie;

4) użytkownik odpowiada za systematyczną zmianę haseł.

§ 18

Niedopuszczalne jest:

1) notowanie hasła;

2) podawanie hasła innym użytkownikom systemu, osobom nie uprawnionym do pracy w systemie lub nie posiadającym uprawnień do przetwarzania danych osobowych.

§ 19

Hasła w systemach informatycznych Ministerstwa zmienia się nie rzadziej niż raz na 30 dni.

§ 20

Hasło lokalnego administratora stacji roboczych pozostaje w wyłącznej dyspozycji Administratora sieci informatycznych lub wytypowanych przez niego i przeszkolonych pracowników komórki organizacyjnej Ministerstwa właściwej w sprawach informatyki.

§ 21

W Ministerstwie stosowane są mechanizmy wymuszania zmiany haseł.

IV. PROCEDURA ROZPOCZĘCIA I ZAKOŃCZENIA PRACY W SYSTEMIE INFORMATYCZNYM

§ 22

1. Użytkownik systemu informatycznego służącego do przetwarzania danych osobowych w Ministerstwie powinien zostać zarejestrowany przez Administratora systemu jako użytkownik odpowiedniej aplikacji.

2. Włączając komputer w celu podjęcia pracy użytkownik dokonuje autoryzacji zgodnie z poleceniami wydawanymi przez system komputerowy.

3. W razie pojawienia się trudności w autoryzacji, pomimo prawidłowo wykonanych czynności, użytkownik zobowiązany jest skontaktować się z Administratorem systemu informatycznego.

4. Jeżeli autoryzacja przebiegła prawidłowo, użytkownik dokonuje wyboru aplikacji, w której zamierza pracować.

§ 23

Obowiązkiem pracowników Ministerstwa jest dbałość o niepozostawianie stanowiska z dostępem do systemów informatycznych służących do przetwarzania danych osobowych, bez należytego zabezpieczenia, w tym:

1) opuszczając stanowisko pracy należy wylogować się z systemu.

2) w przypadku krótkotrwałych przerwach w pracy należy zablokować stację roboczą.

§ 24

Kończąc pracę w systemie, użytkownik zamyka wszystkie otwarte aplikacje, a następnie zamyka system.

V. OBSZARY PRZETWARZANIA DANYCH OSOBOWYCH

§ 25

Pomieszczenie, w którym przetwarzane są dane osobowe powinno spełniać następujące warunki:

1) wyposażenie w zamek mechaniczny lub elektroniczny zamykany każdorazowo, gdy opuszczają je pracownicy zatrudnieni przy przetwarzaniu danych;

2) jeżeli pomieszczenie znajduje się na parterze, lub istnieje możliwość podglądu z zewnątrz, ekrany monitorów umieszcza się w sposób uniemożliwiający podgląd;

3) monitory komputerów, na których przetwarzane są dane osobowe powinny być ustawione w sposób uniemożliwiający ich podgląd osobom nieuprawnionym.

§ 26

Wydzielona część pomieszczenia określona jako obszar przetwarzania danych powinna spełniać następujące warunki:

1) wyposażenie (meble) w tej części pomieszczenia powinno być ustawione w sposób uniemożliwiający lub istotnie utrudniający dostęp do tego obszaru osobom nieuprawnionym;

2) monitory komputerów, na których dokonuje się przetwarzania danych powinny być ustawione w sposób uniemożliwiający ich podgląd osobom nieuprawnionym.

§ 27

Nadzór nad przestrzeganiem zasad ochrony przetwarzania danych osobowych sprawuje Administrator Bezpieczeństwa Informacji.

VI. OPIS METOD I HARMONOGRAM SPORZĄDZANIA KOPII BEZPIECZEŃSTWA

§ 28

1. Administrator systemu informatycznego jest upoważniony do sporządzania kopii bezpieczeństwa plików aplikacji i zbiorów danych oraz systemów operacyjnych i ponosi odpowiedzialność w tym zakresie.
2. Z kopii bezpieczeństwa mogą być odtwarzane zbiory danych osobowych, uprawnienia użytkowników i ustawienia związane ze specyfiką i uwarunkowaniami systemów informatycznych służących do przetwarzania danych osobowych.
3. Odtwarzania dokonuje Administrator systemu informatycznego.

§ 29

1. Kopie bezpieczeństwa nie powinny być przechowywane w tym samym pomieszczeniu, w którym przechowywane są zbiory danych osobowych przetwarzane na bieżąco.
2. Dostęp do kopii bezpieczeństwa posiada Administrator systemu informatycznego, a w razie jego nieobecności Administrator Danych Osobowych lub Administrator Bezpieczeństwa Informacji.

§ 30

1. Co najmniej raz na kwartał Administrator systemu informatycznego dokonuje sprawdzenia zasobów kopii bezpieczeństwa pod kątem ich przydatności do odtworzenia danych osobowych w przypadku awarii systemu.
2. Kopie bezpieczeństwa, które uległy uszkodzeniu, lub zdezaktualizowały się, podlegają bezzwłocznemu zniszczeniu.

§ 31

Opisu czynności sporządzania, okresowego sprawdzania, niszczenia kopii bezpieczeństwa zbiorów danych osobowych zlokalizowanych poza systemem, jak też odtwarzania danych z tych kopii, dokumentuje się w „Dzienniku ewidencji kopii bezpieczeństwa", który przechowywany jest w komórce organizacyjnej Ministerstwa właściwej w sprawach informatyki.

§ 32

Nadzór nad procesem sporządzania, przechowywania i niszczenia kopii bezpieczeństwa sprawuje Administrator Bezpieczeństwa Informacji.

§ 33

1. Kopia systemu operacyjnego powinna być wykonywana po każdej modyfikacji, zmianie, konfiguracji i instalacji nowej wersji oprogramowania w sposób właściwy dla danego systemu operacyjnego.
2. Gromadzeniu podlegają dwie ostatnio wykonane kopie.

§ 34

1. Pełna kopia zabezpieczająca zbiory danych osobowych przetwarzanych w systemach informatycznych wykonywana jest co najmniej raz w tygodniu.
2. Każda kopia powinna zostać opisana w sposób zapewniający następujące informacje:
   1) data wykonania;
   2) nazwa systemu informatycznego;
   3) nazwa zbioru danych.

VII. OPIS METOD ORAZ HARMONOGRAM SPRAWDZANIA OBECNOŚCI WIRUSÓW I ICH USUWANIE

§ 35

1. Bieżące sprawdzanie obecności wirusów komputerowych realizuje się przez stosowanie oprogramowania monitorującego występowanie wirusów.
2. Sprawdzaniu obecności wirusów podlegają wszystkie informatyczne nośniki danych.
3. Administrator systemu informatycznego zobowiązany jest do zapewnienia systematycznej aktualizacji oprogramowania antywirusowego.
4. Sprawdzanie obecności wirusów na dyskach stacji roboczej odbywa się automatycznie po uruchomieniu komputera.

§ 36

1. O wykryciu wirusa na stacji roboczej użytkownik powiadamia Administratora systemu informatycznego.
2. W przypadku problemów z usunięciem wirusa ze stacji roboczej użytkownik nie podejmuje dalszych działań do czasu przybycia Administratora systemu informatycznego.

§ 37

Po dokonanej naprawie lub konserwacji Administrator systemu informatycznego zobowiązany jest do przeprowadzenia procesu sprawdzenia pod kątem występowania wirusów.

§ 38

Nadzór nad prawidłowym funkcjonowaniem oprogramowania antywirusowego sprawuje Administrator systemu informatycznego.

VIII. OGÓLNE ZASADY I ODPOWIEDZIALNOŚĆ PRZY INSTALACJI OPROGRAMOWANIA

§ 39

1. Administrator systemu informatycznego zobowiązany jest prowadzić „Dziennik czynności technologicznych serwera". W dzienniku tym opisuje się wszystkie czynności podejmowane w ramach jego administrowania (takie jak instalacja lub modyfikacja oprogramowania), w szczególności związane z bezpieczeństwem danych osobowych.

2. Do instalacji i modyfikacji oprogramowania na serwerach uprawniony jest wyłącznie Administrator systemu informatycznego.
3. W Ministerstwie może być instalowane tylko oprogramowanie, na które Ministerstwo posiada licencję.
4. Oprogramowanie testowe może być instalowane wyłącznie na wydzielonym serwerze lub systemie informatycznym.
5. Oprogramowanie testowe odinstalowuje się bezzwłocznie po zakończeniu testowania.
6. Podczas prowadzenia testów oprogramowania, praca systemu jest na bieżąco monitorowana przez Administratora systemu informatycznego.

§ 40

Zabrania się użytkownikom dokonywania samodzielnej instalacji jakiegokolwiek oprogramowania. Instalacji oprogramowania dokonują wyłącznie pracownicy komórki organizacyjnej Ministerstwa właściwej w sprawach informatyki.

§ 41

Na komputerach używanych w Ministerstwie dopuszcza się instalację tylko legalnego, licencjonowanego oprogramowania.

§ 42

Wprowadza się następujące zasady korzystania z oprogramowania:

1) oryginalne dokumenty licencyjne oraz nośniki każdego oprogramowania przechowywane są w komórce organizacyjnej Ministerstwa właściwej w sprawach informatyki; nośniki oprogramowania nie mogą znajdować się w żadnym innym miejscu, a szczególnie nie mogą być kopiowane, wypożyczane lub w żaden sposób przekazywane osobom trzecim (dotyczy to również kodów aktywacyjnych produktów);
2) pracownicy Ministerstwa zobowiązani są do pracy na legalnym oprogramowaniu oraz nie są uprawnieni do instalacji i użytkowania oprogramowania pochodzącego ze źródeł innych niż komórka organizacyjna Ministerstwa właściwa w sprawach informatyki;
3) do podstawowych obowiązków pracownika należy korzystanie z oprogramowania w związku z wykonywaniem obowiązków pracowniczych, zgodnie z obowiązującymi przepisami prawa oraz wyłącznie w celach wykonywania tych obowiązków; zabrania się korzystania z jakiegokolwiek oprogramowania, do którego Ministerstwo nie jest uprawnione, w czasie pracy, w miejscu pracy i przy użyciu sprzętu Ministerstwa.

IX. PROCEDURA I OKRES PRZECHOWYWANIA NOŚNIKÓW INFORMACJI, W TYM KOPII ELEKTRONICZNYCH WYDRUKÓW

§ 43

1. Nośniki informacji, w tym kopie elektroniczne i wydruki zawierające dane osobowe przechowuje się w sposób zapewniający dostęp wyłącznie osobom uprawnionym.
2. Dane osobowe zgromadzone na magnetycznych nośnikach informacji usuwa się bezzwłocznie po ich wykorzystaniu, w sposób trwały.
3. Zabrania się sporządzania kopii zbiorów danych na dyskach twardych stacji roboczych lub w folderach ogólnodostępnych w systemach informatycznych Ministerstwa.

§ 44

1. Użytkownik dokonujący wydruku na drukarce sieciowej, zobowiązany jest udać się niezwłocznie do pomieszczenia usytuowania drukarki w celu odbioru wydrukowanego dokumentu.
2. Kopie błędne, nadmiarowe czy z innych powodów niepotrzebne należy niezwłocznie zniszczyć.
3. Wydruki, które nie podlegają archiwizacji należy niezwłocznie zniszczyć.
4. Każdy pracownik, który znajdzie wydruk, nośnik elektroniczny, czy inny dokument zawierający dane osobowe pozostawiony bez dozoru jest obowiązany do jego zabezpieczenia oraz poinformowania Administratora Bezpieczeństwa Informacji.

§ 45

Wydruki zawierające dane osobowe podlegają szczególnej ochronie, polegającej w szczególności na:

1) zakazie pozostawiania wydruków z możliwością dostępu do nich osób nieuprawnionych;
2) obowiązku poddawania zniszczeniu nieudanych lub próbnych wydruków.

X. PROCEDURA I HARMONOGRAM DOKONYWANIA PRZEGLĄDÓW I KONSERWACJI SYSTEMÓW ORAZ ZBIORÓW DANYCH

§ 46

Przeglądu i konserwacji systemów informatycznych służących do przetwarzania danych osobowych w Ministerstwie dokonuje Administrator systemu informatycznego.

§ 47

1. Przegląd systemu polega na sprawdzeniu jego konfiguracji, sprawdzeniu logo systemowych, ze szczególnym uwzględnieniem logo bezpieczeństwa oraz poczynieniu odpowiedniej adnotacji w „Dzienniku czynności technologicznych serwera".
2. Przeglądu systemu dokonuje się codziennie (prócz dni wolnych od pracy).
3. W przypadku stwierdzenia nieprawidłowości w systemie, Administrator systemu informatycznego usuwa je, wykorzystując dostępne narzędzia i odnotowuje ten fakt w „Dzienniku czynności technologicznych serwera".

XI. ZASADY WYPOSAŻANIA I EKSPLOATACJI STACJI ROBOCZYCH

§ 48

1. Zasadność zakupu sprzętu komputerowego oraz oprogramowania podlega ocenie i akceptacji przez dyrektora komórki organizacyjnej Ministerstwa właściwej w sprawach informatyki.

2. Przygotowanie, w tym skonfigurowanie oraz instalacja sprzętu komputerowego na stanowiskach pracy wykonywana jest przez pracowników komórki organizacyjnej Ministerstwa właściwej w sprawach informatyki lub inne osoby nadzorowane przez tych pracowników.

3. Przeniesienie sprzętu do innych pomieszczeń wykonywane jest przez pracowników komórki organizacyjnej Ministerstwa właściwej w sprawach informatyki lub inne osoby nadzorowane przez tych pracowników, na wniosek dyrektora komórki organizacyjnej. Zabrania się samodzielnego przenoszenia sprzętu przez innych pracowników.

4. Zmiana osoby odpowiedzialnej za powierzony sprzęt zgłaszana jest przez dyrektora komórki organizacyjnej pracownikom komórki organizacyjnej Ministerstwa właściwej w sprawach informatyki.

XII. ZASADY WYMIANY INFORMACJI W SIECI KOMPUTEROWEJ

§ 49

1. Użytkownicy systemów informatycznych służących do przetwarzania danych osobowych w Ministerstwie zobowiązani są do prawidłowego rozpoczęcia i zakończenia pracy w systemie.

2. Systemy informatyczne służące do przetwarzania danych osobowych w Ministerstwie powinny być przygotowane do przekazywania informacji zawierających dane osobowe pomiędzy poszczególnymi komórkami organizacyjnymi i uprawnionymi podmiotami zewnętrznymi za pośrednictwem poczty elektronicznej z obowiązkiem szyfrowania.

3. Zabrania się wykorzystywania poczty elektronicznej do przekazywania dokumentów zawierających dane osobowe, bez odpowiedniego sposobu zaszyfrowania.

XIII. POSTANOWIENIA KOŃCOWE

§ 50

Przestrzeganie postanowień niniejszej Instrukcji zarządzania przez użytkowników systemów stanowi podstawę bezpiecznego posługiwania się systemami informatycznymi służącymi do przetwarzania danych osobowych w Ministerstwie.

§ 51

Administrator Bezpieczeństwa Informacji okresowo monitoruje przestrzeganie przez pracowników Ministerstwa zasad i przepisów w zakresie ochrony danych osobowych.