ZARZĄDZENIE NR 49

MINISTRA TRANSPORTU, BUDOWNICTWA I GOSPODARKI MORSKIEJ

z dnia 19 lipca 2012 r.

w sprawie ochrony danych osobowych przetwarzanych w Ministerstwie Transportu, Budownictwa i Gospodarki Morskiej

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.[1)]), w związku z § 3 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.

W Ministerstwie Transportu, Budownictwa i Gospodarki Morskiej wprowadza się do stosowania:

1) „Politykę bezpieczeństwa w zakresie ochrony danych osobowych w Ministerstwie Transportu, Budownictwa i Gospodarki Morskiej", stanowiącą załącznik Nr 1 do zarządzenia;

2) „Instrukcję zarządzania systemem informatycznym służącym do przetwarzania danych osobowych w Ministerstwie Transportu, Budownictwa i Gospodarki Morskiej", stanowiącą załącznik Nr 2 do zarządzenia.

§ 2.

Traci moc zarządzenie Nr 11 Ministra Infrastruktury z dnia 9 kwietnia 2009 r. w sprawie ochrony danych osobowych przetwarzanych w Ministerstwie Infrastruktury zmienione zarządzeniem Nr 32 Ministra Infrastruktury z dnia 9 sierpnia 2010 r. zmieniającym

---

[1)] 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.

zarządzenie w sprawie ochrony danych osobowych przetwarzanych w Ministerstwie Infrastruktury oraz zarządzeniem Nr 41 Ministra Infrastruktury z dnia 12 października 2011 r. zmieniającym zarządzenie w sprawie ochrony danych osobowych przetwarzanych w Ministerstwie Infrastruktury.

§ 3.

Zachowują moc upoważnienia do przetwarzania danych osobowych oraz wyznaczenia do pełnienia funkcji Administratora Systemu Informatycznego, wydane na podstawie dotychczas obowiązujących przepisów.

§ 4.

Zarządzenie wchodzi w życie z dniem ogłoszenia.

MINISTER
TRANSPORTU, BUDOWNICTWA
I GOSPODARKI MORSKIEJ

S. Nowak

Załącznik Nr 1
do zarządzenia Nr 49
Ministra Transportu, Budownictwa
i Gospodarki Morskiej
z dnia 19 lipca 2012 r. (poz. 49)

Polityka bezpieczeństwa w zakresie ochrony danych osobowych w Ministerstwie Transportu, Budownictwa i Gospodarki Morskiej

Postanowienia ogólne

§ 1.

Polityka bezpieczeństwa w zakresie ochrony danych osobowych w Ministerstwie Transportu, Budownictwa i Gospodarki Morskiej, zwanym dalej „Ministerstwem", określa zasady przetwarzania danych osobowych oraz środki techniczne i organizacyjne zastosowane dla zapewnienia poufności, integralności i rozliczalności przetwarzanych danych osobowych.

§ 2.

1. Polityka bezpieczeństwa w zakresie ochrony danych osobowych w Ministerstwie, zwana dalej „Polityką bezpieczeństwa", służy zapewnieniu wysokiego poziomu bezpieczeństwa przetwarzania danych.
2. Polityka bezpieczeństwa dotyczy danych osobowych przetwarzanych w zbiorach manualnych oraz w systemach informatycznych.

§ 3.

1. Administratorem danych osobowych w Ministerstwie jest:
   1) Minister Transportu, Budownictwa i Gospodarki Morskiej – w zakresie danych osobowych przetwarzanych w związku z realizacją ustawowych zadań organu administracji rządowej;
   2) Dyrektor Generalny Ministerstwa – w odniesieniu do zbiorów danych przetwarzanych w związku z zatrudnieniem, odbywaniem staży i praktyk w Ministerstwie oraz funkcjonowaniem Ministerstwa.
2. Administrator danych osobowych decyduje o celach i środkach przetwarzania danych osobowych zgodnie z przepisami ustawy z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (Dz. U. z 2002 r. Nr 101, poz. 926, z późn. zm.[1)]), zwanej dalej „ustawą".
3. Administrator danych osobowych może wyznaczyć, spośród pracowników Ministerstwa posiadających przeszkolenie w zakresie przepisów o ochronie danych osobowych, Administratora bezpieczeństwa informacji, zwanego dalej „ABI", do którego zadań należy nadzór nad przestrzeganiem zasad ochrony danych osobowych, zgodnie z

[1)] Zmiany 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.

przepisami ustawy. Administrator danych osobowych upoważnia ABI do przetwarzania danych osobowych w zbiorach danych przetwarzanych w Ministerstwie. Wzór wyznaczenia do pełnienia funkcji ABI określa załącznik Nr 1 do Polityki bezpieczeństwa. Wzór upoważnienia ABI do przetwarzania danych osobowych określa załącznik Nr 2 do Polityki bezpieczeństwa.

4. Administratorem systemu informatycznego, zwanym dalej „ASI", jest wyznaczony przez Administratora danych osobowych pracownik Ministerstwa odpowiedzialny za bezpieczeństwo danych osobowych przetwarzanych w systemie informatycznym. Wzór wyznaczenia do pełnienia funkcji ASI określa załącznik Nr 3 do Polityki bezpieczeństwa.
5. Zadania ABI, jeśli został ustanowiony, oraz ASI określa załącznik Nr 4 do Polityki bezpieczeństwa.

Zasady przetwarzania danych osobowych

§ 4.

1. Przetwarzaniem danych osobowych jest zbieranie, utrwalanie, przechowywanie, opracowywanie, zmiana, udostępnianie i usuwanie wszelkich informacji dotyczących zidentyfikowanej lub możliwej do zidentyfikowania osoby fizycznej.
2. Dopuszcza się przetwarzanie danych osobowych wyłącznie w zakresie i trybie określonym ustawą, niniejszą Polityką bezpieczeństwa oraz Instrukcją zarządzania systemem informatycznym służącym do przetwarzania danych osobowych w Ministerstwie, zwaną dalej „Instrukcją zarządzania systemem informatycznym".

§ 5.

1. Do przetwarzania danych dopuszczone są wyłącznie osoby przeszkolone w zakresie zasad przetwarzania danych osobowych oraz posiadające upoważnienie nadane przez Administratora danych osobowych.
2. Upoważnienie określa w szczególności:
   1) nazwę zbioru danych osobowych;
   2) zakres przetwarzania danych.
3. Wzór upoważnienia, o którym mowa w ust. 1, określa załącznik Nr 5 do Polityki bezpieczeństwa.
4. Ewidencję osób upoważnionych do przetwarzania danych osobowych, zgodnie ze wzorem określonym w załączniku Nr 6 do Polityki bezpieczeństwa, prowadzi ABI, a w przypadku gdy ABI nie został wyznaczony – Biuro Dyrektora Generalnego w Ministerstwie. Ewidencja jest dostępna na wewnętrznym portalu intranetowym Ministerstwa.
5. Upoważnienia do przetwarzania danych osobowych rejestrowane są w ewidencji, o której mowa w ust. 4.

§ 6.

Przetwarzanie danych może zostać powierzone innemu podmiotowi na podstawie umowy, o której mowa w art. 31 ustawy.

Wykaz budynków, pomieszczeń lub części pomieszczeń, tworzących obszar, w którym przetwarzane są dane osobowe

§ 7.

1. Przetwarzanie danych osobowych odbywa się w Warszawie w budynkach przy ul. Chałubińskiego 4/6 (budynki A, B i C), przy ul. Wspólnej 2/4, przy ul. Kruczej 38/42 oraz przy ul. Karczunkowskiej 30.
2. Wykaz budynków, pomieszczeń lub części pomieszczeń, w których przetwarzane są dane osobowe w Ministerstwie, zgodnie ze wzorem określonym w załączniku Nr 7 do Polityki bezpieczeństwa, prowadzi ABI, a w przypadku gdy ABI nie został wyznaczony – Biuro Dyrektora Generalnego w Ministerstwie.
3. Wykaz budynków, pomieszczeń lub części pomieszczeń, w których przetwarzane są dane osobowe w Ministerstwie dostępny jest na wewnętrznym portalu intranetowym Ministerstwa.

Wykaz zbiorów danych osobowych

§ 8.

1. Wykaz zbiorów danych osobowych w Ministerstwie wraz ze wskazaniem:
   1) Administratora danych osobowych;
   2) podstawy prawnej prowadzenia danego zbioru;
   3) programów zastosowanych do przetwarzania tych danych,

   - zgodnie ze wzorem określonym w załączniku Nr 7 do Polityki bezpieczeństwa, prowadzi ABI, a w przypadku gdy ABI nie został wyznaczony – Biuro Dyrektora Generalnego w Ministerstwie.
2. Wykaz zbiorów danych osobowych w Ministerstwie jest dostępny jest na wewnętrznym portalu intranetowym Ministerstwa.
3. Opis struktury zbiorów danych osobowych, wskazujący zawartość poszczególnych pól informacyjnych i powiązania między nimi oraz sposób przepływu danych pomiędzy poszczególnymi systemami, zgodnie ze wzorem określonym w załączniku Nr 8 do Polityki bezpieczeństwa, prowadzi ABI, a w przypadku gdy ABI nie został wyznaczony – Biuro Dyrektora Generalnego w Ministerstwie.
4. Struktura zbiorów danych, sposób przepływu danych w systemie i zakres przetwarzania danych dostępne są na wewnętrznym portalu intranetowym Ministerstwa.

Środki ochrony danych osobowych

§ 9.

W celu zapewnienia poufności, integralności i rozliczalności przetwarzanych w Ministerstwie danych osobowych stosuje się:

1) środki techniczne;
2) środki organizacyjne

- określone w załączniku Nr 9 do Polityki bezpieczeństwa.

§ 10.

Obowiązanymi do stosowania zasad przetwarzania danych osobowych są osoby, które przetwarzają dane osobowe w zbiorach określonych w Wykazie zbiorów danych osobowych w Ministerstwie.

Załączniki do Polityki bezpieczeństwa
w zakresie ochrony danych osobowych
w Ministerstwie Transportu, Budownictwa
i Gospodarki Morskiej

Załącznik Nr 1

**MINISTERSTWO
TRANSPORTU, BUDOWNICTWA
I GOSPODARKI MORSKIEJ**

Warszawa, dnia ……20….. r.

WZÓR

Wyznaczenie do pełnienia funkcji Administratora Bezpieczeństwa Informacji

Działając na podstawie art. 36 ust. 3 ustawy z dnia 29 sierpnia 1997 r. o ochronie danych osobowych

wyznaczam Panią/Pana:

…….
(imię, nazwisko, stanowisko)

do pełnienia funkcji:

Administratora Bezpieczeństwa Informacji

…….
(pieczęć i podpis Administratora Danych Osobowych)

Przyjęłam/Przyjąłem:

…… (miejscowość i data)

……. (podpis osoby wyznaczonej do pełnienia funkcji Administratora Bezpieczeństwa Informacji)

Wyznaczenie sporządza się w dwóch egzemplarzach, z których jeden otrzymuje ABI, drugi zaś załącza się do akt osobowych pracownika.

Załącznik Nr 2

MINISTERSTWO TRANSPORTU, BUDOWNICTWA I GOSPODARKI MORSKIEJ

Warszawa, dnia ……20….. r.

WZÓR

UPOWAŻNIENIE DO PRZETWARZANIA DANYCH OSOBOWYCH[1)]

Działając na podstawie art. 37 ustawy z dnia 29 sierpnia 1997 r. o ochronie danych osobowych

upoważniam Panią/Pana:

…….
(imię, nazwisko, stanowisko)

wyznaczoną/ego do pełnienia funkcji

Administratora Bezpieczeństwa Informacji

do przetwarzania danych osobowych w zbiorach określonych w Wykazie zbiorów danych osobowych w Ministerstwie Transportu, Budownictwa i Gospodarki Morskiej, dla których Administratorem Danych Osobowych jest[2)]……..…

Upoważnienie jest udzielone na czas pełnienia obowiązków Administratora Bezpieczeństwa Informacji, w zakresie niezbędnym do sprawowania ww. funkcji.

…….
(pieczęć i podpis Administratora Danych Osobowych)

Oświadczam, że zapoznałam/em się z Polityką bezpieczeństwa w zakresie ochrony danych osobowych w Ministerstwie Transportu, Budownictwa i Gospodarki Morskiej oraz Instrukcją zarządzania systemem informatycznym służącym do przetwarzania danych osobowych w Ministerstwie Transportu, Budownictwa i Gospodarki Morskiej.
Zobowiązuję się do przestrzegania zasad przetwarzania danych osobowych określonych w ww. dokumentach oraz nieujawniania informacji zawartych w tych dokumentach, a także danych osobowych, z którymi zapoznam się w trakcie wykonywania obowiązków służbowych. Powyższe informacje zobowiązuję się zachować w tajemnicy przez cały okres zatrudnienia, a także po jego ustaniu.
Oświadczam, że jestem świadoma/my odpowiedzialności karnej, wynikającej z art. 51 – 54a ustawy o ochronie danych osobowych oraz art. 266 Kodeksu karnego.

Przyjęłam/Przyjąłem:

…… ……
(miejscowość i data) (czytelny podpis osoby upoważnionej)

[1)] Upoważnienie dla Administratora Bezpieczeństwa Informacji;
[2)] Należy wpisać właściwego administratora danych (Minister Transportu, Budownictwa i Gospodarki Morskiej lub Dyrektor Generalny Ministerstwa Transportu, Budownictwa i Gospodarki Morskiej).
Upoważnienie sporządza się w dwóch egzemplarzach, z których jeden otrzymuje ABI, drugi zaś załącza się do akt osobowych pracownika.

Załącznik Nr 3

MINISTERSTWO
TRANSPORTU, BUDOWNICTWA
I GOSPODARKI MORSKIEJ

Warszawa, dnia ……20….. r.

WZÓR

Wyznaczenie do pełnienia funkcji Administratora Systemu Informatycznego

Działając na podstawie § 3 ust. 4 Polityki bezpieczeństwa w zakresie ochrony danych osobowych w Ministerstwie Transportu Budownictwa i Gospodarki Morskiej

wyznaczam Panią/Pana:

…….
(imię, nazwisko, stanowisko)

do pełnienia funkcji:

Administratora Systemu Informatycznego

…….
(nazwa zbioru)

Na czas …….

…….
(pieczęć i podpis Administratora Danych Osobowych)

Uzgadniam:

……
(pieczęć i podpis Dyrektora Biura Zarządzania Kryzysowego i Ochrony Informacji Niejawnych)

Przyjęłam/Przyjąłem:

…… (miejscowość i data)

……
(podpis osoby wyznaczonej do pełnienia funkcji Administratora Systemu Informatycznego)

Wyznaczenie sporządza się w trzech egzemplarzach, z których jeden otrzymuje upoważniony, drugi załącza się do akt osobowych pracownika, trzeci otrzymuje ABI.

Załącznik Nr 4

Zadania ABI, ASI, osoby upoważnionej do przetwarzania danych osobowych oraz dyrektora komórki organizacyjnej, w której przetwarzane są dane osobowe

Do zadań **ABI** należy w szczególności:

1) analiza zagrożeń i ryzyk związanych z przetwarzaniem danych osobowych;
2) analiza i w miarę potrzeby aktualizacja dokumentacji w zakresie ochrony danych osobowych;
3) zgłaszanie zbiorów danych osobowych Generalnemu Inspektorowi Ochrony Danych Osobowych oraz zmian dotyczących zarejestrowanych zbiorów, zgodnie z wymogami ustawy;
4) udzielanie upoważnień do przetwarzania danych osobowych;
5) prowadzenie ewidencji osób upoważnionych do przetwarzania danych osobowych;
6) monitorowanie środków ochrony danych osobowych określonych w Polityce bezpieczeństwa, w celu potwierdzenia ich adekwatności;
7) organizowanie i prowadzenie szkoleń dla osób upoważnionych do przetwarzania danych osobowych w Ministerstwie;
8) organizowanie i prowadzenie kontroli przetwarzania danych osobowych w Ministerstwie;
9) przygotowanie procedury określającej sposób postępowania w zakresie realizacji zadań wynikających z ustawy o ochronie danych osobowych i zamieszczenie jej na wewnętrznym portalu intranetowym Ministerstwa;
10) nadzór nad realizacją zadań dotyczących bezpieczeństwa danych osobowych, wykonywanych przez ASI;
11) realizowanie obowiązku informacyjnego wobec osób, których dane są przetwarzane, zgodnie z wymogami ustawy;
12) rozpatrywanie wniosków osób, których dane są przetwarzane, dotyczących uzupełnienia, uaktualnienia, sprostowania, wstrzymania przetwarzania lub usunięcia ich danych osobowych.

Do zadań **ASI** należy w szczególności:

1) analiza zagrożeń i ryzyk związanych z przetwarzaniem danych osobowych;
2) zapewnianie, aby do pracy w systemie dopuszczane były wyłącznie osoby posiadające upoważnienie do przetwarzania danych osobowych w systemie informatycznym;
3) sprawdzanie poprawności działania systemu;
4) informowanie ABI o wszelkich zauważonych nieprawidłowościach i incydentach skutkujących obniżeniem poziomu ochrony danych osobowych;

5) podejmowanie natychmiastowych działań zabezpieczających stan systemu informatycznego w przypadku otrzymania informacji o naruszaniu zabezpieczeń systemu informatycznego lub informacji o zmianach, sposobie działania programu lub urządzeń wskazujących na naruszenie bezpieczeństwa danych osobowych;

6) dokonywanie analizy sytuacji okoliczności i przyczyn, które doprowadziły do naruszenia bezpieczeństwa danych i przygotowanie oraz przedstawienie Administratorowi danych osobowych odpowiednich zmian w regulacjach wewnętrznych, w tym w Instrukcji zarządzania systemem informatycznym;

7) zapewnienie awaryjnego zasilania komputerów oraz innych urządzeń mających wpływ na bezpieczeństwo przetwarzania danych osobowych;

8) zapewnienie funkcjonowania mechanizmów uwierzytelniania użytkowników w systemie informatycznym przetwarzającym dane osobowe oraz kontroli dostępu do danych osobowych;

9) zarządzanie hasłami użytkowników i zapewnianie przestrzegania procedur określających częstotliwość ich zmiany zgodnie z Instrukcją zarządzania systemem informatycznym;

10) sprawdzanie systemu pod kątem obecności wirusów komputerowych zgodnie z Instrukcją zarządzania systemem informatycznym;

11) wykonywanie kopii awaryjnych, ich przechowywanie oraz okresowe sprawdzanie pod kątem ich dalszej przydatności do odtwarzania danych w przypadku awarii systemu;

12) prowadzenie spraw przeglądów, konserwacji oraz uaktualnienia systemów służących do przetwarzania danych osobowych oraz innych czynności wykonywanych na bazach danych osobowych;

13) prowadzenie spraw likwidacji sprzętu komputerowego, na którym przetwarzane były dane osobowe;

14) nadzór nad prawidłowym ustawieniem monitorów komputerów, w których następuje przetwarzanie danych osobowych, w sposób uniemożliwiający wgląd w dane osobowe osobom nieupoważnionym.

Do zadań **osoby upoważnionej do przetwarzania danych osobowych (użytkownika)** należy w szczególności:

1) przestrzeganie zasad ochrony danych osobowych określonych w przepisach o ochronie danych osobowych oraz w Polityce bezpieczeństwa i Instrukcji zarządzania systemem informatycznym;

2) przetwarzanie danych osobowych zgodnie z celami przetwarzania;

3) informowanie przełożonych o wszelkich zauważonych nieprawidłowościach i incydentach skutkujących obniżeniem poziomu ochrony danych osobowych;

4) zapewnienie poufności danych osobowych, do których uzyskuje dostęp w związku z wykonywaniem czynności służbowych;

5) ochrona zbiorów danych przed zniszczeniem i nieupoważnionym dostępem;

6) niepozyskiwanie danych osobowych z nielegalnych źródeł;

7) przestrzeganie zasad ochrony antywirusowej;

8) okresowa analiza zagrożeń i ryzyka związanego z przetwarzaniem danych osobowych oraz przekazywanie ABI propozycji zmian regulacji wewnętrznych, a w przypadku przetwarzania danych osobowych w systemie informatycznym – w porozumieniu z ASI.

Do zadań **dyrektora komórki organizacyjnej**, w której przetwarzane są dane osobowe należy w szczególności:

1) składanie wniosku o nadanie, zmianę lub utratę uprawnień użytkownika;

2) informowanie ASI o planowanych nieobecnościach użytkowników, dłuższych niż 14 dni, w celu zablokowania konta użytkownika na czas jego nieobecności w pracy;

3) informowanie ABI o nowych zbiorach danych osobowych oraz o zmianach w zakresie informacji wskazanych w załącznikach Nr 7 i Nr 8 do Polityki bezpieczeństwa.

Załącznik Nr 5

MINISTERSTWO TRANSPORTU, BUDOWNICTWA I GOSPODARKI MORSKIEJ

Warszawa, dnia ……20….. r.

WZÓR

UPOWAŻNIENIE DO PRZETWARZANIA DANYCH OSOBOWYCH

Działając na podstawie art. 37 ustawy z dnia 29 sierpnia 1997 r. o ochronie danych osobowych

upoważniam Panią/Pana:

…….
(imię, nazwisko, stanowisko)

do przetwarzania danych osobowych w zbiorze (zbiorach) w następującym zakresie:

……
……
(nazwa zbioru danych osobowych zgodnie z Wykazem zbiorów danych osobowych w Ministerstwie)

Upoważnienie jest udzielone na czas trwania zatrudnienia na stanowisku pracy, na którym przetwarzane są dane osobowe w ww. zbiorze (zbiorach)/do ……*

…….
(pieczęć i podpis Administratora Danych Osobowych**)

Oświadczam, że zapoznałam/em się z Polityką bezpieczeństwa w zakresie ochrony danych osobowych w Ministerstwie Transportu, Budownictwa i Gospodarki Morskiej oraz Instrukcją zarządzania systemem informatycznym służącym do przetwarzania danych osobowych w Ministerstwie Transportu, Budownictwa i Gospodarki Morskiej.
Zobowiązuję się do przestrzegania zasad przetwarzania danych osobowych określonych w ww. dokumentach oraz nieujawniania informacji zawartych w tych dokumentach, a także danych osobowych, z którymi zapoznam się w trakcie wykonywania obowiązków służbowych. Powyższe informacje zobowiązuję się zachować w tajemnicy przez cały okres zatrudnienia, a także po jego ustaniu.
Oświadczam, że jestem świadoma/my odpowiedzialności karnej, wynikającej z art. 51 – 52 ustawy o ochronie danych osobowych oraz art. 266 Kodeksu karnego.

Przyjęłam/Przyjąłem:

…… …….
(miejscowość i data) (czytelny podpis osoby upoważnionej)

* Należy wybrać właściwe.

** W przypadku wyznaczenia ABI przez ADO, upoważnienie podpisuje ABI.
Upoważnienie sporządza się w trzech egzemplarzach, z których jeden otrzymuje upoważniony, drugi załącza się do akt osobowych pracownika albo w przypadku umowy cywilnoprawnej przechowuje wraz z umową przez komórkę organizacyjną odpowiadającą za jej realizację, trzeci otrzymuje ABI.

Wypełnia osoba przeprowadzająca szkolenie z zakresu przepisów o ochronie danych osobowych oraz postanowień Polityki bezpieczeństwa i Instrukcji zarządzania systemem informatycznym, przed przekazaniem upoważnienia do podpisania

Pani/Pan ……...

w dniu……...

została/został przeszkolona/y w zakresie przepisów o ochronie danych osobowych oraz postanowień Polityki bezpieczeństwa i Instrukcji zarządzania systemem informatycznym.

…….
(data, czytelny podpis osoby przeprowadzającej szkolenie)

Wypełnia Administrator Systemu Informatycznego w przypadku upoważnienia do przetwarzania danych osobowych w systemie informatycznym

W dniu ……

zostało założone konto użytkownika

……..……
(identyfikator)

umożliwiające przetwarzanie danych w zbiorze

……..……
(nazwa zbioru)

za pomocą systemu informatycznego

…….…….
(nazwa systemu)

z zakresem uprawnień

……
(opis uprawnień)

W dniu …… użytkownik został przeszkolony w zakresie zasad pracy w systemie informatycznym

…….
(data, czytelny podpis Administratora Systemu Informatycznego)

W dniu ……..…… zostało usunięte konto użytkownika

……..
(identyfikator)

…….
(data, czytelny podpis Administratora Systemu Informatycznego)

Upoważnienie sporządza się w trzech egzemplarzach, z których jeden otrzymuje upoważniony, drugi załącza się do akt osobowych pracownika albo w przypadku umowy cywilnoprawnej przechowuje wraz z umową przez komórkę organizacyjną odpowiadającą za jej realizację, trzeci otrzymuje ABI.

Załącznik Nr 6

WZÓR

MINISTERSTWO TRANSPORTU, BUDOWNICTWA I GOSPODARKI MORSKIEJ

EWIDENCJA OSÓB UPOWAŻNIONYCH

DO PRZETWARZANIA

DANYCH OSOBOWYCH

Lp.	**Imię i nazwisko**	**Departament/Biuro** (pełna nazwa)	**Data nadania upoważnienia i numer upoważnienia**	**Data ustania upoważnienia**	**Zakres upoważnienia** (w tym nazwa zbioru)	**Identyfikator**	**Uwagi**

Załącznik Nr 7

WZÓR

WYKAZ BUDYNKÓW, POMIESZCZEŃ LUB CZĘŚCI POMIESZCZEŃ, W KTÓRYCH PRZETWARZANE SĄ DANE OSOBOWE W MINISTERSTWIE TRANSPORTU, BUDOWNICTWA I GOSPODARKI MORSKIEJ ZE WSKAZANIEM ADMINISTRATORA DANYCH OSOBOWYCH, PODSTAWY PRAWNEJ PROWADZENIA DANEGO ZBIORU, PROGRAMÓW ZASTOSOWANYCH DO PRZETWARZANIA TYCH DANYCH

Lp.	Komórka organizacyjna MTBiGM	Nazwa zbioru	Program zastosowany do przetwarzania danych osobowych	Administrator danych osobowych	Podstawa prawna prowadzenia zbioru	Budynki, pomieszczenia lub części pomieszczeń, w których przetwarzane są dane osobowe

Załącznik Nr 8

WZÓR

STRUKTURA ZBIORÓW DANYCH, SPOSÓB PRZEPŁYWU DANYCH W SYSTEMIE I ZAKRES PRZETWARZANIA DANYCH

1. Nazwa zbioru danych osobowych

Nazwa zbioru danych osobowych
POLA INFORMACYJNE PRZETWARZANE W ZBIORZE
1.
2.
3.
4.
5.

Sposób przepływu danych w systemie/pomiędzy poszczególnymi systemami:
(należy przedstawić w formie graficznej)

Załącznik Nr 9

Środki techniczne i organizacyjne zastosowane w celu ochrony danych osobowych

ŚRODKI ORGANIZACYJNE

Środki ochrony fizycznej

1. Ochrona obiektów Ministerstwa przez agencję ochrony osób i mienia.
2. System tripodów przy wejściu na teren Ministerstwa.
3. Instalacja odgromowa, instalacja przeciwpożarowa.

Zasady pracy ze zbiorami danych osobowych

1. Dokumenty zawierające dane osobowe, po zakończeniu dnia pracy, przechowywane są w szafach zamykanych na klucz lub na regałach w pomieszczeniach zamykanych na klucz i plombowanych.
2. Klucze od szaf, w których przechowywane są dokumenty zawierające dane osobowe, umieszczane są przez osobę upoważnioną do przetwarzania danych osobowych po zakończeniu dnia jej pracy w ustalonym, przeznaczonym do tego miejscu.
3. Przetwarzanie danych osobowych w komputerach przenośnych jest zakazane.
4. Drukowanie dokumentów zawierających dane osobowe odbywa się wyłącznie w obecności osoby uprawnionej do przetwarzania danych osobowych zawartych w drukowanych dokumentach.
5. Komputerowy wygaszacz ekranu aktywowany jest automatycznie w przypadku braku aktywności osoby upoważnionej do przetwarzania danych osobowych dłuższej niż 5 minut.
6. Ekrany komputerowe ustawione są w sposób uniemożliwiający zapoznanie się z treścią na nich wyświetloną przez osoby nieupoważnione do przetwarzania danych zawartych w tych komputerach.
7. Osoba upoważniona do przetwarzania danych osobowych, na czas swojej nieobecności zamyka drzwi pokoju na klucz.
8. Osoba upoważniona do przetwarzania danych osobowych po zakończeniu dnia jej pracy, zamyka okna, zamyka drzwi pokoju na klucz, który składa na portierni.
9. Osoby nieuprawnione nie są pozostawiane bez nadzoru w pokojach, w których przetwarzane są dane osobowe.
10. Osoba upoważniona do przetwarzania danych osobowych nie dopuszcza do sytuacji, w której stanowisko pracy pracownika zajmie osoba nieuprawniona do przetwarzania danych osobowych.

Zasady korzystania z haseł przez osoby uprawnione do przetwarzania danych osobowych w systemach informatycznych

1. Hasła ASI chronione są w zamkniętych i opieczętowanych kopertach.
2. Użytkownik końcowy systemu informatycznego:
   1) przechowuje swoje hasło w sposób uniemożliwiający zapoznanie się z nim przez inne osoby;
   2) występuje do ASI o zmianę hasła w przypadku co najmniej podejrzenia ujawnienia hasła.

Zarządzanie nieprawidłowościami systemu informatycznego i zbioru manualnego

1. Każdy ma obowiązek zgłoszenia Administratorowi danych osobowych oraz ABI zauważonych nieprawidłowości oraz incydentów, które mogą skutkować obniżeniem stopnia ochrony danych osobowych.
2. Każda nieprawidłowość oraz incydent, które mogą skutkować obniżeniem stopnia ochrony danych osobowych, są wyjaśniane i usuwane przez ABI, a w przypadku nieprawidłowości systemu informatycznego - we współpracy z ASI.
3. Kontrole ochrony przetwarzania danych przeprowadza ABI.

Szkolenia

Osoba upoważniona do przetwarzania danych osobowych podlega obowiązkowemu szkoleniu w zakresie:

1) przepisów o ochronie danych osobowych oraz postanowień Polityki bezpieczeństwa i Instrukcji zarządzania systemem informatycznym;
2) zasad pracy w systemie informatycznym – w przypadku przetwarzania danych w systemie informatycznym.

ŚRODKI TECHNICZNE

Środki ochrony systemów informatycznych i narzędzi baz danych

1. Dostęp do komend systemu operacyjnego mają tylko użytkownicy, których zakres obowiązków wymaga dostępu do systemu.
2. System informatyczny umożliwia dostęp do bazy tylko upoważnionym użytkownikom.
3. Każdy użytkownik posiada indywidualne hasło i identyfikator.
4. Nazwa profilu użytkownika nie zmienia się przez cały okres jego pracy w Ministerstwie, z wyłączeniem takich przypadków jak np. zmiana nazwiska.
5. Liczba użytkowników posiadających uprawnienia do przetwarzania danych osobowych w danym systemie powinna być ograniczona do niezbędnego minimum, jednak nie mniej niż do dwóch osób.

6. W komputerach użytkowników przetwarzających dane osobowe zainstalowane są jedynie kopie oprogramowania, do których Ministerstwo posiada prawo do instalacji i eksploatacji. Instalacji dokonują wyłącznie pracownicy Pionu Informatyki.
7. W celu zmniejszenia prawdopodobieństwa ataku wirusowego:
   1) oprogramowanie systemów podlega kontroli konfiguracji, wykonywanej przez pracowników Pionu Informatyki;
   2) nośniki ze źródeł zewnętrznych są sprawdzane na obecność wirusów;
   3) w systemie zainstalowane jest wyłącznie autoryzowane oprogramowanie licencjonowane;
   4) wymiana oprogramowania ograniczona jest tylko do uzasadnionych przypadków.

Zabezpieczenie sprzętu

1. Zasilanie oraz kable sieciowe są oznakowane i zabezpieczone przed zniszczeniem.
2. Stanowiska dostępowe podłączane są do sieci zasilającej dedykowanej lub do lokalnych UPS.
3. Konserwacja sprzętu komputerowego, na którym przechowywane są bazy zawierające dane osobowe, odbywa się w terminach określonych przez producenta sprzętu lub dostawcę w instrukcji obsługi, w siedzibie Ministerstwa.
4. Użytkownik po wykryciu usterki sprzętu komputerowego lub innego problemu związanego ze sprzętem lub oprogramowaniem – kontaktuje się z odpowiednim – ASI bądź ABI. ASI – po konsultacji z użytkownikiem, podejmuje decyzje o zasadności zgłoszenia zlecenia naprawy sprzętu bądź oprogramowania i kontaktuje się z pracownikiem Pionu Informatyki odpowiedzialnym za naprawę.
5. Realizacja naprawy o ile to możliwe odbywa się w miejscu użytkowania danego sprzętu komputerowego. Podczas naprawy użytkownik odpowiedzialny za sprzęt nadzoruje prace związane z realizacją naprawy.
6. Ze sprzętu komputerowego przekazywanego do naprawy poza siedzibę Ministerstwa pracownicy Pionu informatyki usuwają wszystkie nośniki informacji, na których przechowywane są dane osobowe. Nośnik te przechowywane są przez użytkownika systemu informatycznego w szafie zamykanej na klucz. Ponownej instalacji nośników dokonują pracownicy Pionu Informatyki
7. Naprawy i konserwacje sprzętu komputerowego, na którym przechowywane są bazy zawierające dane osobowe, są ewidencjonowane na formularzach napraw i konserwacji sprzętu , które zawierają:
   1) datę dokonanej naprawy lub konserwacji;
   2) typ oraz numer sprzętu;
   3) opis wykonanych czynności;
   4) imię i nazwisko osoby dokonującej naprawy;
   5) imię i nazwisko osoby nadzorującej.
8. Formularze, o którym mowa w ust. 7 prowadzi Pion informatyki.

9. W przypadku przekazywania osobom trzecim sprzętu komputerowego wykorzystywanego do przetwarzania danych osobowych pracownicy Pionu informatyki usuwają wszelkie nośniki danych, na których rejestrowane były dane osobowe.

Załącznik Nr 2
do zarządzenia Nr 49
Ministra Transportu,
Budownictwa i Gospodarki Morskiej
z dnia 19 lipca 2012 r. (poz. 49)

Instrukcja zarządzania systemem informatycznym służącym do przetwarzania danych osobowych w Ministerstwie Transportu, Budownictwa i Gospodarki Morskiej

§ 1.

1. Instrukcja zarządzania systemem informatycznym służącym do przetwarzania danych osobowych w Ministerstwie Transportu, Budownictwa i Gospodarki Morskiej, zwanym dalej „Ministerstwem", określa:

1) procedury nadawania uprawnień do przetwarzania danych i rejestrowania tych uprawnień w systemie informatycznym oraz wskazanie osoby odpowiedzialnej za te czynności;

2) stosowane metody i środki uwierzytelnienia oraz procedury związane z ich zarządzaniem i użytkowaniem;

3) procedury rozpoczęcia, zawieszenia i zakończenia pracy przeznaczone dla użytkowników systemu;

4) procedury tworzenia kopii zapasowych zbiorów danych oraz programów i narzędzi programowych służących do ich przetwarzania;

5) sposób, miejsce i okres przechowywania:

a) elektronicznych nośników informacji zawierających dane osobowe,

b) kopii zapasowych, o których mowa w pkt 4;

6) sposób zabezpieczenia systemu informatycznego przed działalnością oprogramowania, o którym mowa w pkt III ppkt 1 załącznika do 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), zwanego dalej „rozporządzeniem";

7) sposób realizacji wymogów, o których mowa w § 7 ust. 1 pkt 4 rozporządzenia;

8) procedury wykonywania przeglądów i konserwacji systemów oraz nośników informacji służących do przetwarzania danych;

9) podstawowe zasady dotyczące funkcjonowania i bezpieczeństwa sieci komputerowej Ministerstwa.

2. Opis procedur, o których mowa w ust. 1, pkt 1-8, odrębnie dla każdego systemu informatycznego służącego do przetwarzania danych osobowych w Ministerstwie, prowadzi ABI, a w przypadku gdy ABI nie został wyznaczony – Biuro Dyrektora Generalnego w Ministerstwie. Procedury są dostępne na wewnętrznym portalu intranetowym Ministerstwa.

§ 2.

6. Do przetwarzania danych osobowych w systemie informatycznym dopuszczone są wyłącznie osoby przeszkolone w zakresie zasad przetwarzania danych osobowych i obsługi systemu informatycznego oraz posiadające upoważnienie do przetwarzania danych osobowych.
7. Wzór upoważnienia, o którym mowa w ust. 1, określa załącznik Nr 5 do Polityki bezpieczeństwa w zakresie ochrony danych osobowych w Ministerstwie Transportu, Budownictwa i Gospodarki Morskiej, zwanej dalej „Polityką bezpieczeństwa".

§ 3.

Ustala się następujące podstawowe zasady dotyczące funkcjonowania i bezpieczeństwa sieci komputerowej Ministerstwa, o których mowa w § 1 ust. 1 pkt 9.

1. Sieci LAN oparte są o topologię Ethernet, realizowaną na zarządzanych modularnych przełącznikach rozlokowanych w węzłach sieci. W zależności od potrzeb tworzy się wirtualne sieci typu VLAN oparte na warstwie fizycznej okablowania strukturalnego w budynkach, w poszczególnych siedzibach Ministerstwa. W szczególności sieci typu VLAN są utworzone dla sieci wydzielonych. Urządzenia zabezpieczone są hasłem dostępowym, do każdego urządzenia przydzielony jest indywidualny adres (numer) IP.
2. Dla realizacji bezpiecznego połączenia sieci komputerowej z siecią Internet na brzegu sieci LAN są wdrożone i eksploatowane specjalizowane i konfigurowane urządzenia. Urządzenia te pozwalają na monitorowanie ataków, ich zapobieganie, poprzez analizę pakietów w ruchu sieciowym i raportowanie ogólnych nieprawidłowości komunikacyjnych. Ochrona sprzętowa wspierana jest odpowiednim oprogramowaniem, w tym antywirusowym chroniącym przed kodem złośliwym. Zarządzanie urządzeniami i konfigurowanie oprogramowania jest możliwe tylko z określonych konsoli administratorskich przypisanych do administratora LAN i Administratora Systemu Informatycznego, zwanego dalej „ASI" lub innych upoważnionych osób.
3. Serwery sieciowe oparte są na systemach operacyjnych Microsoft Windows i/lub Linux lub jego pochodne. Dane zapisane na dyskach serwerowych zabezpieczone są za pomocą praw NTFS i praw do udziałów.
4. W węzłach sieci eksploatowane są szafy dystrybucyjne (krosownicze). Węzły sieci realizujące zadania systemów wydzielonych VLAN są zabezpieczone w system alarmowy monitorowany przez system ochrony obiektów lub znajdują się w pomieszczeniach objętych podwyższonym poziomem kontroli dostępu.
5. Okablowanie strukturalne poprowadzone jest nadtynkowo w korytkach PCV.
6. Zasilanie elektryczne sprzętu teleinformatycznego jest realizowane w części obiektów należących do Ministerstwa w układzie wydzielonych instalacji elektrycznych, przeznaczonych wyłącznie dla sprzętu komputerowego. W innych obiektach wykorzystywana jest instalacja tzw. ogólna. Serwery oraz stacje robocze w sieci podłączone są do zasilaczy awaryjnych (UPS), podtrzymujących zasilanie z baterii dla stacji roboczych na kilka minut, a dla serwerów na kilkanaście lub kilkadziesiąt minut. Ze względów bezpieczeństwa i zapewnienia zasilania systemów część szaf dystrybucyjnych wyposażono w zasilacze awaryjne.
7. Część urządzeń sieciowych o podwyższonym znaczeniu dla bezpieczeństwa sieci oraz ciągłości działania usług sieciowych jest eksploatowana w układach zdwojonych, gwarantujących nieprzerwaną pracę w przypadkach awarii jednego z urządzeń w układzie.

8. Serwerownie są centralnymi węzłami sieci komputerowych, posiadającymi dodatkowe zabezpieczenia chroniące przed nieupoważnionym dostępem. Pomieszczenia serwerowi są monitorowane przez włączenie do systemu ochrony obiektów Ministerstwa albo mają podwyższony poziom kontroli dostępu. Dostęp do serwerowni mają tylko osoby uprawnione.

9. Dla zapewnienia bezpieczeństwa, poprawności i ciągłości działania systemów informatycznych, w tym sieci komputerowej, Ministerstwo podejmuje działania polegające na zlecaniu wyspecjalizowanym firmom części zadań informatycznych w drodze usług wsparcia informatycznego.