Straż Miejska w Cieszynie
ul. Limanowskiego 7
43-400 CIESZYN
Tel. 33/8579 400, tel./fax 33/8579 402

Załącznik Nr 1
do Zarządzenia Nr 6/2011
Komendanta Straży Miejskiej w Cieszynie
z dnia 15 marca 2011 roku

POLITYKA BEZPIECZEŃSTWA STRAŻY MIEJSKIEJ W CIESZYNIE

Cieszyn 2011

Podstawa prawna § 3 i § 4 Rozporządzenia Ministra Spraw Wewnętrznych Administracji z dnia 29 kwietnia 2004 roku 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 z 2004 roku, poz. 1024).

SPIS TREŚCI

ZAŁĄCZNIKI:

I. WSTĘP

Jedną z podstawowych cech współczesnego społeczeństwa jest łatwość i szybkość uzyskania interesujących informacji. Możliwość łatwego uzyskania informacji - danych, wiąże się jednak z pewnymi zagrożeniami, wynikającymi z nieuzasadnionego dostępu do tych danych, które ze względu na dobro państwa, firmy, instytucji, czy osoby nie powinny być udostępniane.

Najbardziej znanymi rodzajami zagrożeń, które mogą dotknąć współczesną instytucję, są m.in. **nieuzasadnione udostępnienie, zniszczenie, kradzież danych, uniemożliwienie dostępu, celowa modyfikacja, podszycie się, podsłuch**. Celem ataku mogą być zarówno tradycyjnie (manualnie) prowadzone kartoteki, jak również wydruki komputerowe, elektronicznie prowadzone bazy danych, które mogą zostać skradzione, zniszczone, zmodyfikowane. Coraz częściej celem ataku jest również poczta elektroniczna, elektroniczny obieg dokumentów, Biuletyn Informacji Publicznej, strony internetowe instytucji.

W celu wyeliminowania tych zagrożeń Komendant Straży Miejskiej w Cieszynie wprowadza "Politykę bezpieczeństwa Straży Miejskiej w Cieszynie", uznając zabezpieczenie danych osobowych jako jeden z priorytetów, zapewniając przy tym środki techniczne i organizacyjne jakimi powinny odpowiadać pomieszczenia, urządzenia i systemy informatyczne służące do przetwarzania danych osobowych. "Polityka bezpieczeństwa Straży Miejskiej w Cieszynie" jest swoistego rodzaju "przewodnikiem", który ma ułatwiać pracownikom ochronę danych osobowych przed niepowołanym dostępem. Wskazuje ona miejsca przetwarzania danych, posiadane zbiory oraz sposób ochrony i postępowania w razie nieuzasadnionego dostępu do tych danych. Odnosi się ona całościowo do problemu zabezpieczenia danych osobowych zarówno przetwarzanych tradycyjnie, jak również w systemach informatycznych.

Należy jednak pamiętać, że **najlepiej opracowana "Polityka bezpieczeństwa", najnowocześniejszy sprzęt i oprogramowanie zabezpieczające nie wyeliminuje wszystkich zagrożeń, jeśli nie będzie to poparte zaangażowaniem samych pracowników w ochronę tych danych**. Dlatego każdy z pracowników powinien dołożyć wszelkich starań, aby dane osobowe były należycie chronione. Wszyscy pracownicy, stażyści, praktykanci pracujący w Straży Miejskiej muszą zapoznać się z "Polityką bezpieczeństwa", "Instrukcją zarządzania systemem informatycznym" oraz z innymi dokumentami dotyczącymi

ochrony danych osobowych w Komendzie Straży Miejskiej w Cieszynie w zakresie niezbędnym do wykonywania ich zadań. Potwierdzają to złożonym oświadczeniem stanowiącym załącznik nr 1 do niniejszego dokumentu. Jednocześnie powinni śledzić na bieżąco akty normatywne, dotyczące w/w tematyki oraz wykazywać chęć pogłębiania wiedzy w zakresie ochrony danych osobowych.

Pracownicy Straży Miejskiej w Cieszynie są zobowiązani do zwracania uwagi na sytuacje, które mogą doprowadzić do utraty danych osobowych, jak również zgłaszać Komendantowi Straży Miejskiej wszelkie uwagi dotyczące przetwarzania i ochrony tych danych.

Należy również podkreślić, że "Polityka bezpieczeństwa Straży Miejskiej w Cieszynie" jest dokumentem, który będzie na bieżąco aktualizowany w miarę zmieniających się zagrożeń, wprowadzania nowych zabezpieczeń, rozszerzania się ilości przetwarzanych zbiorów itp.

"Polityka bezpieczeństwa Straży Miejskiej w Cieszynie" oraz „Instrukcja zarządzania systemem informatycznym Straży Miejskiej w Cieszynie" została opracowana w oparciu o:

1. Ustawę z dnia 29 sierpnia 1997r o ochronie danych osobowych (Dz. U. Nr 101 z 2002r, poz. 926 z późn. zm.).
2. Rozporządzenie Ministra Spraw Wewnętrznych i Administracji z dnia 29 kwietnia 2004r 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).
3. Wytyczne Generalnego Inspektora Ochrony Danych Osobowych w zakresie opracowania i wdrożenia polityki bezpieczeństwa (www.giodo.gov.pl), 17.03.08r.
4. Wskazówki dotyczące sposobu opracowania instrukcji określającej sposób zarządzania systemem informatycznym, służącym do przetwarzania danych osobowych, ze szczególnym uwzględnieniem wymogów bezpieczeństwa informacji. (www.giodo.gov.pl), 17.03.08r.
5. ABC zasad bezpieczeństwa przetwarzania danych osobowych przy użyciu systemów informatycznych. Wydawnictwo Sejmowe. Warszawa 2007. (www.giodo.gov.pl),17.03.08 r.
6. Ogólne zalecenia dla pomieszczeń w których przetwarzane są dane osobowe. Warunki organizacyjno-techniczne doręczania dokumentów elektronicznych

podmiotom publicznym, www.e-slask.pl, 16.01.08r.

7. Przemysław Bańko: Polityka bezpieczeństwa informacji i wymagania bezpieczeństwa dla partnerów. SB.CPD1c_Wersja 1. Aram Sp. z o.o. 2007. www.e-slask.pl, 21.03.08r.

8.Dokumenty wewnętrzne Straży Miejskiej w Cieszynie dotyczące organizacji i pracy Straży: Regulamin organizacyjny, Regulamin pracy.

UWAGA: *Zgodnie art. 39 ust. 2 ustawy o ochronie danych osobowych, osoby które zostały upoważnione do przetwarzania danych, są obowiązane zachować w tajemnicy* ***te dane osobowe*** *oraz* ***sposoby ich zabezpieczenia*** *(Dz.U. z 2002 Nr 101, poz. 926 z późn. zm.).*

Do sposobów ich zabezpieczenia należą fizyczne, logiczne oraz organizacyjne sposoby zabezpieczenia danych osobowych w tym „Polityka bezpieczeństwa" i „Instrukcja zarządzania systemem informatycznym". ***W związku z powyższym treść Polityki bezpieczeństwa i Instrukcji zarządzania systemem informatycznym ma charakter informacji chronionej tajemnicą pracodawcy na zasadzie art. 100 § 2 pkt 4 Kodeksu pracy.***

II. PODSTAWOWE POJĘCIA

Dane osobowe – za dane osobowe uważa się wszelkie informacje dotyczące zidentyfikowanej lub możliwej do zidentyfikowania osoby fizycznej. Osobą możliwą do zidentyfikowania jest osoba, której tożsamość można określić bezpośrednio lub pośrednio, w szczególności przez powołanie się na numer identyfikacyjny albo jeden lub kilka specyficznych czynników określających jej cechy fizyczne, fizjologiczne, umysłowe, ekonomiczne, kulturowe lub społeczne (Dz.U. Nr 101 z 2002, poz. 926 z późn. zm.).

Zbiór danych – rozumie się przez to każdy posiadający strukturę zestaw danych o charakterze osobowym, dostępnych według określonych kryteriów, niezależnie od tego, czy zestaw ten jest rozproszony lub podzielony funkcjonalnie.

Przetwarzanie danych – rozumie się przez to jakiekolwiek operacje wykonywane na danych osobowych, takie jak zbieranie, utrwalanie, przechowywanie, opracowywanie, zmienianie, udostępnianie.

Polityka bezpieczeństwa (PB) – to dokument zawierający cele i zasady zabezpieczenia danych osobowych, a w szczególności zestaw praw, reguł i praktycznych doświadczeń regulujących sposób zarządzania, ochroną i dystrybucją

danych osobowych wewnątrz instytucji. Polityka bezpieczeństwa zgodnie z ustawą o ochronie danych osobowych odnosi się całościowo do problemu zabezpieczenia danych osobowych zarówno do danych przetwarzanych tradycyjnie jak i danych przetwarzanych w systemach informatycznych.

Instrukcja zarządzania systemem informatycznym (IZSI) – to dokument określający sposób zarządzania systemem informatycznym, służącym do przetwarzania danych osobowych, w tym precyzuje zapisy dotyczące zarządzania systemem informatycznym zapisane w Polityce bezpieczeństwa.

System informatyczny – jest to zespół współpracujących ze sobą urządzeń, programów, procedur przetwarzania informacji i narzędzi programowych zastosowanych w celu przetwarzania danych.

Administrator Danych (AD) – jest to organ, jednostka organizacyjna, podmiot lub osoba, które mają siedzibę albo miejsce zamieszkania na terytorium Rzeczypospolitej Polskiej, albo w państwie trzecim, o ile przetwarzają dane osobowe przy wykorzystaniu środków technicznych znajdujących się na terytorium Rzeczypospolitej Polskiej. Ilekroć w Polityce i Instrukcji mowa jest o Administratorze Danych należy przez to rozumieć Komendanta Straży Miejskiej lub upoważnioną przez niego osobę do wykonywania określonych zadań Administratora Danych.

Administrator Bezpieczeństwa Informacji (ABI)- jest to osoba lub osoby wyznaczone przez Administratora Danych do nadzoru nad bezpieczeństwem danych osobowych przetwarzanych w Komendzie Straży Miejskiej w Cieszynie. Administratora Bezpieczeństwa Informacji wyznacza zarządzeniem wewnętrznym Komendant Straży Miejskiej. Szczegółowy zakres obowiązków ABI określa zakres czynności.

Administrator Systemu Informatycznego (ASI) – jest to osoba lub osoby wyznaczone zarządzeniem wewnętrznym przez Komendanta Straży Miejskiej do nadzoru nad sprawnym, bezpiecznym i ciągłym funkcjonowaniem systemu informatycznego służącym do przetwarzania danych osobowych. W tym stosowanie technicznych i organizacyjnych środków ochrony przewidzianych w tym systemie zgodnym z ustawą o ochronie danych osobowych i rozporządzeniem. W Straży Miejskiej w Cieszynie przez Administratora Systemu Informatycznego należy rozumieć administratora sieci, administratora aplikacji oraz baz danych, w którym przetwarzane są dane osobowe. Szczegółowy zakres obowiązków ASI określa zakres czynności.

Użytkownik – to pracownik, stażysta, praktykant lub inna osoba dopuszczona do przetwarzania danych osobowych w zbiorach SM w Cieszynie w zakresie zgodnym z upoważnieniem.

Identyfikator użytkownika (login) – rozumie się przez to ciąg znaków literowych, cyfrowych lub innych jednoznacznie identyfikujących osobę upoważnioną do przetwarzania danych osobowych w systemie informatycznym.

Hasło – rozumie się przez to ciąg znaków literowych, cyfrowych lub innych, znany jedynie osobie uprawnionej do pracy w systemie informatycznym.

Odbiorca danych - zgodnie z ustawą o ochronie danych osobowych przez odbiorcę danych należy rozumieć każdego komu udostępnia się dane, z wyłączeniem: osoby, której dane dotyczą; osoby upoważnionej do przetwarzania danych; przedstawiciela podmiotu w Rzeczypospolitej Polskiej, który ma siedzibę lub miejsce zamieszkania w państwie trzecim; podmiotu, któremu powierzyło się przetwarzanie danych; organów państwowych lub organów samorządu terytorialnego, którym dane są udostępniane w związku z prowadzonym postępowaniem.

III. WYKAZ BUDYNKÓW, POMIESZCZEŃ LUB CZĘŚCI POMIESZCZEŃ TWORZĄCYCH OBSZAR, W KTÓRYM PRZETWARZANE SĄ DANE OSOBOWE

Dane osobowe należące do Straży Miejskiej w Cieszynie przetwarzane są w dwóch budynkach:

1. Komenda Straży Miejskiej w Cieszynie przy ul. Limanowskiego 7,
2. Urząd Miejski w Cieszynie przy ul. Rynek 1.

Do miejsc przetwarzania danych osobowych zalicza się również siedziby podmiotów, które stale lub czasowo mają dostęp do zbiorów danych osobowych SM w Cieszynie poprzez sieć telekomunikacyjną w zakresie szerszym niż wgląd do swoich danych.

Szczegółowy wykaz pomieszczeń tworzących obszar, w którym przetwarzane są dane osobowe, stanowiący załącznik nr 2 do Polityki bezpieczeństwa, prowadzi Administrator Bezpieczeństwa Informacji.

Wykaz osób upoważnionych do przetwarzania danych osobowych oraz szczegółowy opis zbiorów danych osobowych przetwarzanych w Komendzie Straży Miejskiej w Cieszynie, wynika z następujących dokumentów:

1. Ewidencja osób upoważnionych do przetwarzania danych osobowych w zbiorach Straży Miejskiej w Cieszynie, stanowiąca załącznik nr 3 do niniejszego opracowania

obejmująca imię i nazwisko osoby upoważnionej, datę nadania i ustania oraz zakres upoważnienia do przetwarzania danych osobowych, identyfikator, jeżeli dane są przetwarzane w systemie informatycznym. Dodatkowo ewidencja może zostać rozszerzona o inne pozycje w tym: datę wydania oświadczenia, aneksu do zakresu czynności oraz miejsca przetwarzania danych przez osobę.

IV. SZCZEGÓŁOWY OPIS ZBIORÓW DANYCH OSOBOWYCH ORAZ EWIDENCJA OSÓB UPOWAŻNIONYCH DO PRZETWARZANIA DANYCH OSOBOWYCH

1.Wykaz zbiorów danych osobowych prowadzonych w Komendzie Straży Miejskiej w Cieszynie wraz ze wskazaniem programów zastosowanych do przetwarzania tych danych, stanowi załącznik nr 4 do niniejszego opracowania. Dokumentację określoną w pkt 1 i 2 prowadzi Administrator Danych.

2.Szczegółowy opis struktury zbiorów danych wskazujący zawartość poszczególnych pól informacyjnych i powiązania między nimi oraz sposób przepływu danych pomiędzy poszczególnymi systemami stanowi załącznik nr 5 do Polityki bezpieczeństwa.

V. OKREŚLENIE ŚRODKÓW TECHNICZNYCH I ORGANIZACYJNYCH NIEZBĘDNYCH DLA ZAPEWNIENIA POUFNOŚCI, INTEGRALNOŚCI I ROZLICZALNOŚCI DANYCH

1. W celu ochrony danych osobowych oraz sprawnego funkcjonowania systemu informatycznego przetwarzającego dane osobowe Komenda Straży Miejskiej w Cieszynie ma wyznaczonego:
   a/ Administratora Systemu Informatycznego (ASI).
   b/ Pracownika wyznaczonego d/s obsługi archiwum zakładowego, upoważnionego do przetwarzania danych osobowych w zakresie niezbędnym do wykonywania prac archiwizacyjnych oraz odpowiedzialnego za właściwe prowadzenie Archiwum Zakładowego SM w Cieszynie zgodnie z Ustawą z dnia 14 lipca 1983 r. o narodowym zasobie archiwalnym i archiwach (Dz.U. z 2002 r. Nr 171, poz. 139 z późn. zm.).
2. W celu lepszego zabezpieczenia danych osobowych można wyznaczyć dodatkowo innych pracowników bezpośrednio odpowiedzialnych za dany zbiór,

system lub zobowiązanych do prowadzenia dokumentacji z zakresu ochrony danych osobowych przetwarzanych w danym wydziale, biurze.

3. Za prawidłowe przetwarzanie danych osobowych w wydziale - biurze bezpośrednio jest odpowiedzialny Komendant Straży Miejskiej, który nadzoruje i kontroluje przetwarzanie danych przez podległych mu pracowników-stażystów.
4. Problemy bezpieczeństwa danych uwzględniane są już na etapie rekrutacji pracowników
   i włączone w zakresy obowiązków z nich wynikających. W stosunku do każdego pracownika ustalane są szczegółowe wymagania.
5. Każdy nowy pracownik przechodzi podstawowe szkolenie z zakresu prawidłowego logowania się, złożoności hasła oraz obsługi systemu informatycznego w zakresie niezbędnym do wykonywania swoich obowiązków, a po zakończeniu pracy zachowania w tajemnicy wszystkich danych osobowych oraz sposobów ich zabezpieczenia.
6. Zapoznanie się z w/w informacjami przez pracownika, a w przypadku osoby odchodzącej z pracy również poświadczenie zablokowania konta w systemie informatycznym potwierdzane jest na karcie obiegowej pracownika.
7. Wszyscy pracownicy, kontrahenci i osoby trzecie zobowiązani są do oddania wszystkich aktyw (pamięci pendrive, laptopów, kluczy, pieczątek itp.) należących do Straży Miejskiej, przed zakończeniem zatrudnienia, umowy.
8. Komendant, Z-ca Komendanta lub bezpośredni przełożony zobowiązany jest przed dopuszczeniem pracownika, stażysty, praktykanta do pracy przeprowadzić podstawowe szkolenie stanowiskowe oraz poinformować go o rodzajach danych przetwarzanych w wydziale - biurze i sposobach ich zabezpieczenia.
9. Okresowo przeprowadzane są szczegółowe szkolenia z zakresu ochrony danych osobowych w Komendzie Straży Miejskiej w Cieszynie dla nowych pracowników, stażystów i praktykantów prowadzone przez Administratora Bezpieczeństwa Informacji lub inną wyznaczoną osobę.
10. Każda osoba przetwarzająca dane osobowe ma pisemne upoważnienie i jest bezpośrednio odpowiedzialna za bezpieczeństwo przetwarzanych przez siebie danych. Dostęp do zbiorów określany jest zgodnie z kompetencjami wyznaczonymi przez Komendanta Straży Miejskiej.
11. Administrator Danych po wydaniu pozytywnej decyzji w uzgodnieniu z Administratorem Bezpieczeństwa Informacji i Administratorem Systemu Informatycznego przekazuje pracownikowi pisemne upoważnienie do

przetwarzania danych osobowych; informując o tym fakcie osobę nadzorującą pracę w wydziale. Na tej podstawie Komendant, Z-ca Komendanta sporządza aneks do zakresu czynności pracownika, stażysty uwzględniając w nim obowiązki wynikające z przepisów odnoszących się do ochrony danych osobowych. Jednocześnie przygotowuje oświadczenie o zapoznaniu się z polityką bezpieczeństwa i instrukcją zarządzania systemem informatycznym. Aneks i oświadczenie podpisuje pracownik w przypadku wydania pierwszego upoważnienia do przetwarzania danych osobowych. Wzór oświadczenia, upoważnienia oraz odwołania do przetwarzania danych osobowych stanowi odpowiednio załącznik nr 1, 7 i 8. Na podstawie wydanego upoważnienia, jeśli dotyczy to zbiorów prowadzonych w systemie informatycznym, Administrator Systemu Informatycznego zakłada konto w systemie i nadaje uprawnienia zgodnie z upoważnieniem. W przypadku kiedy nie ma możliwości szczegółowego ograniczenia wykonywanych czynności lub zakresu dostępu do danej aplikacji należy pamiętać, że użytkownik pomimo tego nie może przetwarzać w systemie danych w zakresie większym niż jest to przewidziane w upoważnieniu.

12. Przekazanie loginu i hasła użytkownikowi może nastąpić dopiero po wydaniu upoważnienia.
13. Jeden komplet dokumentów upoważnienie, aneks oraz oświadczenie Komendant zobowiązany jest dostarczyć do akt osobowych pracownika.
14. Odwołanie upoważnienia lub wygaśnięcie ważności upoważnienia skutkuje natychmiastowym zablokowaniem dostępu użytkownikowi do zbiorów danych osobowych
    i odnotowaniem tego faktu w ewidencji osób upoważnionych do przetwarzania danych osobowych.
15. Zablokowanie dostępu do zbiorów danych osobowych następuje na wniosek Komendanta lub automatycznie w przypadku wygaśnięcia ważności upoważnienia, a w uzasadnionych przypadkach na wniosek Administratora Bezpieczeństwa Informacji lub Administratora Systemu Informatycznego.
16. Okresowo sprawdza się zgodność ewidencji osób upoważnionych do przetwarzania danych osobowych ze stanem faktycznym.
17. Przed przystąpieniem do przetwarzania danych osobowych w nowym zbiorze, Komendant zobowiązany jest do pisemnego poinformowania Administratora Danych o powstającym w ramach pracy wydziału zbiorze zawierającym dane osobowe zarówno podlegającym rejestracji jak i zwolnionym z rejestracji.

W przypadku kiedy zbiór podlega rejestracji niezwłocznie po otrzymaniu takiej informacji Administrator Danych występuje z wnioskiem do Generalnego Inspektora Ochrony Danych Osobowych o zarejestrowanie zbioru danych osobowych. Komendant powiadamia również Administratora Danych o wszelkich zmianach w zbiorze danych osobowych.

18. Komendant, a w przypadku zbiorów informatycznych również Administrator Systemu Informatycznego zobowiązany jest dostarczyć Administratorowi Danych wszelkich niezbędnych informacji o danym zbiorze, w celu prawidłowego zaewidencjonowania zbioru i jeśli jest taka konieczność również zgłoszenia zbioru do GIODO.
19. Ochronę fizyczną pomieszczeń Straży Miejskiej oraz danych osobowych stanowią:

a/ zamki drzwiowe.

b/ szafy pancerne, metalowe, drewniane zamykane.

c/ system obiektowego monitoringu kamerowego.

d/ strażnicy miejscy – dyżurny, pomocnik dyżurnego, których jednym z zadań jest ochrona budynku komendy.

20. Przebywanie na terenie Komendy Straży Miejskiej:

a/ Pracownikom Straży Miejskiej wolno przebywać na terenie Komendy tylko w godzinach pracy – dyżuru.

b/ Przebywanie innych pracowników w budynku Straży Miejskiej, poza wyznaczonymi godzinami pracy oraz w dni wolne, wymaga zezwolenia Komendanta Straży Miejskiej, Zastępcy Komendanta Straży Miejskiej lub gdy ich nie ma - Dyżurnego Komendy. Dodatkowo osoby upoważnione do przetwarzania danych osobowych, chcące przetwarzać dane osobowe poza godzinami wyznaczonymi w regulaminie pracy powinni uzyskać pisemną zgodę Komendanta Straży Miejskiej lub Zastępcy Komendanta Straży Miejskiej.

c/ Pracownicy przebywający poza godzinami pracy w Komendzie powinni przebywać tylko w pomieszczeniach Komendy, które są niezbędne do wykonania ich pracy.

d/ Pracownicy firm zewnętrznych wykonujący pracę poza godzinami pracy Komendy powinni pracować pod nadzorem wyznaczonego pracownika Straży Miejskiej.

e/ Przebywanie innych osób nieuprawnionych na terenie Komendy poza godzinami pracy jest dopuszczalne wyłącznie w wyznaczonych pomieszczeniach i