Załącznik Nr 1 do Zarządzenia Nr 98/11
Burmistrza Miasta Bielsk Podlaski
z dnia 21 czerwca 2011 r.

POLITYKA BEZPIECZEŃSTWA DANYCH OSOBOWYCH w Urzędzie Miasta Bielsk Podlaski

Rozdział 1
Postanowienia ogólne

§ 1. Podstawa prawna

Podstawę prawną dla polityki bezpieczeństwa danych osobowych w Urzędzie Miasta Bielsk Podlaski stanowią:

1) Ustawa z dnia 29 sierpnia 1997 r. o ochronie danych osobowych. (tekst jednolity: Dz. U. 2002 r. Nr 101 poz. 926, ze zm.),

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

§ 2. Definicje

Definicje stosowanych pojęć:

1) **dane osobowe** – wszelkie informacje dotyczące zidentyfikowanej lub możliwej do zidentyfikowania osoby,

2) **osoba możliwa do zidentyfikowania** – każda 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,

3) **zbiór danych** – każdy posiadający strukturę zestaw danych o charakterze osobowym, dostępnych według określonych kryteriów, niezależnie od tego, czy zestaw ten jest rozproszony lub podzielony funkcjonalnie,

4) **komputerowy zbiór danych** – zbiór danych osobowych w formie elektronicznej,

5) **tradycyjny zbiór danych** – zbiór danych osobowych w formie papierowej (np. księgi, wykazy, ewidencje),

6) **przetwarzanie danych** – jakiekolwiek operacje wykonywane na danych osobowych, takie jak zbieranie, utrwalanie, przechowywanie, opracowywanie, zmienianie, udostępnianie i usuwanie, a zwłaszcza te, które wykonuje się w systemach informatycznych,

7) **Urząd** – Urząd Miasta Bielsk Podlaski z siedzibą: 17–100 Bielsk Podlaski, ul. Mikołaja Kopernika 1,

8) **Administrator Danych Osobowych** – Burmistrz Miasta Bielsk Podlaski reprezentujący Urząd, który decyduje o celach i środkach przetwarzania danych osobowych oraz monitoruje wdrożone zabezpieczenia systemu informatycznego,

9) **Administrator Bezpieczeństwa Informacji** – osoba nadzorująca przestrzeganie zasad przetwarzania i ochrony danych osobowych,

10) **Informatyk** – osoba odpowiedzialna za bezpieczeństwo danych osobowych przetwarzanych w systemach informatycznych w Urzędzie, w tym w szczególności za przeciwdziałanie dostępowi osób trzecich do systemów oraz podejmowanie odpowiednich działań w przypadku wykrycia naruszeń w tych systemach,

11) **osoba upoważniona** – osoba posiadająca upoważnienie do przetwarzania danych osobowych w określonym zakresie wydane przez Administratora Danych Osobowych,

12) **osoba uprawniona** – osoba upoważniona lub inna osoba uprawniona do przetwarzania danych osobowych na podstawie szczególnych przepisów prawa (lex specialis),

13) **osoba trzecia** – każda osoba nieuprawniona do przetwarzania danych osobowych będących w posiadaniu Administratora Danych Osobowych, a także osoba posiadająca upoważnienie wydane przez Administratora Danych Osobowych, ale podejmująca czynności w zakresie przekraczającym zakres jej upoważnienia,

14) **użytkownik** – osoba upoważniona do przetwarzania danych osobowych w określonym zakresie w systemie informatycznym,

15) **stacja robocza** - stacjonarny lub przenośny komputer, umożliwiający użytkownikowi dostęp do danych przetwarzanych w formie elektronicznej,

16) **zewnętrzne nośniki danych** - przedmiot fizyczny służący do zapisywania, przechowywania, przetwarzania i transmisji danych (np. pendrive, CD, DVD),

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

18) **zakres czynności** – zakres czynności, upoważnień, odpowiedzialności i zastępstwa wynikającego ze stanowiska służbowego i pełnionego stanowiska,

19) **zabezpieczenie systemu informatycznego** – wdrożone przez Administratora Bezpieczeństwa Informacji oraz Informatyka odpowiednie środki organizacyjne i techniczne w celu zabezpieczenia zasobów oraz ochrony danych przed dostępem, modyfikacją ujawnieniem, pozyskaniem lub zniszczeniem przez użytkownika lub osobę trzecią. Zapewnienie bezpieczeństwa systemów informatycznych oznacza, utrzymanie takich atrybutów informacji jak:
    a) **poufność** – rozumie się przez to ograniczony i ściśle zdefiniowany krąg osób mających dostęp do informacji,
    b) **integralność** – rozumie się przez to właściwość zapewniającą, że dane osobowe nie zostały zmienione lub zniszczone w sposób nieautoryzowany,
    c) **rozliczalność** – rozumie się przez to właściwość zapewniającą, że działania podmiotu mogą być przypisane w sposób jednoznaczny tylko temu podmiotowi,
    d) **uwierzytelnianie** – rozumie się przez to działanie, którego celem jest weryfikacja deklarowanej tożsamości podmiotu za pomocą:
        – **identyfikatora użytkownika** – przypisanego jednej osobie identyfikatora jednoznacznie określającego użytkownika w systemie informatycznym,
        – **hasła** – ciągu znaków (stanowiącego tajemnicę użytkownika), który w połączeniu z identyfikatorem użytkownika umożliwia uwierzytelnienie go w systemie informatycznym.

Rozdział 2
Cel i zakres polityki bezpieczeństwa danych osobowych

§ 3. Cel polityki bezpieczeństwa

1. Celem niniejszej Polityki jest określenie kierunków działań oraz wsparcia dla zapewnienia wysokiego bezpieczeństwa przetwarzania danych osobowych w Urzędzie Miasta Bielsk Podlaski.

2. Przez bezpieczeństwo danych osobowych rozumie się zapewnienie ich poufności, integralności i dostępności oraz zapewnienie rozliczalności działań podejmowanych zgodnie z niniejszą Polityką.

3. Urząd zarządza bezpieczeństwem danych osobowych w celu:

1) zapewnienia sprawnego i zgodnego z przepisami prawa wykonywania swoich zadań oraz zadań realizowanych na podstawie umów lub porozumień,

2) minimalizacji ryzyk w obszarze przetwarzania i ochrony danych osobowych wymienionych w Załączniku nr 1.

§ 4. Zakres polityki bezpieczeństwa

1. Zakres przedmiotowy niniejszej Polityki obejmuje dane osobowe przetwarzane w Urzędzie, zarówno w formie elektronicznej, jak i tradycyjnej.

2. Procedury i zasady określone w niniejszej Polityce stosuje się do wszystkich pracowników Urzędu, jak i innych osób mających dostęp do danych osobowych przetwarzanych w Urzędzie (np. osób realizujących zadania na podstawie umów zlecenia lub o dzieło, wolontariuszy, stażystów, praktykantów, serwisantów).

Rozdział 3
Organizacja przetwarzania danych osobowych

§ 5. Administrator Danych Osobowych

1. Administrator Danych Osobowych zabezpiecza dane osobowe przed ich udostępnianiem osobom nieupoważnionym, pozyskaniem przez osobę nieuprawnioną, przetwarzaniem z naruszeniem ustawy o ochronie danych osobowych, nieautoryzowaną zmianą, utratą, uszkodzeniem lub zniszczeniem.

2. Administrator Danych Osobowych przetwarza dane osobowe zgodnie z prawem oraz realizuje zadania w zakresie ochrony danych osobowych, w tym zwłaszcza:

1) podejmuje decyzje o celach i środkach przetwarzania danych osobowych z uwzględnieniem zmian w obowiązującym prawie, organizacji Urzędu oraz technik zabezpieczenia danych osobowych, w szczególności o:

a) zbieraniu danych osobowych wyłącznie dla oznaczonych, przewidzianych prawem celów,

b) przetwarzaniu danych osobowych w postaci umożliwiającej identyfikację osób, których dotyczą,

c) informowaniu osoby, której dane zostały umieszczone w zbiorze danych, o przysługujących jej prawach, zgodnie z §11 niniejszej Polityki,

d) przetwarzaniu danych osobowych nie dłużej niż jest to niezbędne do osiągnięcia celu przetwarzania,

e) zapewnieniu kontroli nad tym, jakie dane osobowe, kiedy i przez kogo zostały wprowadzone do zbioru i komu są przekazywane,

f) udostępnianiu danych osobowych innym podmiotom wyłącznie w sposób zgodny z prawem.

2) nadaje upoważnienia do przetwarzania danych osobowych w określonym indywidualnie zakresie, odpowiadającym zakresowi czynności, oraz prowadzi ich ewidencję,

3) zgłasza zbiory danych osobowych do rejestracji Generalnemu Inspektorowi Ochrony Danych Osobowych, z wyjątkiem zbiorów ustawowo zwolnionych,

4) wyznacza Administratora Bezpieczeństwa Informacji oraz określa jego zakres czynności,

5) zleca Kierownikowi Referatu Organizacyjno-Gospodarczego, by we współpracy z Administratorem Bezpieczeństwa Informacji zapewnił użytkownikom odpowiednie stanowiska pracy umożliwiające bezpieczne przetwarzanie danych,

6) w razie stwierdzenia lub podejrzenia naruszenia zasad przetwarzania i ochrony danych osobowych, a w szczególności zabezpieczeń systemu informatycznego, na wniosek Administratora Bezpieczeństwa Informacji podejmuje odpowiednie działania w celu usunięcia zagrożenia lub minimalizacji jego skutków,

7) udostępnia dane osobowe ze zbioru na żądanie uprawnionych podmiotów w przypadkach wskazanych prawem.

§ 6. Administrator Bezpieczeństwa Informacji

1. Administrator Bezpieczeństwa Informacji sprawuje nadzór nad przestrzeganiem zasad przetwarzania i ochrony danych osobowych w imieniu i na rzecz Administratora Danych Osobowych.

2. W szczególności Administrator Bezpieczeństwa Informacji jest odpowiedzialny za:

1) prowadzenie oraz aktualizację dokumentacji opisującej sposób przetwarzania danych osobowych oraz środki techniczne i organizacyjne zapewniające ochronę przetwarzanych danych osobowych, tj:

a) „Polityki bezpieczeństwa danych osobowych”, zawierającej m.in.:

- wykaz budynków i pomieszczeń tworzących obszar, w którym przetwarzane są dane osobowe - Załącznik nr 2,
- wykaz zbiorów danych osobowych wraz ze wskazaniem programów zastosowanych do ich przetwarzania - Załącznik nr 3,
- opis struktury zbiorów danych wskazujący zawartość poszczególnych pól informacyjnych i powiązania między nimi - Załącznik nr 4,

b) „Instrukcji zarządzania systemem informatycznym służącym do przetwarzania danych osobowych”,

2) nadzorowanie przestrzegania zasad określonych w „Polityce bezpieczeństwa danych osobowych” i „Instrukcji zarządzania systemem informatycznym służącym do przetwarzania danych osobowych”,

3) szkolenie osób dopuszczonych do przetwarzania danych osobowych lub przebywania w obszarze przetwarzania danych osobowych z zakresu zasad przetwarzania i ochrony tych danych oraz zasad bezpieczeństwa informatycznego w oparciu o przygotowywane przez siebie materiały szkoleniowe oraz prowadzenie adekwatnej dokumentacji w tym zakresie (np. potwierdzenie przeszkolenia),

4) nadzorowanie prawidłowości udostępniania danych osobowych odbiorcom danych,

5) nadzorowanie zamieszczania w umowach z użytkownikami upoważnionymi do przetwarzania danych osobowych, firmami, którym powierzono przetwarzanie danych osobowych lub konserwacje urządzeń służących do przetwarzania danych oraz pracownikami tych firm, a także w innych dokumentach odpowiednich zapisów dotyczących ochrony danych osobowych (Przykładową treść takiego zapisu stanowi Załącznik nr 5 do niniejszej Polityki),

6) nadzorowanie wdrożenia adekwatnych do zagrożeń środków fizycznych, a także organizacyjnych i technicznych służących zapewnieniu bezpieczeństwa,

7) nadzorowanie obiegu oraz przechowywania dokumentów zawierających dane osobowe w zakresie związanych z bezpieczeństwem tych danych osobowych,

8) koordynowanie kontroli wewnętrznych z zakresu przestrzegania przepisów o ochronie danych osobowych, w tym prowadzenie szczegółowej dokumentacji z kontroli dot.:

- **a)** zakresu przestrzegania przepisów o ochronie danych osobowych,
- **b)** stwierdzonych naruszeń bezpieczeństwa danych osobowych, obejmującej m.in. analizę sytuacji, okoliczności przyczyn, które doprowadziły do naruszenia bezpieczeństwa danych (jeśli takie wystąpiło).

9) podejmowanie lub wnioskowanie o podjęcie odpowiednich działań w przypadku naruszenia lub podejrzenia naruszenia bezpieczeństwa systemu informatycznego oraz prowadzenie adekwatnej dokumentacji w tym zakresie (np. opis incydentu, dokumentacja dot. reakcji na incydent).

§ 7. Informatyk

Informatyk realizuje zadania w zakresie zarządzania i bieżącego nadzoru nad systemem informatycznym Administratora Danych Osobowych, w szczególności:

1) zarządza systemem informatycznym, w którym przetwarzane są dane osobowe, posługując się hasłem dostępu do wszystkich stacji roboczych z poziomu administratora,

2) zarządza systemem komunikacji w sieci komputerowej oraz przesyłania danych za pośrednictwem urządzeń teletransmisji,

3) nadzoruje funkcjonowanie mechanizmów uwierzytelniania użytkowników w systemie informatycznym służącym do przetwarzania danych osobowych oraz kontroli dostępu do danych osobowych,

4) wykonuje kopie bezpieczeństwa komputerowych zbiorów danych zgodnie z zasadami określonymi w „Instrukcji zarządzania systemem informatycznym służącym do przetwarzania danych osobowych”, oraz okresowo sprawdza je pod kątem ich dalszej przydatności do odtwarzania danych w przypadku awarii systemu informatycznego,

5) przydziela każdemu użytkownikowi indywidualny identyfikator oraz hasło do systemu informatycznego oraz dokonuje ewentualnych modyfikacji uprawnień, a także w porozumieniu z Kierownikiem Referatu Organizacyjno-Gospodarczego usuwa konta użytkowników zgodnie z zasadami określonymi w „Instrukcji zarządzania systemem informatycznym służącym do przetwarzania danych osobowych”,

6) zmienia okresowo hasła dostępu użytkowników do systemu informatycznego w przypadkach, gdy system informatyczny nie wymusza okresowej zmiany haseł użytkowników określonej w „Instrukcji zarządzania systemem informatycznym służącym do przetwarzania danych osobowych”,

7) osobiście wykonuje lub sprawuje nadzór nad wykonywaniem: napraw, konserwacji oraz likwidacji urządzeń komputerowych, które mogą zawierać dane osobowe.

§ 8. Kierownik Referatu Organizacyjno-Gospodarczego

Kierownik Referatu Organizacyjno-Gospodarczego realizuje następujące zadania w zakresie ochrony danych osobowych:

1) występuje z wnioskiem do Administratora Danych Osobowych o nadanie, modyfikację lub odwołanie upoważnienia do przetwarzania danych osobowych,

2) prowadzi ewidencję upoważnień do przetwarzania danych osobowych,

3) przechowuje upoważnienia do przetwarzania danych osobowych w aktach osobowych,

4) informuje Administratora Bezpieczeństwa Informacji o nadaniu, modyfikacji lub odwołaniu przez Administratora Danych Osobowych upoważnienia do przetwarzania danych osobowych,

5) nadzoruje wykonywanie kopii bezpieczeństwa komputerowych zbiorów danych, ich przechowywanie oraz okresowe sprawdzanie pod kątem ich dalszej przydatności do odtwarzania danych w przypadku awarii systemu,

6) nadzoruje przeprowadzanie przeglądów, konserwacji oraz uaktualniania systemów służących do przetwarzania danych osobowych oraz wszystkich innych czynności wykonywanych przez Informatyków na komputerowych zbiorach danych.

§ 9. Kierownicy referatów

Kierownicy referatów są odpowiedzialni za:

1) nadzorowanie przestrzegania zasad przetwarzania i ochrony danych osobowych przyjętych w Urzędzie przez podległy personel, w szczególności:

- **a)** przetwarzania danych osobowych w celu i zakresie określonym w imiennym upoważnieniu do przetwarzania danych osobowych,
- **b)** stosowania przydzielonych im indywidualnych identyfikatorów dostępu do systemu informatycznego przez podległych pracowników,
- **c)** przeciwdziałania dostępowi osób nieuprawnionych do danych osobowych i systemu informatycznego, w którym są przetwarzane,
- **d)** prawidłowego zabezpieczania danych osobowych oraz miejsc ich przechowywania w trakcie i po zakończeniu pracy,

2) niedopuszczenie do używania zewnętrznych nośników danych do celów innych niż niezbędne do realizacji zadań referatu lub tworzenia kopii bezpieczeństwa, z wyjątkiem sytuacji gdy jest to niezbędne ze względu na specyfikę zadania,

3) współdziałanie z Administratorem Bezpieczeństwa Informacji w zakresie przestrzegania zasad przetwarzania i ochrony danych osobowych w Urzędzie oraz identyfikacji i analizy ryzyk z tym związanych,

4) niezwłoczne informowanie Administratora Bezpieczeństwa Informacji, o każdym stwierdzeniu lub podejrzeniu naruszenia bezpieczeństwa danych osobowych lub systemu informatycznego, w którym są przetwarzane oraz współdziałanie przy usuwaniu skutków takiego naruszenia.

§ 10. Osoby przetwarzające dane osobowe

1. Każda osoba przetwarzająca dane osobowe posiada odpowiednie upoważnienie do przetwarzania danych osobowych zawierające: imię i nazwisko, datę nadania i okres jego obowiązywania, zakres danych, które osoba może przetwarzać (zbiory danych) oraz identyfikator w przypadku gdy dane osobowe są przetwarzane w systemie informatycznym, (wzór upoważnienia stanowi Załącznik nr 6 do niniejszej Polityki),

2. Każda osoba upoważniona do przetwarzania danych osobowych jest zobowiązana do:

1) przetwarzania danych osobowych wyłącznie w zakresie ustalonym indywidualnie przez Administratora Danych Osobowych w upoważnieniu i tylko w celu wykonywania nałożonych na nią obowiązków,

2) poznania i bezwzględnego przestrzegania obowiązujących u Administratora Danych Osobowych zasad przetwarzania i ochrony danych osobowych oraz bezpieczeństwa systemu informatycznego,

3) zachowania w tajemnicy danych, które przetwarza oraz sposobów ich zabezpieczenia przez cały okres zatrudnienia u Administratora Danych Osobowych, a także po ustaniu stosunku pracy lub odwołaniu z pełnionej funkcji,

4) korzystania z systemu informatycznego Administratora Danych Osobowych w sposób zgodny ze wskazówkami zawartymi w instrukcjach obsługi urządzeń wchodzących w skład systemu informatycznego, oprogramowania i nośników oraz zasadami przyjętymi w Urzędzie,

5) zabezpieczania danych osobowych oraz informacji o zabezpieczeniach systemu informatycznego przed ich udostępnianiem osobom nieuprawnionym, nieuprawnioną modyfikacją, utratą lub zniszczeniem.

§ 11. Osoby, których dane dotyczą

1. Każdej osobie, której dotyczą dane osobowe przetwarzane u Administratora Danych Osobowych, przysługuje prawo do:

1) dostępu do treści przetwarzanych danych osobowych tej osoby,

2) poprawiania treści przetwarzanych danych osobowych tej osoby (bez zbędnej zwłoki), tj. do uzupełnienia, uaktualnienia, sprostowania danych osobowych, a także żądania czasowego lub trwałego wstrzymania ich przetwarzania bądź usunięcia ze zbioru, jeżeli są one niekompletne, nieaktualne, nieprawdziwe lub zostały zebrane z naruszeniem ustawy, albo są już zbędne dla realizacji celu, dla którego zostały zebrane,

3) kontroli przetwarzanych danych osobowych tej osoby, w szczególności uzyskania informacji o:

a) istnieniu zbioru danych osobowych i jego administratorze (wraz z siedzibą),

b) celu, zakresie i sposobie przetwarzania danych osobowych,

c) terminie rozpoczęcia przetwarzania danych osobowych w zbiorze,

d) treści jej danych osobowych (podanej w powszechnie zrozumiałej formie),

e) źródle, z jakiego pochodzą te dane (chyba że Administrator Danych Osobowych jest zobowiązany do zachowania w tym zakresie tajemnicy państwowej, służbowej lub zawodowej),

f) sposobie udostępniania jej danych osobowych (w szczególności o odbiorcach lub kategoriach odbiorców, którym dane są udostępniane),

g) przesłankach podjęcia rozstrzygnięcia indywidualnej sprawy uwzględniającej wniosek osoby, której dane dotyczą, podjętego podczas zawierania lub wykonywania umowy

wyłącznie na podstawie operacji na danych osobowych prowadzonych w systemie informatycznym,

h) obowiązku lub dobrowolności podania danych, a także jeśli taki obowiązek istnieje – o jego podstawie prawnej,

i) prawie dostępu do treści swoich danych i ich poprawiania, o których mowa w pkt. 1 i 2,

j) wniesienia sprzeciwu wobec ich wykorzystania w celach marketingowych lub przekazania innemu administratorowi danych (z uwzględnieniem wyjątków ustawowych),

k) udzielenia informacji o przysługujących prawach osobie, której dane dotyczą, na jej wniosek w terminie 30 dni.

2. W przypadku zbierania danych osobowych bezpośrednio od osoby, której one dotyczą, na jej żądanie udziela się informacji wskazanych w ust. 1 pkt 3 lit. a-f, ale nie częściej niż raz na 6 miesięcy.

3. Informacja, o której mowa w ust. 1 pkt. 3, powinna być udzielana w zrozumiałej formie oraz na piśmie, jeśli osoba o to wnioskuje.

4. W przypadku, gdy w niedużym odstępie czasowym dochodzi do ponownego lub kolejnego zbierania danych tej samej osoby do tych samych celów, można powołać się na fakt wcześniejszego udzielenia informacji, o których mowa w ust. 1 pkt. 3.

5. Obowiązek informacyjny nie występuje w przypadku, gdy:

1) ze względu na okoliczności przekazania danych osobowych do przetwarzania w zbiorze zachodzi pewność (tj. obiektywna świadomość), że osoba, której dane dotyczą, posiada wszystkie informacje, o których mowa w ust. 1 pkt 3,

2) dane są przetwarzane dla celów naukowych, dydaktycznych, historycznych, statystycznych lub archiwalnych, a udzielenie informacji pociągałoby za sobą nakłady niewspółmierne z zamierzonym celem,

3) przekazanie informacji spowodowałoby:

a) ujawnienie wiadomości zawierających informacje niejawne,

b) zagrożenie dla obronności lub bezpieczeństwa państwa, życia lub zdrowia ludzi lub bezpieczeństwa publicznego,

c) zagrożenie dla podstawowego interesu gospodarczego lub finansowego państwa,

d) istotne naruszenie dóbr osobistych osób, których dane dotyczą lub innych osób.

Rozdział 4
OKREŚLENIE ŚRODKÓW TECHNICZNYCH I ORGANIZACYJNYCH, NIEZBĘDNYCH DLA ZAPEWNIENIA POUFNOŚCI, INTEGRALNOŚCI I ROZLICZALNOŚCI PRZETWARZANYCH DANYCH OSOBOWYCH

§ 12. Zachowanie poufności

1. W przypadku naboru na wolne stanowiska należy zwracać uwagę miedzy innymi na takie cechy kandydata, jak uczciwość, odpowiedzialność, przewidywalność zachowań.

2. Ryzyko utraty bezpieczeństwa danych przetwarzanych przez Administratora Danych Osobowych, pojawiające się ze strony osób trzecich, które mają dostęp do danych osobowych (np. serwisanci, usługodawcy), jest minimalizowane przez wprowadzanie do podpisanych umów zapisów o powierzeniu przetwarzania danych osobowych.

3. Ryzyko ze strony osób, które potencjalnie mogą w łatwiejszy sposób uzyskać dostęp do danych osobowych (np. konserwatorzy i osoby sprzątające pomieszczenia Administratora Danych Osobowych), jest minimalizowane przez zobowiązywanie ich do zachowania tajemnicy na podstawie odrębnych, pisemnych oświadczeń (wzór oświadczenia stanowi Załącznik nr 7 do niniejszej Polityki)

§ 13. Środki techniczne

Opis środków technicznych znajduje się w „Instrukcji zarządzania systemem informatycznym służącym do przetwarzania danych osobowych".

§ 14. Szkolenia w zakresie ochrony danych osobowych

1. Administrator Bezpieczeństwa Informacji jest odpowiedzialny za szkolenie:

1) każdej osoby, która ma zostać dopuszczona do przetwarzania danych osobowych,

2) wszystkich osób upoważnionych do przetwarzania danych osobowych w przypadku:

a) zmiany zasad przetwarzania i ochrony danych osobowych,

b) stwierdzenia istotnych lub powtarzalnych naruszeń zasad przetwarzania i ochrony danych osobowych lub naruszenia bezpieczeństwa systemu informatycznego,

3) osób dopuszczonych do przebywania w obszarze przetwarzania danych osobowych,

4) osób innych niż upoważnione do przetwarzania danych osobowych, jeśli pełnione przez nie funkcje wiążą się z przetwarzaniem i ochroną danych osobowych.

2. Tematyka szkoleń jest dostosowana do stanowiska/funkcji danej osoby i obejmuje:

1) zasady przetwarzania i ochrony danych osobowych, sporządzania i przechowywania ich kopii, niszczenia wydruków i/lub zapisów na zewnętrznych nośnikach danych,

2) sposoby ochrony danych osobowych przed osobami nieuprawnionymi i procedury udostępniania danych osobom, których one dotyczą,

3) obowiązki osób upoważnionych do przetwarzania danych osobowych,

4) odpowiedzialność za naruszenie zasad przetwarzania i ochrony danych osobowych,

5) zasady powiadamiania i reakcji na stwierdzenie lub podejrzenie naruszenia zasad przetwarzania i ochrony danych osobowych,

6) zasady i procedury określone w „Polityce bezpieczeństwa danych osobowych" i „Instrukcji zarządzania systemem informatycznym służącym do przetwarzania danych osobowych".

§ 15. Odpowiedzialność osób upoważnionych do przetwarzania danych osobowych

1. Niezastosowanie się do obowiązujących u Administratora Danych zasad bezpieczeństwa danych osobowych, w szczególności świadome naruszenie procedur ochrony danych przez pracowników upoważnionych do przetwarzania danych osobowych, może być potraktowane jako ciężkie naruszenie obowiązków pracowniczych, skutkujące rozwiązaniem stosunku pracy bez wypowiedzenia na podstawie art. 52 Kodeksu pracy.

2. Niezależnie od rozwiązania stosunku pracy osoby popełniające przestępstwo będą pociągane do odpowiedzialności karnej zwłaszcza na podstawie art. 51-52 ustawy oraz art. 266 Kodeksu karnego. Przykładowo przestępstwo można popełnić wskutek:

1) stworzenia możliwości dostępu do danych osobowych osobom nieupoważnionym albo osobie nieupoważnionej,

2) niezabezpieczenia nośnika lub komputera przenośnego,

3) zapoznania się z hasłem innego pracownika wskutek wykonania nieuprawnionych operacji w systemie informatycznym Administratora Danych Osobowych.

§ 16. Przeglądy i aktualizacje „Polityki bezpieczeństwa danych osobowych"

1. Niniejsza Polityka podlega przeglądowi pod kątem aktualności i stosowalności nie rzadziej niż raz do roku. Przeglądu dokonuje Administrator Bezpieczeństwa Informacji.

2. Niniejsza Polityka podlega aktualizacji każdorazowo w przypadku:

1) likwidacji, utworzenia lub zmiany zawartości informacyjnej zbioru,

2) zmiany lokalizacji zbioru,

3) zmiany opiekuna zbioru lub administratora informacji,

4) zmiany przepisów prawa dotyczącego ochrony danych osobowych, wymagającej aktualizacji niniejszej Polityki,

5) innych znaczących zmian w funkcjonowaniu Urzędu dotyczących danych osobowych.

3. Aktualizacji niniejszej Polityki dokonuje Administrator Bezpieczeństwa Informacji. Zatwierdzenia zaktualizowanej Polityki dokonuje Administrator Danych Osobowych.

4. Administrator Bezpieczeństwa Informacji po uzgodnieniu z Administrator Danych Osobowych może, stosownie do potrzeb, przeprowadzić wewnętrzną kontrolę zgodności przetwarzania danych z przepisami o ochronie danych osobowych. Zakres, przebieg i rezultaty kontroli są dokumentowane na piśmie w protokole podpisywanym przez Administratora Bezpieczeństwa Informacji i Administratora Danych Osobowych.

Rozdział 5
POSTANOWIENIA KOŃCOWE

§ 17.

1. Niniejsza Polityka zostaje wprowadzona zarządzeniem Burmistrza Miasta Bielsk Podlaski.

2. Każda osoba upoważniona do przetwarzania danych osobowych zobowiązana jest zapoznać się z niniejszym dokumentem przed dopuszczeniem do przetwarzania danych oraz złożyć stosowne oświadczenie, potwierdzające znajomość jego treści.