Zarządzenie nr 106/2015
Burmistrza Miasta Radymna
z dnia 08 grudnia 2015 roku

w sprawie wprowadzenia „Polityki bezpieczeństwa i instrukcji zarządzania systemem informatycznym służącym do przetwarzania danych osobowych w Urzędzie Miasta Radymna".

Na podstawie art. 36 ust. 2 ustawy z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (Dz.U. z 2014 r. poz. 1182 ze zm.) oraz § 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. z 2004 r. nr 100, poz. 1024) zarządzam, co następuje:

§ 1

Wprowadzam „Politykę bezpieczeństwa i instrukcję zarządzania systemem informatycznym służącym do przetwarzania danych osobowych w Urzędzie Miasta Radymna" zwaną dalej „Polityką bezpieczeństwa", która stanowi załącznik do niniejszego zarządzenia.

§ 2

Zobowiązuję pracowników Urzędu Miasta Radymna do stosowania zasad określonych w Polityce bezpieczeństwa.

§ 3

Nadzór nad wykonaniem zarządzenia powierzam Sekretarzowi Miasta Radymna .

§ 4

Traci moc Zarządzenie Nr 66/2007 Burmistrza Miasta Radymno z dnia 28 grudnia 2007 r. w sprawie wprowadzenia Polityki Bezpieczeństwa dotyczącej ochrony danych osobowych przetwarzanych w Urzędzie Miasta Radymno.

§ 5

Zarządzenie wchodzi w życie z dniem podpisania.

Burmistrz
Miasta Radymna
Krzysztof Roman

Załącznik nr 1 do
Zarządzenia Nr 106/2015 Burmistrza
Miasta Radymna
z dnia 08 grudnia 2015 r.

Polityka bezpieczeństwa i instrukcja zarządzania systemem informatycznym służącym do przetwarzania danych osobowych w Urzędzie Miasta Radymna

§ 1
Postanowienia ogólne

1. Polityka bezpieczeństwa przetwarzania danych osobowych w Urzędzie Miasta Radymna zwana dalej „Polityką" została opracowana w związku z § 3 ust. 1 rozporządzenia Ministra Spraw Wewnętrznych i Administracji z dnia 29 kwietnia 2004 r. w sprawie dokumentacji przetwarzania danych osobowych oraz warunków technicznych i organizacyjnych, jakim powinny odpowiadać urządzenia i systemy informatyczne służące do przetwarzania danych osobowych (Dz. U. z 2004 r. nr 100, poz. 1024).
2. Celem Polityki jest stworzenie podstaw dla właściwego wykonywania obowiązków Administratora Danych Osobowych w zakresie zabezpieczenia i prawidłowej ochrony przetwarzanych danych osobowych.
3. Polityka określa zasady przetwarzania danych osobowych oraz ich zabezpieczania, jako zestaw praw, reguł i zaleceń, regulujących sposób ich zarządzania i ochrony w Urzędzie Miasta Radymna.
4. Polityka zawiera informacje dotyczące rozpoznawania procesów przetwarzania danych osobowych oraz wprowadzonych zabezpieczeń technicznych i organizacyjnych, zapewniających ochronę danych osobowych.
5. Niniejszą Politykę stosuje się do:
   1) Danych osobowych:
      a. przetwarzanych w systemach informatycznych,
      b. przetwarzanych na zewnętrznych nośnikach informacji,
      c. przetwarzanych tradycyjnie.
   2) Informacji dotyczących bezpieczeństwa przetwarzania danych osobowych:
      a. służących do uwierzytelnienia w systemach informatycznych, w których są przetwarzane dane osobowe,
      b. dotyczących wdrożonych zabezpieczeń technicznych i organizacyjnych.
6. Bez względu na zajmowane stanowisko, miejsce wykonywanej pracy oraz charakter stosunku pracy, zasady określone w niniejszej Polityce oraz dokumentach powiązanych powinny być znane i stosowane przez pracowników oraz w niezbędnym zakresie przez współpracowników przetwarzających dane osobowe, których administratorem jest Urząd Miasta w Radymna.
7. Obszarem przetwarzania danych osobowych w Urzędzie Miasta Radymna jest budynek Urzędu, mieszczący się przy ul. Lwowska 20 w Radymnie.

§ 2
Definicje

Użyte w niniejszej Polityce pojęcia są wspólne dla wszystkich dokumentów powiązanych z niniejszą Polityką oraz dla wszystkich pozostałych dokumentów, które zostały przyjęte przez Urząd Miasta Radymna, w zakresie ochrony danych osobowych w Urzędzie.

1. **Administrator Danych Osobowych (ADO)** – podmiot, który decyduje o środkach i celach przetwarzania danych osobowych, reprezentowany przez Burmistrza Miasta Radymna.
2. **Administrator Bezpieczeństwa Informacji (ABI)** – osoba wyznaczona przez Burmistrza Miasta Radymna, odpowiedzialna za nadzorowanie stosowania środków technicznych i organizacyjnych

zapewniających ochronę przetwarzanych danych osobowych, w tym w szczególności za przeciwdziałanie dostępowi osób trzecich do systemu, w którym przetwarzane są dane osobowe oraz za podejmowanie odpowiednich działań w przypadku wykrycia naruszeń w systemie ochrony danych osobowych.

3. **Administrator Systemów Informatycznych (ASI)** – informatyk, odpowiedzialny za właściwe funkcjonowanie infrastruktury informatycznej, na którą składa się sieć, sprzęt informatyczny oraz systemy i aplikacje informatyczne.
4. **Bezpieczeństwo przetwarzania danych osobowych** – zachowanie poufności, integralności i rozliczalności danych osobowych; dodatkowo mogą być brane pod uwagę inne własności, takie jak dostępność, autentyczność, niezaprzeczalność i niezawodność.
5. **Dane osobowe** – każda informacja dotycząca żyjącej osoby fizycznej, która pozwala na bezpośrednią lub pośrednią identyfikację tej osoby.
6. **GIODO** – Generalny Inspektor Ochrony Danych Osobowych.
7. **Integralność danych** – właściwość zapewniająca, że dane nie zostały zmienione lub zniszczone w sposób nieautoryzowany.
8. **Naruszenie ochrony danych osobowych** – zamierzone lub przypadkowe naruszenie środków technicznych i organizacyjnych, zastosowanych w celu ochrony danych osobowych. W szczególności, gdy stan urządzenia, zawartość zbioru danych osobowych, ujawnione metody pracy, sposób działania programu lub jakość komunikacji w sieci telekomunikacyjnej mogą wskazywać na naruszenie ochrony danych osobowych.
9. **Poufność** – właściwość zapewniająca, że informacja jest dostępna jedynie osobom upoważnionym.
10. **Przetwarzanie danych osobowych** – jakiekolwiek operacje wykonywane na danych osobowych, takie jak zbieranie, utrwalanie, opracowywanie, przechowywanie, zmieniane, udostępnianie i usuwanie, a zwłaszcza te, które wykonuje się w systemach informatycznych.
11. **Rozporządzenie** - Rozporządzenie Ministra Spraw Wewnętrznych i Administracji z dnia 29 kwietnia 2004 r. w sprawie dokumentacji przetwarzania danych osobowych oraz warunków technicznych i organizacyjnych, jakim powinny odpowiadać urządzenia i systemy informatyczne służące do przetwarzania danych osobowych (Dz. U. z 2004 r. nr 100, poz. 1024).
12. **Rozliczalność** – właściwość zapewniająca, że działania podmiotu mogą być przypisane w sposób jednoznaczny tylko temu podmiotowi.
13. **System informatyczny** – zespół współpracujących urządzeń, programów, procedur przetwarzania informacji i narzędzi programowych zastosowanych w celu przetwarzania danych.
14. **Urząd** – Urząd Miasta Radymna.
15. **Ustawa** – ustawa z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (Dz.U. z 2014 r., poz. 1182 ze zm.),
16. **Użytkownik systemu** – osoba upoważniona do bezpośredniego dostępu do danych osobowych przetwarzanych w systemie informatycznym, która posiada ustalony identyfikator i hasło.
17. **Użytkownik zewnętrzny** – osoba nie będąca pracownikiem lub stażystą Urzędu, posiadająca uprawnienia do przetwarzania informacji, w związku z wykonywaniem czynności na rzecz Urzędu.
18. **Właściciel zasobów danych osobowych** – osoba kierująca komórką organizacyjną odpowiedzialną za ochronę danych osobowych przetwarzanych w podległej komórce. Jest ona zobowiązana do stosowania środków technicznych i organizacyjnych, zapewniających ochronę przetwarzanych danych osobowych odpowiednią do zagrożeń oraz kategorii danych objętych ochroną, a w szczególności zabezpieczyć dane przed ich udostępnieniem osobom nieupoważnionym, zabraniem przez osobę nieuprawnioną, przetwarzaniem z naruszeniem ustawy oraz nieautoryzowaną zmianą, utratą, uszkodzeniem lub zniszczeniem.
19. **Zbiór danych osobowych** – każdy, posiadający strukturę zestaw danych o charakterze osobowym, dostępnych według określonych kryteriów, niezależnie od tego, czy zestaw ten jest rozproszony, czy podzielony funkcjonalnie.
20. **Zbiór nieinformatyczny** - każdy, posiadający strukturę zestaw danych o charakterze osobowym, dostępnych według określonych kryteriów, niezależnie od tego, czy zestaw ten jest rozproszony, czy podzielony funkcjonalnie, prowadzony poza systemem informatycznym, w szczególności w formie kartoteki, skorowidza, księgi, wykazu lub innego zbioru ewidencyjnego.

§ 3
Deklaracja Administratora Danych Osobowych

ADO zobowiązuje się do podjęcia odpowiednich kroków, mających na celu zapewnienie prawidłowej ochrony danych osobowych, w szczególności do zapewnienia, że przez cały okres ich przetwarzania dane będą;

1) Przetwarzane zgodnie z prawem,
2) Zbierane dla oznaczonych, zgodnych z prawem celów i nie poddawane dalszemu przetwarzaniu, niezgodnemu z tymi celami,
3) Merytorycznie poprawne i adekwatne w stosunku do celów, w jakich są przetwarzane,
4) Przechowywane w postaci umożliwiającej identyfikację osób, których dotyczą, nie dłużej niż jest to niezbędne do osiągnięcia celu przetwarzania,
5) Zabezpieczone środkami technicznymi i organizacyjnymi, które zapewniają rozliczalność, integralność oraz poufność danych.

§ 4
Przegląd dokumentacji z zakresu ochrony danych osobowych

1. Niniejsza Polityka oraz dokumenty z nią powiązane powinny być aktualizowane wraz ze zmieniającymi się przepisami prawnymi o ochronie danych osobowych oraz zmianami faktycznymi w ramach Urzędu, które mogą powodować, że zasady ochrony danych osobowych określone w obowiązujących dokumentach będą nieaktualne lub nieadekwatne.
2. Fakty wystąpienia poważnych naruszeń ochrony danych osobowych powinny skutkować zmianami w dokumencie niniejszej Polityki i dokumentach powiązanych.
3. Zmiany niniejszej Polityki wymagają przeglądu innych dokumentów obowiązujących w Urzędzie, dotyczących ochrony danych osobowych.
4. Wszystkie znaczące zmiany Polityki powinny być zatwierdzane przez Burmistrza Miasta Radymna.

§ 5
Zarządzanie ochroną danych osobowych

1. Realizację zamierzeń w celu zwiększenia skuteczności ochrony danych osobowych powinny zagwarantować następujące założenia:
   1) Przypisanie użytkownikom określonych atrybutów pozwalających na ich identyfikację w systemach informatycznych (identyfikatory, hasła), umożliwiających im dostęp do danych osobowych, stosownie do zakresu upoważnienia i indywidualnych poziomów uprawnień,
   2) Okresowe sprawdzanie przestrzegania przez użytkowników wdrożonych metod postępowania przy przetwarzaniu danych osobowych,
   3) Podejmowanie niezbędnych działań, w celu likwidacji słabych ogniw w systemie ochrony danych osobowych,
   4) Śledzenie osiągnięć w dziedzinie bezpieczeństwa systemów informatycznych i – w miarę możliwości organizacyjnych i techniczno – finansowych – wdrażanie nowych narzędzi i metod pracy oraz sposobów zarządzania systemami informatycznymi, służących wzmocnieniu bezpieczeństwa przetwarzania danych osobowych.
2. Na każdym etapie przetwarzania danych osobowych należy brać pod uwagę w niezbędnym zakresie integralność, poufność oraz rozliczalność dla przetwarzanych danych osobowych.
3. Administrator Danych Osobowych powinien być zapewniony, że pracownicy, wykonawcy oraz użytkownicy zewnętrzni:
   1) Są odpowiednio wprowadzani w swoje obowiązki i odpowiedzialności związane z ochroną danych osobowych i ich przetwarzaniem przed przyznaniem im dostępu do danych osobowych,
   2) Otrzymali zalecenia określające wymagania w zakresie bezpieczeństwa danych osobowych związane z ich obowiązkami w Urzędzie,

3) Będą wypełniali zalecenia i warunki zatrudnienia, które uwzględniają zasady ochrony danych osobowych oraz właściwe metody pracy,
4) W sposób ciągły utrzymywali odpowiednie umiejętności i kwalifikacje.

4. Za bieżącą, operacyjną ochronę danych osobowych odpowiada każda osoba przetwarzająca te dane w zakresie zgodnym z zakresem upoważnienia, kompetencjami lub rolą sprawowaną w procesie przetwarzania danych.

§ 6
Dokumenty powiązane

Na dokumentację ochrony danych osobowych, powiązaną z niniejszą Polityką składają się:
1) Ewidencja osób upoważnionych przez ADO do przetwarzania danych osobowych,
2) Ewidencja zbiorów danych osobowych przetwarzanych w Urzędzie Miejskim w Radymnie oraz programów zastosowanych do ich przetwarzania,
3) Oryginały i kopie dokumentów dotyczących ochrony danych osobowych (w tym kopie wniosków o rejestrację/aktualizację zbiorów danych do GIODO oraz uchwały, zarządzenia, polityki itd. dotyczące ochrony danych osobowych).

§ 7
Odpowiedzialność Administratora Danych Osobowych

1. Administrator Danych Osobowych jest odpowiedzialny za przetwarzanie i ochronę danych osobowych, zgodnie z przepisami prawa, w tym wprowadzenie do stosowania procedur postępowania zapewniających prawidłowe przetwarzanie danych osobowych, rozumiane jako ochronę danych przed ich udostępnieniem osobom nieupoważnionym, zmianą lub zabraniem przez osobę nieuprawnioną, przetwarzaniem z naruszeniem przepisów ustawy oraz utratą, uszkodzeniem lub zniszczeniem.
2. Do kompetencji ADO należy w szczególności:
   1) Wyznaczenie Administratora Bezpieczeństwa Informacji,
   2) Wyznaczanie właścicieli zasobów danych osobowych,
   3) Określanie celów i strategii ochrony danych osobowych,
   4) Podział zadań i obowiązków związanych z organizacją ochrony danych osobowych.
3. Do obowiązków ADO należy:
   1) Zapewnienie szkoleń dla pracowników w zakresie przepisów o ochronie danych osobowych oraz zagrożeń związanych z ich przetwarzaniem,
   2) Przyjmowanie i zatwierdzanie niezbędnych, wymaganych przez przepisy prawa dokumentów regulujących ochronę danych osobowych w urzędzie,
   3) Nadawanie upoważnień pracownikom Urzędu oraz użytkownikom zewnętrznym do przetwarzania danych osobowych,
   4) Zapewnienie środków finansowych na ochronę fizyczną pomieszczeń, w których przetwarzane są dane osobowe,
   5) Zapewnienie środków finansowych niezbędnych do ochrony danych osobowych przetwarzanych w systemach informatycznych oraz zbiorach tradycyjnych,
   6) Zapewnienie środków finansowych na merytoryczne przygotowanie osób odpowiedzialnych za nadzór nad ochroną danych osobowych.

§ 8
Odpowiedzialność Administratora Bezpieczeństwa Informacji

1. Administrator Danych Osobowych wyznacza Administratora Bezpieczeństwa Informacji, który nadzoruje przestrzeganie zasad ochrony danych osobowych, zarówno w systemach informatycznych, jak również w zbiorach prowadzonych w formie papierowej i elektronicznej.
2. Do kompetencji Administratora Bezpieczeństwa Informacji należy:
   1) Określenie zasad ochrony danych osobowych,
   2) Wnioskowanie o ukaranie osób winnych naruszenia przepisów i zasad dotyczących ochrony danych osobowych.
3. Do obowiązków ABI należy:
   1) Nadzór nad wdrożeniem stosownych środków organizacyjnych, technicznych i fizycznych w celu ochrony przetwarzanych danych osobowych,
   2) Nadawanie, cofanie oraz zmienianie uprawnień do przetwarzania danych osobowych na wniosek Właścicieli zasobów po akceptacji ADO dla pracowników oraz użytkowników zewnętrznych,
   3) Nadzór nad zapewnieniem przez właścicieli zasobów danych osobowych dostosowania funkcjonalności systemów przetwarzających dane osobowe do wymagań określonych w rozporządzeniu,
   4) Prowadzenie dokumentacji opisującej zastosowaną ochronę danych osobowych (niniejsza Polityka oraz wynikające z niej instrukcje i procedury), w tym zapewnienie ich publikacji i dystrybucji oraz prowadzenie dokumentacji o której mowa w § 6,
   5) Reprezentowanie Urzędu w kontaktach z GIODO,
   6) Przygotowywanie zgłoszeń zbiorów danych do rejestracji w GIODO,
   7) Reagowanie na zgłaszane incydenty związane z naruszeniem ochrony danych osobowych oraz analizowanie ich przyczyn i kierowanie wniosków dotyczących ukarania winnych naruszeń,
   8) Sprawdzanie wypełniania obowiązków technicznych i organizacyjnych związanych z ochroną danych osobowych.
4. ABI w zakresie realizacji swoich obowiązków ma prawo żądać od pozostałych osób, bez względu na rangę zajmowanego stanowiska udzielania natychmiastowej pomocy w razie stwierdzenia, że doszło do naruszenia przepisów o ochronie danych osobowych, które może skutkować postawieniem Urzędu albo Administratora Danych Osobowych popełnienia jednego z przestępstw wymienionych w rozdziale 8 Ustawy.
5. Sprawowanie nadzoru nad przestrzeganiem zastosowanych środków technicznych i organizacyjnych zapewniających ochronę przetwarzanym danym osobowym adekwatną do zagrożeń oraz kategorii danych objętych ochroną powinno być głównym zadaniem ABI.
6. Zapewnienie realizacji obowiązku zgłoszenia i aktualizacji zbiorów danych osobowych do rejestracji GIODO,
7. Sporządzanie sprawozdań z realizacji zadań z zakresu ochrony danych osobowych.

§ 9

Odpowiedzialność Administratora Systemów Informatycznych

1. Rolę ASI pełni informatyk Urzędu,
2. Do kompetencji ASI należy:
   1) Zabezpieczenie systemów przetwarzania danych osobowych zgłoszonych ASI, w zależności od kategorii przetwarzanych w tym systemie danych.
   2) Zapewnienie poufności, integralności, dostępności i rozliczalności danych przetwarzanych w systemach informatycznych.
3. Do obowiązków ASI należy:
   1) Bieżący nadzór oraz zapewnienie optymalnej ciągłości działania systemu informatycznego,
   2) Reagowanie bez zbędnej zwłoki, w przypadku naruszenia bądź powstania zagrożenia bezpieczeństwa danych osobowych,
   3) Przeciwdziałanie próbom naruszenia bezpieczeństwa danych osobowych,
   4) Zapewnienie zgodności wszystkich wdrażanych systemów przetwarzania danych osobowych z Ustawą oraz niniejszą Polityką,

5) Instalacja i konfiguracja oprogramowania i sprzętu sieciowego i serwerów, używanych do przetwarzania danych osobowych,
6) Konfiguracja i administracja oprogramowaniem systemowym i sieciowym zabezpieczającym dane osobowe przed nieuprawnionym dostępem,
7) Nadzór nad czynnościami związanymi ze sprawdzaniem systemu pod kątem obecności szkodliwego oprogramowania,
8) Nadzór nad systemem komunikacji w sieci komputerowej oraz przesyłaniem danych za pośrednictwem urządzeń teletransmisji,
9) Nadzór nad naprawami, konserwacją oraz likwidacją urządzeń, na których zapisane są dane osobowe,
10) Przyznawanie ściśle określonych praw dostępu do danych osobowych w danym systemie,
11) Świadczenie pomocy technicznej w ramach oprogramowania, a także serwis sprzętu komputerowego będącego na stanie Urzędu, służącego do przetwarzania danych osobowych,
12) Diagnozowanie i usuwanie awarii sprzętu komputerowego oraz realizacja umów z firmami świadczącymi usługi gwarancyjnego i pogwarancyjnego serwisu sprzętu komputerowego,
13) Wykonywanie i zarządzanie kopiami awaryjnymi oprogramowania systemowego i sieciowego,
14) Nadzór nad wdrożeniem oraz zarządzanie aplikacjami (przeglądanie, nadawanie uprawnień, cofanie uprawnień użytkownikom itp.), w których przetwarza się dane osobowe.

§ 10
Odpowiedzialność Właścicieli zasobów danych osobowych

1. Administrator Danych Osobowych wyznacza Właścicieli zasobów danych osobowych, którzy są odpowiedzialni za ochronę przypisanych i przetwarzanych zbiorów danych osobowych w podległej komórce organizacyjnej.
2. Do kompetencji właścicieli zasobów należy:
   1) Określanie celów w jakich mają być przetwarzane dane osobowe, zakresu oraz czasu trwania przetwarzania danych osobowych,
   2) Określenie sposobu przetwarzania danych osobowych (system informatyczny czy nieinformatyczny).
3. Do obowiązków Właścicieli zasobów danych osobowych należy:
   1) Zapewnienie podstaw prawnych do przetwarzania danych osobowych od chwili zebrania danych osobowych do chwili ich usunięcia,
   2) Zapewnienie aktualności, adekwatności oraz merytorycznej poprawności danych osobowych przetwarzanych w określonym przez nich celu,
   3) Realizację obowiązku informowania o przetwarzania danych osobowych osób, których dane osobowe są pozyskiwane,
   4) W przypadku utworzenia nowego zbioru danych osobowych ustalenie, kogo dotyczą dane osobowe, jaki jest ich zakres, cel przetwarzania oraz komu dane osobowe mają być udostępniane. Wszystkie te informacje winny zostać niezwłocznie przekazane do Administratora Bezpieczeństwa Informacji.

§ 11
Odpowiedzialność pracowników i użytkowników systemu

1. W celu osiągnięcia i utrzymania wysokiego poziomu bezpieczeństwa przetwarzania danych osobowych konieczne jest zaangażowanie ze strony każdego pracownika i użytkownika zewnętrznego w zakresie ochrony danych osobowych.
2. Pracownicy Urzędu oraz użytkownicy zewnętrzni są zobowiązani do informowania o wszelkich podejrzeniach lub zauważonych naruszeniach oraz słabościach systemu przetwarzającego dane osobowe bezpośrednio do Administratora Bezpieczeństwa Informacji.

3. Pracownicy/użytkownicy zewnętrzni są zobowiązani do:
   1) Postępowania zgodnie z Polityką,
   2) Zachowania tajemnicy danych osobowych oraz informacji o sposobach ich zabezpieczenia,
   3) Ochrony danych osobowych oraz środków przetwarzających dane osobowe przed nieuprawnionym dostępem, ujawnieniem, modyfikacją lub zniszczeniem.
   4) Wykonywania konkretnych działań i procesów w celu zapewnienia ochrony danych osobowych.
4. Pracownicy/użytkownicy zewnętrzni powinni mieć świadomość możliwości zaistnienia sytuacji naruszenia ochrony danych osobowych. W tym celu powinni:
   1) Informować ABI o podejrzanych osobach,
   2) Pracownicy/użytkownicy zewnętrzni powinni na podstawie dokonanej identyfikacji ewentualnych zagrożeń, przedkładać ABI projekty i propozycje nowych rozwiązań, których celem jest zwiększenie poziomu ochrony danych osobowych

§ 12
Sankcje za naruszenie zasad ochrony danych osobowych

1. Naruszenie zasad ochrony danych osobowych przez pracownika/użytkownika zewnętrznego może skutkować postawieniem mu zarzutu popełnienia jednego z przestępstw określonych w rozdziale 8 Ustawy.
2. Zgodnie z art. 100 § 2 pkt 5 Kodeksu pracy, pracownik jest obowiązany przestrzegać tajemnicy określonej w odrębnych przepisach. Dane osobowe, którym Urząd nadaje charakter poufny mają charakter takiej tajemnicy, a jej ujawnienie w zależności od zakresu ujawnionych danych osobowych oraz nastawienia pracownika dopuszczającego się nieuprawnionego ujawnienia danych, może mieć charakter naruszenia lub ciężkiego naruszenia obowiązków pracowniczych.

§ 13
Wymiana informacji dotyczących danych osobowych

1. Pracownicy Urzędu oraz użytkownicy zewnętrzni w celu ochrony wymienianych informacji dotyczących danych osobowych powinni podczas przetwarzania uwzględniać następujące zasady:
   1) Wykorzystywanie technik kryptograficznych do ochrony poufności, integralności i rozliczalności danych osobowych przesyłanych publicznymi sieciami telekomunikacyjnymi,
   2) Ochrona wymienianych danych osobowych przed przechwyceniem, kopiowaniem, modyfikacją, błędnym wyborem drogi komunikacji lub zniszczeniem,
   3) Zabezpieczenia i ograniczenia związane z możliwościami przekazywania wiadomości za pomocą środków komunikacji,
   4) Zakaz pozostawiania informacji zawierających dane osobowe przy urządzeniach drukujących (kopiarkach, drukarkach, faksach), do których mogą mieć dostęp osoby nieupoważnione,
   5) Upewnienie się przed przekazaniem danych osobowych, czy rozmówca jest osobą upoważnioną do uzyskania określonych danych,
   6) Zachowania szczególnej ostrożności w trakcie rozmów telefonicznych, unikając podsłuchania danych osobowych przez osoby nieupoważnione,
   7) Właściwe postępowanie z faksami i fotokopiarkami, ponieważ mają one podręczną pamięć i przechowują dane w przypadku błędów transmisji,
2. Transport danych osobowych w formie elektronicznej i papierowej pomiędzy obszarami, w których są przetwarzane dane osobowe powinien być prowadzony przez osoby upoważnione, w sposób ograniczający możliwość ich pozyskania przez osoby nieuprawnione.

§ 14
Przetwarzanie danych osobowych w obszarze bezpiecznym

1. Dane osobowe w Urzędzie Miejskim mogą być przetwarzane wyłącznie we wskazanych pomieszczeniach.

2. Na pomieszczenia przetwarzania danych osobowych składają się pomieszczenia biurowe oraz część pomieszczeń, gdzie Urząd prowadzi działalność.
3. Do pomieszczeń przetwarzania danych osobowych zalicza się:
   1) Serwerownia,
   2) Pomieszczenia biurowe, w których zlokalizowane są stacje robocze,
   3) Pomieszczenia, w których przechowywane są sprawne oraz uszkodzone elektroniczne nośniki informacji, kopie zapasowe,
   4) Pomieszczenia, w których przechowuje się dokumenty źródłowe oraz wydruki z systemu informatycznego,
   5) Pomieszczenia, w których zlokalizowane są zbiory nieinformatyczne.
4. Przebywanie wewnątrz obszarów o których mowa w ust. 3 osób nieuprawnionych do przetwarzania danych osobowych jest dopuszczalne tylko w obecności osoby upoważnionej lub za zgodą Właściciela zasobów danych osobowych.
5. Budynek lub pomieszczenia, w których przetwarzane są dane osobowe powinny być zamykane podczas nieobecności osób upoważnionych do przetwarzania danych osobowych, w sposób ograniczający możliwość dostępu do nich osobom nieupoważnionym.
6. W celu ograniczenia dostępu osób nieupoważnionych do pomieszczeń, w których zlokalizowano przetwarzanie danych osobowych należy zapewnić:
   1) Jasne określenie granic obszaru przetwarzania danych osobowych oraz umiejscowienie dostosowane do wymagań bezpieczeństwa w odniesieniu do aktywów znajdujących się wewnątrz obszaru.
   2) Jednolite granice budynków lub pomieszczeń, gdzie zlokalizowano środki przetwarzania danych osobowych (tzn. aby granice nie miały luk lub punktów, przez które łatwo się włamać),
   3) Ściany zewnętrzne pomieszczeń solidnej konstrukcji oraz wszystkie drzwi zewnętrzne odpowiednio zabezpieczone przed nieautoryzowanym dostępem za pomocą mechanizmów zabezpieczeń.
   4) Zamykanie drzwi i okien w pomieszczeniach pozostawianych bez dozoru.
7. Obszary bezpieczne powinny być odpowiednio zabezpieczone przed skutkami pożaru.
8. Ochrona obszarów bezpiecznych powinna być zapewniona poprzez odpowiednie fizyczne zabezpieczenie wejścia, zapewniające, że jedynie osoby upoważnione mogą uzyskać dostęp, w tym celu należy zapewnić:
   1) Nadzorowanie pobytu osób nie będących pracownikami Urzędu w obszarach bezpiecznych, chyba że ich dostęp został wcześniej zaakceptowany,
   2) Kontrolowanie i ograniczanie dostępu do obszarów, gdzie są przetwarzane dane osobowe tylko dla uprawnionego personelu,
   3) Regularne przeglądanie praw dostępu do obszarów bezpiecznych i ich uaktualniane.
9. Przetwarzanie danych osobowych jest zakazane w pomieszczeniach, gdzie osoby trzecie wykonują prace techniczne.
10. Każdorazowe uchybienie zabezpieczeń fizycznych, chroniących dostęp da zbiorów danych osobowych musi być zgłaszane do Administratora Bezpieczeństwa Informacji.

§ 15
Dopuszczenie osób do przetwarzania danych osobowych

1. Przetwarzanie danych osobowych jest możliwe wyłącznie po uzyskaniu przez pracownika/użytkownika zewnętrznego formalnego upoważnienia do przetwarzania danych osobowych, zaakceptowanego przez Administratora Danych Osobowych,
2. Oświadczenia i upoważnienia o których mowa w ust. 1 przechowuje się w aktach osobowych pracownika,
3. Przełożony pracownika/użytkownika zewnętrznego jest zobowiązany niezwłocznie po ustaniu potrzeby przetwarzania danych osobowych przez pracownika/użytkownika zewnętrznego złożyć rezygnację do ABI dotyczącą jego dostępu do danych osobowych. Rezygnacja nie jest wymagana w przypadku udzielenia upoważnienia do przetwarzania danych na czas określony – w przypadku upływu okresu upoważnienia.

§ 16
Ewidencja osób upoważnionych do przetwarzania danych osobowych

1. Osoby upoważnione do przetwarzania danych osobowych powinny być wpisywane do ewidencji. Ewidencję osób upoważnionych do przetwarzania danych osobowych prowadzi ABI.
2. Właściciele zasobów danych osobowych, przełożeni pracowników/użytkowników zewnętrznych odpowiadają za niezwłoczne zgłoszenie do Administratora Bezpieczeństwa Informacji osób, które utraciły uprawnienia do dostępu do danych osobowych.
3. W oparciu o informacje wskazane w ust. 2 ABI winien podjąć działania, których celem jest uniemożliwienie tym osobom dostępu do danych osobowych i wykreślić ich z ewidencji, o której mowa w ust. 1.

§ 17
Rejestracja zbiorów danych osobowych

1. Upoważnieni pracownicy są zobowiązani do wnioskowania ABI zamiaru utworzenia nowego zbioru danych osobowych, wraz z wskazaniem podstawy prawnej przetwarzania danych, uzasadnieniem celu oraz określeniem zakresu i sposobu zbierania danych osobowych.
2. ABI weryfikuje wniosek o utworzenie nowego zbioru danych osobowych oraz analizuje pod kątem obowiązku zgłoszenia zasobu, jako zbioru danych do rejestracji w GIODO.
3. W sytuacji, gdy rejestracja nowopowstałego zbioru lub zbioru wymagającego aktualizacji danych osobowych jest ustawowo wymagana, Właściciel zasobu przygotowuje projekt zgłoszenia zbioru danych osobowych /zgłoszenia zmian do rejestracji/zmiany w GIODO (w części A-D wniosku).
4. ABI sprawdza opisane w zgłoszeniu rejestracyjnym warunki techniczne i organizacyjne dotyczące zabezpieczeń w systemie informatycznym, a w przypadku niewystarczającego poziomu zabezpieczeń występuje z wnioskiem do Administratora Danych Osobowych o podniesienie poziomu tych zabezpieczeń.
5. Sprawdzony przez ABI projekt zgłoszenia zbioru danych osobowych do rejestracji w GIODO jest przedstawiany Administratorowi Danych Osobowych do akceptacji.
6. Wniosek o rejestrację zbioru/aktualizację do GIODO przesyła ABI.

§ 18
Udostępnianie danych osobowych

1. Dane osobowe mogą być udostępniane podmiotom uprawnionym do ich otrzymywania na mocy przepisów prawa.
2. Udostępnianie danych osobowych osobie nieupoważnionej do przetwarzania danych osobowych może nastąpić wyłącznie za zgodą Właściciela zasobów danych osobowych. Zgoda może dotyczyć również udostępniania danych osobowych w przyszłości. Zarówno wniosek, jak i zgoda winny posiadać formę pisemną.
3. Udostępniając dane osobowe należy zaznaczyć, że można je wykorzystać wyłącznie zgodnie z przeznaczeniem, dla którego zostały udostępnione.
4. Na pisemny wniosek pochodzący od osoby, której dane dotyczą, informacje o osobie powinny być udzielone w terminie 30 dni od daty złożenia wniosku.
5. Za przygotowanie danych osobowych do udostępnienia w zakresie wskazanym we wniosku odpowiedzialny jest Właściciel zasobów danych osobowych.
6. Informacje zawierające dane osobowe są przekazywane uprawnionym podmiotom lub osobom za potwierdzeniem odbioru, np. w następujący sposób:
    1) Listem poleconym za pokwitowaniem odbioru,
    2) Teletransmisji danych zgodnie z zasadami wymiany informacji opisanymi w niniejszym dokumencie,
    3) Innym bezpiecznym, określonym wymogiem prawnym lub umową.

§ 19

Powierzanie przetwarzania danych osobowych

1. Powierzenie przetwarzania danych osobowych występuje wówczas, gdy podmioty zewnętrzne współpracujące z Urzędem mają dostęp do danych osobowych przetwarzanych przez Urząd.
2. Wskazane w ust. 1 powierzenie przetwarzania danych osobowych może odbywać się wyłącznie w trybie przewidzianym w art. 31 Ustawy poprzez zawarcie umowy na piśmie powierzenia przetwarzania danych osobowych, pomiędzy Urzędem, a danym podmiotem, któremu zleca się czynności związane z przetwarzaniem danych osobowych lub uwzględnienie kwestii powierzenia w umowach.
3. W sytuacji powierzenia przetwarzania danych osobowych podmiotowi zewnętrznemu, w umowie powierzenia przetwarzania danych osobowych określa się przede wszystkim:
   1) Cel i zakres przetwarzanych danych,
   2) Obowiązek zachowania tajemnicy danych osobowych oraz informacji o zabezpieczeniach tych danych,
   3) Konsekwencje prawne i kary finansowe wynikające z niestosowania się do warunków umowy (z punktu widzenia ochrony danych osobowych),
   4) Wymagania bezpieczeństwa dla procesu przetwarzania danych osobowych.
4. Zalecane jest, aby w umowach powierzenia przetwarzania danych osobowych oraz w umowach, na podstawie których dochodzi do wymiany informacji uwzględnić następujące elementy:
   1) Definicję informacji, która ma być chroniona,
   2) Spodziewany czas trwania umowy, włączając w to przypadki, w których obowiązek zachowania poufności może być bezterminowe.
   3) Wymagane działania w momencie zakończenia umowy,
   4) Odpowiedzialność i działania sygnatariuszy podejmowane w celu uniknięcia nieupoważnionego ujawnienia informacji,
   5) Własność informacji,
   6) Zasady zwrotu lub niszczenia danych osobowych przy zakończeniu umowy,
   7) Działania podejmowane w przypadku naruszenia warunków umowy.

§ 20
Postępowanie w przypadku naruszenia lub podejrzenia

1. Poniższe postanowienia mają zastosowanie zarówno w przypadku naruszenia, jak i podejrzenia naruszenia ochrony danych osobowych przetwarzanych w systemach informatycznych i zbiorach nieinformatycznych.
2. Przed przystąpieniem do pracy pracownicy/użytkownicy zewnętrzni zobowiązani są dokonać sprawdzenia stanu urządzeń informatycznych oraz oględzin swojego stanowiska pracy, ze zwróceniem szczególnej uwagi czy nie zaszły okoliczności wskazujące na naruszenie lub próbę naruszenia ochrony danych osobowych.
3. Za okoliczności uznawane za naruszenie lub podejrzenie naruszenia ochrony systemu przetwarzającego dane osobowe uważa się w szczególności:
   1) Nieuprawniony dostęp lub próbę dostępu do danych osobowych lub pomieszczeń w których się one znajdują,
   2) Nieuprawnione naruszenie lub próby naruszenia poufności, integralności i rozliczalności danych systemu,
   3) Niezamierzoną zmianę lub utratę danych zapisanych na kopiach zapasowych,
   4) Nieuprawniony dostęp do danych osobowych,
   5) Udostępnienie osobom nieupoważnionym danych osobowych lub ich części,
   6) Inny stan systemu informatycznego lub pomieszczeń, niż pozostawiony przez użytkownika po zakończeniu pracy,
   7) Zdarzenia losowe, obniżające poziom ochrony systemu (np. brak zasilania, pożar, huragan itp.),
   8) Kradzież sprzętu informatycznego lub nośników zewnętrznych zawierających dane osobowe (np. wydruków komputerowych, płyt CD/DVD, dysków twardych, pamięci zewnętrznych itp.)

4. W przypadku stwierdzenia naruszenia lub zaistnienia okoliczności wskazujących na próbę naruszenia ochrony danych osobowych pracownicy zobowiązani są do bezzwłocznego powiadomienia o tym fakcie Administratora Bezpieczeństwa Informacji.
5. Do czasu przybycia ABI zgłaszający:
   1) Powstrzymuje się od rozpoczęcia lub kontynuowania pracy, jak również od podejmowania jakichkolwiek czynności, mogących spowodować zatarcie śladów naruszenia bądź innych dowodów,
   2) Zabezpiecza elementy systemu informatycznego lub dane na nośniku nieinformatycznym, poprzez uniemożliwienie dostępu do nich osobom nieuprawnionym,
   3) Podejmuje stosownie do zaistniałej sytuacji wszelkie niezbędne działania celem zapobieżenia dalszym zagrożeniom, które mogą skutkować utratą danych osobowych,
   4) Wykonuje polecenia ABI.
6. W przypadku stwierdzenia naruszenia lub zaistnienia okoliczności wskazujących na naruszenie ochrony danych osobowych ABI, po przybyciu na miejsce:
   1) Ocenia zastałą sytuację, biorąc pod uwagę w szczególności stan pomieszczeń, w których przetwarzane są dane osobowe oraz stan urządzeń, a także szacuje wielkość negatywnych następstw incydentu,
   2) Wysłuchuje relacji osoby, która dokonała powiadomienia oraz innych osób związanych z incydentem,
   3) Podejmuje decyzję o toku dalszego postępowania, stosownie do zakresu naruszenia lub zasadności podejrzenia naruszenia ochrony danych osobowych.

7. ABI sporządza raport z przebiegu zdarzenia, w którym powinny się znaleźć w szczególności informacje o:
   1) Dacie i godzinie powiadomienia,
   2) Godzinie pojawienia się w pomieszczeniach, w których przetwarzane są dane,
   3) Sytuacji, jaką zastał,
   4) Podjętych działaniach i ich uzasadnieniu.
8. W przypadku naruszenia lub zaistnienia okoliczności wskazujących na próbę naruszenia ochrony danych osobowych, użytkownik może kontynuować pracę dopiero po otrzymaniu pozwolenia od ABI.
9. W przypadku gdy naruszenie ochrony danych osobowych jest wynikiem uchybienia obowiązującej w Urzędzie dyscypliny pracy, ABI wyjaśnia wszystkie okoliczności incydentu i podejmuje stosowne działania wobec osób, które dopuściły się wskazanego naruszenia.
10. Po zakończeniu czynności naprawczych system powinien otrzymać poziom ochrony nie niższy niż przed wystąpieniem incydentu związanego z naruszeniem ochrony danych osobowych.

§ 21
Zasady ochrony danych osobowych w zbiorach nieinformatycznych

1. Zbiory nieinformatyczne powinny być odpowiednio zabezpieczone przed nieuprawnionym dostępem i zniszczeniem,
2. Dokumenty i wydruki zawierające dane osobowe należy przechowywać w zamykanych pomieszczeniach, do których dostęp mają jedynie upoważnione osoby.
3. Na czas nieużytkowania dokumenty i wydruki zawierające dane osobowe powinny być zamykane w szafach biurowych lub szufladach.
4. Wydruki robocze, błędne lub zdezaktualizowane powinny być niezwłocznie niszczone przy użyciu niszczarki do papieru lub w inny sposób, zapewniający skuteczne ich usunięcie lub zanonimizowanie.

§ 22
Sposób podziału identyfikatorów i haseł dla użytkowników

1. Mając na względzie, iż system informatyczny przetwarzający dane osobowe powinien być wyposażony w mechanizmy uwierzytelniania użytkownika oraz kontroli dostępu do tych danych –

dla każdej osoby ustalany jest odrębny identyfikator i hasło. Bezpośredni dostęp do danych osobowych przetwarzanych w systemie informatycznym może mieć miejsce wyłącznie po podaniu identyfikatora i właściwego hasła. Hasła dostępu i identyfikatory przyznawane są indywidualnie dla każdego z użytkowników i znane są tylko właścicielowi. Przyznane hasło dla użytkownika zostaje przez niego zmienione przy pierwszym logowaniu.

Przyznane hasła i identyfikatory muszą być chronione przez użytkownika.

2. Użytkownik jest odpowiedzialny za wszystkie czynności wykonywane przy użyciu hasła.
3. W przypadku powzięcia przez użytkownika podejrzenia lub stwierdzenia, że z hasłem mogły zapoznać się osoby trzecie, obowiązany jest on niezwłocznie zmienić swoje hasło i powiadomić o tym fakcie ABI.
4. Identyfikator użytkownika jest blokowany lub całkowicie usuwany z systemu w każdym przypadku utraty przez niego uprawnień do dostępu do danych osobowych (zmiana zakresu obowiązków, ustanie zatrudnienia itp.).
5. Zablokowanie lub usunięcie identyfikatora użytkownika, który utracił uprawnienia dostępu do systemu informatycznego powoduje, że osoba ta nie ma możliwości zalogowania się do sieci lub aplikacji.

§23
Kopie bezpieczeństwa i bezpieczeństwo przed szkodliwym oprogramowaniem

1. Tworzenie, przechowywanie kontrolowanie i likwidację kopii bezpieczeństwa realizuje informatyk. Kopie zapasowe są:
   1) Tworzone na odpowiednio opisanych nośnikach danych,
   2) Sprawdzane wybiórczo pod kątem ich dalszej przydatności do odtworzenia danych w przypadku awarii systemu informatycznego,
   3) Przechowywane w odpowiednio zabezpieczonym miejscu, do którego dostęp mają wyłącznie osoby upoważnione przez Administratora Danych Osobowych,
   4) Bezzwłocznie usuwane po ustaniu ich użyteczności w sposób trwały, uniemożliwiający ich odczytanie.
2. Na bieżące i bezpośrednie sprawdzanie obecności szkodliwego oprogramowania pozwala oprogramowanie automatycznie monitorujące występowanie w/w oprogramowania w trakcie załączania i wczytywania danych z zewnętrznych nośników, sieci lokalnej bądź Internetu.
3. Nadzór nad instalowaniem nowego oprogramowania antywirusowego oraz bieżącą jego aktualizacją sprawuje informatyk.

§ 24
Procedury rozpoczęcia i zakończenia pracy

1. Przed przystąpieniem do pracy w systemie użytkownik obowiązany jest dokonać sprawdzenia stanu urządzeń komputerowych, służących do przetwarzania danych osobowych oraz dokonać oględzin swojego stanowiska pracy, ze szczególnym uwzględnieniem czy nie zaszły okoliczności wskazujące na naruszenie ochrony danych osobowych.
2. W przypadku, gdy przerwa w pracy trwa dłuższy okres oraz kończąc pracę użytkownik obowiązany jest wylogować się z aplikacji i systemu komputerowego; sprawdzić czy nie zostały pozostawione bez zamknięcia nośniki informacji. Opuszczając stanowisko użytkownik zamyka przez niego szafy i pomieszczenia, w których przechowuje się dokumentację i nośniki informacji.
3. W przypadku zauważenia przez użytkownika naruszenia zabezpieczenia systemu informatycznego, zauważenia, że stan urządzenia, wartość zbioru danych osobowych, ujawnione metody pracy, sposób działania programu lub jakość komunikacji w sieci mogą wskazywać na naruszenie zabezpieczeń danych osobowych, użytkownik ten zobowiązany jest niezwłocznie poinformować o tym fakcie ABI.

§ 25
Eksploatacja i konserwacja systemów i sprzętu

1. Przeglądy i konserwacje sprzętu komputerowego dokonuje się w miarę potrzeb wynikających z jego obciążenia, warunków zewnętrznych, w których eksploatowany jest sprzęt.
2. Prace dotyczące przeglądów, konserwacji i napraw, wymagające autoryzowanych firm zewnętrznych są wykonywane przez uprawnionych przedstawicieli tych firm pod nadzorem ABI lub upoważnionej przez niego osoby, bez możliwości dostępu do danych osobowych.
3. Urządzenia, dyski lub inne informatyczne nośniki informacji, przeznaczone do napraw, gdzie wymagane jest zaangażowanie autoryzowanych podmiotów zewnętrznych pozbawia się przed naprawą zapisu tych danych albo naprawia się je pod nadzorem osoby upoważnionej przez ABI.
4. Urządzenia, na których przetwarzane są dane osobowe winny być wyposażone w sprawne zasilanie awaryjne (UPS).
5. Sprzęt przenośny, taki jak laptopy (tablety) musi być zabezpieczony podczas transportu przed uszkodzeniem fizycznym i kradzieżą oraz zabezpieczone przed dostępem osób nieuprawnionych (np. hasłem).

§ 26
Użytkowanie sprzętu komputerowego oraz oprogramowania

1. Sprzęt informatyczny powinien być użytkowany wyłącznie w celach służbowych. Na stanowiskach pracy może być wykorzystywane wyłącznie oprogramowanie legalne.
2. Instalacje oprogramowania na stanowiskach pracy w Urzędzie Miejskim w Radymnie dokonywane są z nośników znajdujących się w zasobach w/w jednostki przez upoważnione osoby.
3. Zabrania się instalowania oprogramowania, którego jednostka nie ma prawa używać (np. z powodu braku licencji).
4. Zabrania się dokonywania nieuprawnionych zmian w systemach informatycznych lub informacjach w nich przetwarzanych.
5. Zabrania się wykorzystywania komputera, a w szczególności sieci Internet i poczty elektronicznej do celów innych niż służbowe.
6. Zabrania się wyłączania lub wstrzymywania funkcjonowania oprogramowania antywirusowego i monitorującego komputer.
7. Zabrania się podłączania nośników danych nie stanowiących własności Urzędu.
8. Zabrania się ingerowania w sprzęt komputerowy osobom nieupoważnionym.
9. Zabrania się podejmowania nieuprawnionych działań, mogących obniżyć poziom bezpieczeństwa infrastruktury teleinformatycznej, wynikających z niestosowania się do reguł zapisanych w niniejszej Polityce.
10. Przystępując do pracy, pracownik składa pisemne oświadczenie, że przyjmuje do wiadomości i stosowania przepisy Polityki bezpieczeństwa i instrukcji zarządzania systemem informatycznym w Urzędzie.

§ 27
Postanowienia końcowe

1. W sprawach nieuregulowanych w niniejszej Polityce mają zastosowanie przepisy ustawy z dnia 29 sierpnia 1997 r. o ochronie danych osobowych oraz przepisy wykonawcze do tej ustawy.
2. Załącznikami do niniejszej Polityki są:
   1) Wzór upoważnienia do przetwarzania danych,
   2) Wzór oświadczenia o zapoznaniu się z Polityką i jej stosowaniu,
   3) Wzór ewidencji zbiorów danych osobowych oraz programów zastosowanych do ich przetwarzania w Urzędzie Miejskim w Radymnie,
   4) Wzór ewidencji osób upoważnionych przez Administratora Danych Osobowych do przetwarzania danych osobowych,
   5) Wzór raportu z naruszenia bezpieczeństwa systemu w Urzędzie Miejskim w Radymnie.

Załącznik nr 1
do Polityki bezpieczeństwa
i instrukcji zarządzania
systemem informatycznym

Radymno, dnia .....

UPOWAŻNIENIE NR ...../.....

Na podstawie art. 37 ustawy z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (Dz.U. z 2014 r. poz. 1182)

upoważniam Pana/Panią .....
zatrudnionego/zatrudnioną na stanowisku .....
.....
do przetwarzania, w ramach wykonywanych obowiązków służbowych następujących zbiorów danych osobowych:
.....
.....
.....

oraz do obsługi systemu informatycznego i urządzeń wchodzących w jego skład, służących do przetwarzania danych osobowych na zajmowanym stanowisku w Urzędzie Miasta Radymna .

Upoważnienie wydaje się na czas:

.....
(od dnia ... do dnia.../ zatrudnienia w Urzędzie Miejskim)

Jednocześnie zobowiązuję Pana/Panią do przestrzegania przepisów dotyczących ochrony danych osobowych zawartych w powołanej wyżej ustawie z dnia 29 sierpnia 1997 r. o ochronie danych osobowych.

.....
(podpis Administratora danych osobowych)

Przyjmuję do wiadomości i przestrzegania, zobowiązuję się do zachowania tajemnicy danych osobowych przetwarzanych w Urzędzie Miasta Radymna oraz sposobów ich zabezpieczeń.

.....
(data i podpis pracownika)

Załącznik nr 2
do Polityki bezpieczeństwa
i instrukcji zarządzania
systemem informatycznym

.....
(nazwisko i imię)

.....
(stanowisko służbowe)

OŚWIADCZENIE

Oświadczam, że przyjąłem/przyjęłam do wiadomości i stosowania przepisy Polityki bezpieczeństwa i instrukcji zarządzania systemem informatycznym w Urzędzie Miasta Radymna, a w szczególności, iż w Urzędzie obowiązuje całkowity zakaz:

1. Samodzielnego podłączania jakichkolwiek urządzeń oraz nośników zewnętrznych do komputerów służbowych,
2. Dokonywania nieuprawnionych zmian w systemach informatycznych lub informacji w nich przetwarzanych,
3. Dokonywania nieuprawnionych prób testowania zauważonych podatności (luk w zabezpieczeniu systemu)
4. Wykorzystywania komputera, Internetu i poczty elektronicznej do celów innych niż służbowe,
5. Wprowadzania nieuprawnionych zmian w zatwierdzonej konfiguracji bazowej, stosowania nielegalnego oprogramowania, nieupoważnionego logowania się poza nominalnymi godzinami pracy, prób dostępu do plików i folderów, do których użytkownik nie ma dostępu,
6. Nieuprawnionego pozyskiwania informacji o zasobach informatycznych i środkach ich ochrony,

Sprzęt informatyczny winien być użytkowany wyłącznie w celach służbowych.
Instalacje oprogramowania na stanowiskach pracy w Urzędzie Miejskim dokonywane są z nośników znajdujących się w zasobach Urzędu przez upoważnione osoby.

Nieprzestrzeganie przepisów i ustaleń w przedmiotowym zakresie stanowić będzie poważne naruszenie obowiązków służbowych oraz dyscypliny pracy. Podejmowanie nieuprawnionych działań mogących obniżyć poziom bezpieczeństwa infrastruktury teleinformatycznej Urzędu, wynikających z niestosowania się do reguł, o których mowa w Polityce bezpieczeństwa, będzie uznane za szkodę na rzecz Urzędu Miasta Radymna i może być podstawą do pociągnięcia do odpowiedzialności karnej lub służbowej.

Zapoznałem(am) się z w/w poleceniami, co potwierdzam własnoręcznym podpisem.

.....	.....	.....
(miejscowość)	(data)	(podpis składającego oświadczenie)

Załącznik nr 3
do Polityki bezpieczeństwa
i instrukcji zarządzania
systemem informatycznym

Ewidencja zbiorów danych osobowych oraz programów zastosowanych do ich przetwarzania w Urzędzie Miasta Radymna

Lp.	Nazwa zbioru	Nazwa zastosowanego programu	Forma przekazania	Data rejestracji/ zmiany w GIODO	Nr księgi GIODO
1	2	3	4	5	6

Załącznik nr 4
do Polityki bezpieczeństwa
i instrukcji zarządzania
systemem informatycznym

Ewidencja osób upoważnionych przez Administratora Danych Osobowych do przetwarzania danych osobowych w Urzędzie Miasta Radymna

Lp.	Numer	Imię i nazwisko	Data		zakres[1]	identyfikator[2]
			nadania	ustania		
1	2	3	4	5	6	7

[1] Zakres: p – przetwarzanie danych osobowych, k – przetwarzanie danych osobowych oraz obsługa systemu informatycznego oraz urządzeń wchodzących w jego skład, służących do przetwarzania danych w Urzędzie

[2] Identyfikator sieciowy, jeśli został nadany

Załącznik nr 5
do Polityki bezpieczeństwa
i instrukcji zarządzania
systemem informatycznym

Raport z naruszenia bezpieczeństwa systemu w Urzędzie Miasta Radymna

1. Data, godzina i miejsce zdarzenia:

   .....

   .....

   .....

2. Osoba powiadamiająca o zaistniałym zdarzeniu:

   .....

   .....

3. Rodzaj naruszenia bezpieczeństwa oraz okoliczności towarzyszące:

   .....

   .....

   .....

   .....

   .....

4. Podjęte działania:

   .....

   .....

   .....

   .....

5. Przyczyny wystąpienia zdarzenia:

   .....

   .....

   .....

   .....

.....
(podpis Administratora Bezpieczeństwa Informacji)