Zarządzenie Nr 3/W/2015

Burmistrza Krobi

z dnia 10 lutego 2015r.

w sprawie : wdrożenia dokumentacji przetwarzania i ochrony danych osobowych w Urzędzie Miejskim w Krobi

Na podstawie art.31 oraz art.33 ust.3 ustawy z dnia 8 marca 1990 r. o samorządzie gminnym (Dz.U z 2013 r.,poz.594 z późn.zm.) , w związku z art.36 ustawy z dnia 29 sierpnia 1997r. o ochronie danych osobowych (Dz. U. z 2014 r., poz.1182 z późn.zm.) oraz § 3 rozporządzenia Ministra Spraw Wewnętrznych i 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 , poz.1024)- zarządzam , co następuje:

§ 1

1.Wprowadzam do stosowania „Politykę bezpieczeństwa przetwarzania danych osobowych w Urzędzie Miejskim w Krobi stanowiącą załącznik nr 1 do zarządzenia.

2.Wprowadzam do stosowania „Instrukcję zarządzania systemem informatycznym służącym do przetwarzania danych osobowych" stanowiącą załącznik nr 2 do zarządzenia .

§ 2

1.Wykonanie zarządzenia powierzam Administratorowi Bezpieczeństwa Informacji,

2. Zobowiązuję pracowników Urzędu Miejskiego w Krobi do zapoznania się z dokumentami przywołanymi w § 1 zarządzenia.

3.Nadzór nad wykonaniem zarządzenia powierzam Sekretarzowi Gminy.

§ 3

1.Traci moc zarządzenie nr 74/2007 Burmistrza Krobi z dnia 27 czerwca 2007r. w sprawie wprowadzenia „Polityki bezpieczeństwa przetwarzania danych osobowych w Urzędzie

Miejskim w Krobi „ oraz Instrukcji Zarządzania Systemem Informatycznym służącym do przetwarzania danych osobowych w Urzędzie Miejskim w Krobi.

2.Zarządzenie wchodzi w życie z dniem podpisania

Otrzymują :

1)Naczelnicy UM w Krobi

2) WO –a/a

BURMISTRZ
Sebastian Czwojda

Załącznik Nr 1 do Zarządzenia nr 3/W/2015z dnia 10 lutego 2015.

POLITYKA BEZPIECZEŃSTWA PRZETWARZANIA

DANYCH OSOBOWYCH

w Urzędzie Miejskim w Krobi

Dokumenty powiązane :

Instrukcja zarzadzania systemem informatycznym służącym do przetwarzania danych osobowych

w Urzędzie Miejskim w Krobi.

§ 1

POSTANOWIENIA OGÓLNE

1. Polityka bezpieczeństwa przetwarzania danych osobowych w Urzędzie Miejskim w Krobi zwana dalej „POLITYKĄ „, została opracowana w związku z § 3 ust.1 rozporządzenia Ministra Spraw Wewnętrznych i 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. z 2004 roku ,Nr 100,poz.1024).

2. Celem Polityki jest wskazanie podstaw dla właściwego wykonania obowiązków Administratora danych w zakresie bezpieczeństwa i prawidłowej ochrony przetwarzanych danych osobowych.
3. Polityka określa zasady przetwarzania danych osobowych oraz ich zabezpieczenia, jako zbiór reguł i zaleceń , regulujących sposób ich zarzadzania , ochrony i przetwarzania w Urzędzie Miejskim w Krobi .

4. Polityka zawiera zestaw informacji dotyczących szacowania procesów przetwarzania danych osobowych oraz obowiązujących zabezpieczeń technicznych i organizacyjnych, zapewniających właściwą ochronę przetwarzania danych osobowych.

5. **Opracowaną Politykę stosuje się do danych osobowych :**
   - **przetwarzanych w systemach informatycznych ,**
   - **przetwarzanych na nośnikach elektronicznych,**
   - **przetwarzanych w sposób tradycyjny.**

§ 2

DEFINICJE I POJĘCIA ZAWARTE W POLITYCE

Wszystkie pojęcia i definicje zawarte w polityce znajdują wspólne powiązania za warte w niniejszym dokumencie także są powiązane z innymi dokumentami , które obowiązują w Urzędzie Miejskim w Krobi ,w zakresie ochrony danych osobowych .

1. **ADMINISTRATOR DANYCH OSOBOWYCH /ADO/-** ten, który decyduje o środkach i celach przetwarzania danych osobowych , reprezentowany przez Burmistrza Krobi.

2. **ADMINISTRATOR BEZPIECZEŃSTWA INFORMACJI/ABI/** – osoba wyznaczona przez ADO , odpowiedzialna za nadzorowanie stosowania środków technicznych i organizacyjnych zapewniających ochronę przetwarzanych danych osobowych , w tym w szczególności za przeciwdziałanie dostępowi osób nieuprawnionych do systemu , w którym przetwarzane są dane osobowe oraz podejmowanie stosownych działań w przypadku wykrycia naruszeń w systemie ochrony danych osobowych.

3. **ADMINISTRATOR SYSTEMÓW INFORMATYCZNYCH** – osoba wyznaczona przez ADO , odpowiedzialna za funkcjonowanie infrastruktury informatycznej na którą składa się wyposażenie informatyczne oraz systemy i aplikacje informatyczne , za ich ich przeglądy , konserwację oraz za stosowanie technicznych i organizacyjnych środków bezpieczeństwa w systemach informatycznych.

4. **BEZPIECZEŃSTWO PRZETWARZANIA DANYCH OSOBOWYCH** – zachowanie integralności, poufności i rozliczalności danych osobowych ; ponadto należy brać pod uwagę inne cechy , w szczególności dostępność, niezawodność.

5. **DANE OSOBOWE** – jest to jakakolwiek informacja , która daje możliwość bezpośrednio lub poprzez inne cechy identyfikację osoby fizycznej ,

6. **GIODO** – Generalny Inspektor Ochrony Danych Osobowych.

7. **INTEGRALNOŚĆ DANYCH** – właściwość zapewniająca pewność ,iż nie dokonano zmiany lub zniszczenia danych w sposób nieautoryzowany,

8. **NARUSZENIE OCHRONY DANYCH OSOBOWYCH** – jest to zamierzone lub niezamierzone naruszenie obowiązujących środków technicznych i organizacyjnych zastosowanych w celu ochrony danych osobowych . W szczególności , gdy stan urządzenia , zawartość zbioru danych osobowych , ujawnione metody pracy, zasady funkcjonowania oprogramowania i komunikacji w sieci telekomunikacyjnej, które mogą wskazywać na naruszenie ochrony danych osobowych.

9. **POUFNOŚĆ** – jest to właściwość dająca pewność że do danych osobowych ma dostęp wyłącznie osoba upoważniona.

10. **ROZLICZALNOŚĆ –** jest to właściwość zapewniająca ,że działania podmiotu mogą być przypisane w sposób jednoznaczny tylko temu podmiotowi.

11. **PRZETWARZANIE DANYCH OSOBOWYCH** – są to jakiekolwiek działania wykonywane na danych osobowych , w szczególności takie jak: pozyskiwanie, gromadzenie, wgląd, przenoszenie, utrwalanie, udostępnianie, usuwanie , a również te , które wykonuje się w systemach informatycznych.

12. **USTAWA** – Ustawa o ochronie danych osobowych z dnia 29 sierpnia 1997 roku (Dz.U. z 2014 roku,poz.1182 z późn.zm.).

13. **ROZPORZĄDZENIE**- rozporządzenie Ministra Spraw Wewnętrznych i 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, poz.1024).

14. **URZĄD-** Urząd Miejski w Krobi, ul.Rynek 1, 63-840 Krobia .

15. **UŻYTKOWNIK SYSTEMU** – osoba posiadająca upoważnienie, identyfikator, hasło dostępu upoważniające do przetwarzania danych osobowych w systemie informatycznym,

16. **UŻYTKOWNIK ZEWNĘTRZNY** – osoba nie będąca pracownikiem Urzędu Miejskiego w Krobi, posiadająca uprawnienia do przetwarzania danych osobowych w związku z wykonywaniem obowiązków na stanowisku pracy.

17. **WŁAŚCICIEL ZASOBÓW DANYCH OSOBOWYCH** – osoba kierująca komórką organizacyjną, odpowiedzialna za ochronę danych osobowych przetwarzanych w podległej komórce . osoba ta jest zobowiązana zastosować wszelkie środki techniczne i organizacyjne zapewniające właściwą ochronę przetwarzanych danych osobowych , stosowną do zagrożeń oraz kategorii danych objętych ochroną, a w szczególności zabezpieczenie danych osobowych przed ich udostępnieniem osobie nieupoważnionej, zabraniem przez osobę nieuprawnioną, przetwarzaniem z naruszeniem ustawy o ochronie danych osobowych , przed nieautoryzowaną zmianą, utratą , uszkodzeniem lub zniszczeniem.

18. **SYSTEM INFORMATYCZNY** – jest to zespół współpracujących urządzeń , programów, procedur związanych z przetwarzaniem danych osobowych oraz narzędzi programowych zastosowanych w celu przetwarzania danych osobowych.

19. **ZBIÓR DANYCH OSOBOWYCH** – jest to każdy posiadający strukturę zestaw o charakterze osobowym, dostępnych według określonych kryteriów , niezależnie od tego , czy zestaw ten jest rozproszony czy podzielony funkcjonalnie.

20. **ZBIÓR NIEINFORMATYCZNY** – jest to każdy posiadający strukturę zestaw danych o charakterze osobowym, dostępnych według określonych kryteriów , niezależnie od tego czy zestaw jest rozproszony lub podzielony funkcjonalnie , prowadzony w formie nieelektronicznej, poza systemem informatycznym, w szczególności w formie kartoteki, skorowidza, księgi ,wykazu a także w każdej innej formie w postaci zbioru.

§ 3

OBOWIĄZKI ADMINISTRATORA DANYCH OSOBOWYCH

1. ADO zobowiązany jest do podjęcia wszelkich działań , których celem jest zapewnienie prawidłowej ochrony danych osobowych , w szczególności zapewnienie przetwarzania danych ze szczególną starannością realizując następujące zasady:

   1) Przetwarzanie zgodnie z przepisami prawa,
   2) Zbieranie danych dla określonych celów i nie poddawanie dalszemu przetwarzaniu niezgodnie z tymi celami,
   3) Dane będą merytorycznie poprawne i adekwatne w stosunku do celów , w jakich są przetwarzane,
   4) Przechowywane w postaci umożliwiającej identyfikację osób, których dotyczą , jednak nie dłużej niż jest to niezbędne do osiągnięcia celu przetwarzania,
   5) Zabezpieczenie środkami technicznymi i organizacyjnymi , które zapewnią rozliczalność, poufność i integralność.

2. W Urzędzie Miejskim w Krobi stosuje się średni poziom bezpieczeństwa w rozumieniu zapisów § 6 ust.4 rozporządzenia.

§ 4

AKTUALIZACJA DOKUMENTACJI ZWIĄZANEJ Z OCHRONĄ DANYCH OSOBOWYCH

1. Niniejsza Polityka oraz wszystkie dokumenty z nią powiązane powinny być aktualizowane wraz ze zmianami w przepisach prawa dotyczącymi ochrony danych osobowych oraz zmianami wynikającymi z organizacji i funkcjonowania Urzędu .

2. W przypadku potrzeby wynikającej ze zdarzeń związanych z naruszeniem ochrony danych osobowych należy dostosować dokumentację do właściwych procedur, które w sposób skuteczny będą chroniły dane osobowe.

3. W każdym przypadku zmiany zapisów niniejszej Polityki wymagają aktualizacji inne dokumenty powiązane z Polityką.

4. O wszelkich zmianach w dokumentacji powinien być informowany ADO a w przypadku konieczności również powinny być zatwierdzane przez ADO.

§ 5

ZARZĄDZANIE OCHRONĄ DANYCH OSOBOWYCH

1. Celem właściwej realizacji zamierzeń a także skutecznej ochrony danych osobowych należy stosować następujące obowiązki:

    1) Przeszkolić pracowników uprawnionych do przetwarzania do przetwarzania danych osobowych w zakresie zasad bezpieczeństwa ,
    2) Przypisać użytkownikom określonych cech pozwalających na ich identyfikację w systemach informatycznych , dających możliwość dostęp do przetwarzania danych osobowych odpowiednio do zakresu upoważnienia,
    3) Okresowo kontrolować użytkowników sposób postepowania przy przetwarzaniu danych osobowych,
    4) W przypadku stwierdzonych nieprawidłowości podejmować stosowne działania celem ich wyeliminowanie,
    5) Na bieżąco wdrażać nowe rozwiązania organizacyjne i techniczne , które wzmocnią bezpieczeństwo przetwarzania danych osobowych.

2. W procesie nadzoru należy szczególnie uwzględniać zabezpieczenie w zakresie integralności, poufności oraz rozliczalności przetwarzania danych osobowych.

3. W procesie zarządzania należy stosować działania , które spowodują, że pracownicy , użytkownicy zewnętrzni będą :
    1) Odpowiednio przygotowani i wprowadzeni do przetwarzania danych osobowych ,
    2) Zapoznają się z obowiązującymi procedurami i zasadami przetwarzania danych osobowych w Urzędzie Miejskim w Krobi .
    3) Na bieżąco informowani o wszelkich zmianach w procedurach,

§ 6

DOKUMENTACJA POWIĄZANA Z POLITYKĄ

Na dokumentację powiązaną z procesem bezpieczeństwa przetwarzania danych osobowych w Urzędzie Miejskim w Krobi składają się:

Lp.	NAZWA DOKUMENTU	ODPOWIEDZIALNY
1.	Upoważnienie do przetwarzania danych osobowych Zał.Nr.3- WZÓR	Administrator Bezpieczeństwa Informacji
2.	Ewidencja osób upoważnionych do przetwarzania danych osobowych Zał.nr 1- WZÓR	Administrator Bezpieczeństwa Informacji
3.	Ewidencja zbiorów danych osobowych oraz programów stosowanych do ich przetwarzania Zał. Nr 2- WZÓR	Administrator Bezpieczeństwa Informacji
4.	Opis struktur zbiorów	Administrator Systemów Informatycznych
5.	- Wnioski związane ze zgłoszeniem zbioru do GIODO i ich aktualizacje, - obowiązujące przepisy prawa w zakresie ochrony danych osobowych, - zarządzenia ADO, - wzór legitymacji inspektora GIODO,	Administrator Bezpieczeństwa Informacji
6.	Protokoły : - bieżącej i okresowej kontroli prowadzonej przez ABI, - kontroli zewnętrznych kontroli,	Administrator Bezpieczeństwa Informacji
7.	Ewidencja przenośnych nośników informacji używanych przez pracowników	Administrator Systemów Informatycznych

§ 7

ODPOWIEDZIALNOŚĆ ADMINISTRATORA DANYCH OSOBOWYCH

1. Administrator Danych Osobowych jest odpowiedzialny za prawidłowe przetwarzanie danych osobowych i ich ochronę zgodnie z obowiązującymi przepisami prawa. Ponadto jest obowiązany do stosowania odpowiednich procedur zapewniających prawidłowe przetwarzanie danych osobowych , a także za zapewnienie ochrony przed zmianą ,uszkodzeniem zniszczeniem danych osobowych przez nieuprawnioną osobę.

2. Do kompetencji Administratora Danych Osobowych należy :
    1) Wyznaczenie Administratora Bezpieczeństwa Informacji – chyba ,że sam pełni tę funkcję,
    2) Wyznaczenie Właścicieli zasobów danych osobowych,
    3) Określenie celów o strategii działań w zakresie ochrony danych osobowych,
    4) Podział zadań i obowiązków związanych z organizacją ochrony danych osobowych .
3. Do obowiązków Administratora Danych Osobowych należy:
    1. Zapewnienie szkoleń dla pracowników w zakresie przepisów o ochronie danych osobowych oraz zagrożeń związanych z ich przetwarzaniem,
    2. Zatwierdzanie opracowanej dokumentacji związanej z ochrona danych osobowych w jednostce,

3. Nadawanie upoważnień pracownikom oraz użytkownikom zewnętrznym do przetwarzania danych osobowych,
4. Zapewnienie ochrony fizycznej pomieszczeń , w których są przetwarzane dane osobowe,
5. Zapewnienie ochrony danych osobowych przetwarzanych w systemach informatycznych oraz nieinformatycznych,
6. Zapewnienie środków na szkolenia osób funkcyjnych związanych z ochroną danych osobowych,
7. Zapewnienie rejestracji zbiorów danych osobowych do GIODO oraz ich aktualizacji .

§ 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 danych osobowych prowadzonych w formie papierowej i elektronicznej *(WZÓR zał. Nr 2),*
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 Administratora Bezpieczeństwa Informacji należy:
   1) Nadzór nad wdrożeniem stosownych środków organizacyjnych, technicznych i fizycznych w celu ochrony przetwarzanych danych osobowych.
   2) Nadawanie, zmienianie oraz cofanie uprawnień do przetwarzania danych osobowych na wniosek Właścicieli zasobów po akceptacji Administratora Danych Osobowych 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 (Polityka oraz wynikające z niej instrukcje i procedury) .
   5) Zapoznawanie pracowników z przepisami i zasadami ochrony danych osobowych oraz informowanie o zagrożeniach związanych z ich przetwarzaniem.
   6) Reprezentowanie ADO w kontaktach z GIODO.
   7) Przygotowywanie wniosków zgłoszeniowych zbiorów danych osobowych do rejestracji w Biurze GIODO.
   8) Reagowanie na zgłaszane incydenty związane z naruszeniem ochrony danych osobowych oraz analizowanie ich przyczyn i kierowanie wniosków dla ADO.

9) Kontrola oraz sprawdzanie wypełnienia obowiązków technicznych i organizacyjnych związanych z ochroną danych osobowych.

4. Administrator Bezpieczeństwa Informacji w zakresie realizacji swoich obowiązków, ma prawo żądania od pracowników bezzwłocznej pomocy w razie stwierdzenia naruszenia przepisów o ochronie danych osobowych, które mogłoby skutkować odpowiedzialnością karną zawartą w Rozdziale 8 Ustawy.

§ 9

ODPOWIEDZIALNOŚĆ ADMINISTRATORA SYSTEMÓW INFORMATYCZNYCH

1. Obowiązki ASI pełni pracownik wyznaczony przez Administratora Danych Osobowych.

2. Do zakresu obowiązków Administratora Systemów Informatycznych 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) Bieżący nadzór oraz zapewnianie optymalnej ciągłości działania systemu informatycznego w tym opracowanie procedur określających zarządzanie systemem informatycznym przetwarzającym dane osobowe.
4) W przypadku powstania zagrożenia ochrony danych osobowych bezzwłoczne podjęcie stosowanych działań .
5) Przeciwdziałanie próbom naruszenia bezpieczeństwa danych osobowych.
6) Analiza raportów wszelkich zdarzeń w tym incydentów związanych z bezpieczeństwem systemów przetwarzania danych.
7) Zapewnienie zgodności wszystkich wdrażanych systemów przetwarzania danych osobowych z Ustawą, Rozporządzeniem , Polityką bezpieczeństwa i Instrukcją Zarządzania Systemem Informatycznym .
8) Instalację i konfigurację oprogramowania i sprzętu używanego do przetwarzania danych osobowych.
9) Konfigurację i administrację oprogramowaniem systemowym i sieciowym zabezpieczającym dane osobowe przed nieupoważnionym dostępem.
10) Nadzór nad czynnościami związanymi ze sprawdzaniem systemu pod kątem obecności szkodliwego oprogramowania.
11) Nadzór nad systemem komunikacji w sieci komputerowej oraz przesyłaniem danych za pośrednictwem urządzeń teletransmisji.

12) Nadzór nad naprawami, konserwacją oraz likwidacją urządzeń komputerowych, na których zapisane są dane osobowe.
13) Przyznawanie na wniosek Właściciela zasobów, za zgodą Administratora Danych Osobowych i zatwierdzeniu przez Administratora Bezpieczeństwa Informacji ściśle określonych praw dostępu do danych osobowych w danym systemie.
14) Udzielanie pomocy w ramach realizacji serwisu dla potrzeb Urzędu .
15) Diagnozowanie i usuwanie awarii sprzętu komputerowego oraz realizacje umów z firmami świadczącymi usługi pogwarancyjnego sprzętu komputerowego.
16) Wykonywanie i zarządzanie kopiami awaryjnymi oprogramowania systemowego (w tym danych osobowych oraz zasobów umożliwiających ich przetwarzanie) i sieciowego.
17) Wykonywanie i przechowywanie dokumentacji należącej do kompetencji ASI.
18) Nadzór nad wdrożeniem i zarządzanie aplikacjami (przeglądanie, nadawanie i odbieranie uprawnień użytkownikom, itp.), w których przetwarza się dane osobowe.
19) Wspólnie z ABI współdziałanie w wypełnianiu wniosków zgłoszeń do rejestracji zbiorów danych osobowych w części E i F.
20) Współpraca w trakcie kontroli GIODO w zakresie dotyczącym systemu informatycznego.

§ 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 danych osobowych należy:

   1) Określanie celów w jakich mają być przetwarzane dane osobowe, zakresu oraz czasu trwania przetwarzania danych osobowych.
   2) Określenie sposobu przetwarzania danych osobowych (czy w systemach informatycznych czy w zbiorach nieinformatycznych).
   3) Ustalenie, czy dane przetwarzane dla określonego celu mają charakter danych podlegających szczególnej ochronie.

3. Do obowiązków Właścicieli zasobów danych osobowych należy:
   1) Zapewnienie niezbędnych uprawnień do przetwarzania danych osobowych.
   2) Zapewnienie aktualności, adekwatności oraz merytorycznej poprawności danych osobowych przetwarzanych w określonym przez nich celu.

3) Realizację obowiązku informacyjnego o przetwarzaniu danych osobowych osób, których dane osobowe są pozyskiwane.
4) Zapewnienie na żądanie uprawnionych osób, udostępnianie informacji o przetwarzanych danych osobowych oraz podmiotach, którym zostały one udostępnione.
5) Zapewnienie złożenia przez pracowników oświadczenia o znajomości przepisów o ochronie danych osobowych oraz zobowiązania do zachowania w tajemnicy danych osobowych oraz informacji na temat zabezpieczania danych osobowych.
6) Zapewnienie uzyskania przez pracowników przetwarzających dane osobowe, upoważnienia do przetwarzania danych osobowych.
7) Współpraca i informowanie ABI oraz ASI w przypadku utworzenia nowego zbioru danych osobowych ustalenie, kogo dotyczą dane osobowe, jaki jest ich zakres (np. imię i nazwisko, adres zamieszkania, NIP, PESEL itp.), cel przetwarzania oraz komu dane osobowe mają być udostępniane.
8) Przygotowanie wniosku do rejestracji/aktualizacji zbioru do GIODO w części A-D.
9) Wnioskowanie do Administratora Danych Osobowych o nadanie upoważnień dla pracowników podległej komórki organizacyjnej.
10) Prowadzenie ewidencji, o której mowa w § 6 w odniesieniu do Właścicieli zasobów.

§ 11

ODPOWIEDZIALNOŚĆ PRACOWNIKÓW I UZYTKOWNIKÓW SYSTEMU

1. W celu osiągnięcia i utrzymania wysokiego poziomu bezpieczeństwa przetwarzania danych osobowych konieczne jest szczególne zaangażowanie ze strony każdego pracownika i użytkownika zewnętrznego w zakresie ochrony danych osobowych.

2. Pracownicy oraz użytkownicy zewnętrzni są zobowiązani do informowania o wszelkich podejrzeniach naruszenia 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 w tajemnicy danych osobowych oraz informacji o sposobach ich

zabezpieczenia.

3) Ochrony danych osobowych oraz środków przetwarzających dane osobowe przed nieuprawnionym dostępem, ujawnieniem, modyfikacją, zniszczeniem lub zniekształceniem.

4. Wykonywania niezbędnych działań i w procesie przetwarzania danych celem zapewnienia właściwej ich ochrony, w tym celu powinni:

1) Przestrzegać procedur związanych z otwieraniem i zamykaniem pomieszczeń, a także z wejściem do obszarów przetwarzania danych osobowych osób nieupoważnionych.

2) Informować Administratora Bezpieczeństwa Informacji lub pracowników ochrony o podejrzanych osobach poruszających się w obszarze przetwarzania danych osobowych,

3) Pracownicy powinni na podstawie dokonanej identyfikacji ewentualnych zagrożeń, przedkładać Administratorowi Bezpieczeństwa Informacji projekty i propozycje nowych rozwiązań, których celem jest zwiększenie poziomu bezpieczeństwa ochrony danych osobowych.

§ 12
ODPOWIEDZIALNOŚĆ ZA NARUSZENIE ZASAD OCHRONY DANYCH OSOBOWYCH

1. Rozdział 8 ustawy a także art.266 Kodeksu Karnego określa odpowiedzialność pracownika w przypadku naruszenia ochrony danych osobowych.

2. Zgodnie z art.100 §2 pkt 5 Kodeksu Pracy – obowiązkiem pracownika jest przestrzeganie tajemnic prawnie chronionych określonych w odrębnych przepisach.

3. Ciężkie naruszenie obowiązków pracowniczych może skutkować rozwiązaniem umowy o pracę z winy pracownika bez wypowiedzenia umowy o pracę.

§ 13
SZKOLENIA

1. Przed rozpoczęciem przetwarzania danych osobowych każdy pracownik, stażysta, praktykant powinien zostać przeszkolony przez Administratora Bezpieczeństwa Informacji. Szkolenie powinno obejmować następujące zagadnienia:
   1) obowiązuję przepisy w zakresie o ochronie danych osobowych,
   2) procedury oraz zasady przetwarzania danych osobowych,
   3) procedury dotyczące bezpiecznego przetwarzania danych osobowych w systemach informatycznych .
   4) zasady użytkowania oprogramowania , urządzeń i systemów informatycznych służących do przetwarzania danych osobowych.

5) rodzaje zagrożeń jakie mogą być związane z przetwarzaniem danych osobowych w systemach informatycznych,
6) zasady dostępu do pomieszczeń, w których przetwarzane są dane osobowe,
7) Zasady i sposób postępowania w przypadku naruszenia ochrony danych osobowych lub systemu informatycznego.
8) odpowiedzialność w przypadku naruszenia ochrony danych osobowych.

2. Szkolenia należy przeprowadzać nie rzadziej niż dwa razy do roku ,a także każdorazowo w przypadku osoby nowozatrudnionej , stażystów i praktykantów,

§ 14
ZASADY SZCZEGÓLNEJ STARANNOŚCI

1. Każdy pracownik dla właściwego sposobu i zasad przetwarzania danych osobowych zobowiązany jest do zachowania szczególnej staranności przy przetwarzaniu danych osobowych a w szczególności:

   1) stosowanie wszelkich metod zabezpieczeń wynikających z Polityki,
   2) zabezpieczenie wydruków elektronicznych a także tych , które mogą być tworzone w trakcie kserowania, kopiowania,
   3) udzielanie informacji zawierających dane osobowe tylko osobom, podmiotom uprawnionym,
   4) prowadzenie rozmów telefonicznych w sposób bezpieczny , na zasadzie by osoba nieuprawniona nie pozyskiwała informacji jeżeli nie jest ona dla niej przeznaczona,

§ 15
MIEJSCA I POMIESZCZENIA PRZEZNACZONE DO PRZETWARZANIA DANYCH OSOBOWYCH

1. Dane osobowe można przetwarzać wyłącznie w miejscach bezpiecznych i będących pod właściwym nadzorem osoby, która przetwarza i nadzoruje przetwarzanie danych osobowych,
2. Pomieszczenia bezpieczne to takie , które nie są pozostawione bez nadzoru odpowiedzialnego pracownika,
   1) pomieszczenie biurowe,
   2) biuro obsługi interesanta,
   3) archiwum ,
   4) pomieszczenie , w którym znajdują się zbiory danych osobowych ,

3. Pomieszczenia , w których są przetwarzane dane osobowe są zamykane na klucz podczas nieobecności osoby upoważnionej/nadzorującej,

4. Obiekt jak i pomieszczenia są zabezpieczone fizycznie zgodnie z obowiązującymi procedurami i potrzebami,

5. W przypadku potrzeby należy zastosować dodatkowe zabezpieczenie fizyczne takie jak: kraty, rolety antywłamaniowe , szczególnie w przypadku pomieszczeń usytuowanych na parterze budynku,

6. Pomieszczenie powinno być wyposażone w sprzęt ppoż.,

7. W przypadku wykonywania prac naprawczych , remontowych , montażowych przez firmy zewnętrzne , pomieszczenie jest pod stałym nadzorem osoby upoważnionej- pracownika urzędu,

8. Przechowywanie kopii zapasowych powinno być realizowane w innym pomieszczeniu niż znajdują się zasoby podstawowe,

9. Każdy pracownik w przypadku zauważenia uchybień w zabezpieczeniu pomieszczenia zobowiązany jest niezwłocznie poinformować o tym fakcie Administratora Bezpieczeństwa Informacji.

§ 16
UPOWAŻNIENIA DO PRZETWARZANIA DANYCH OSOBOWYCH

1. Przetwarzanie danych osobowych jest możliwe wyłącznie po uzyskaniu przez pracownika upoważnienia do przetwarzania danych osobowych podpisanego przez Administratora danych Osobowych.

2. Upoważnienie do podpisania przez ADO przygotowuje Administrator Bezpieczeństwa Informacji,

3. Wzór upoważnienia stanowi zał.nr 3 do Polityki Bezpieczeństwa,

4. ABI prowadzi dla pracowników szkolenia z zakresu obowiązujących przepisów prawa i procedur zawartych w Polityce Bezpieczeństwa,
5. Pracownik po przeszkoleniu podpisuje oświadczenie o zapoznaniu się z przepisami i procedurami,

6. Wzór oświadczenia stanowi zał.nr 4 do Polityki Bezpieczeństwa.

7. Upoważnienie oraz oświadczenie jest przechowywane w aktach osobowych , oraz w dokumentacji ABI,

§ 17
EWIDENCJA OSÓB UPOWAŻNIONYCH

1. Administrator Bezpieczeństwa Informacji prowadzi ewidencję osób upoważnionych do przetwarzania danych osobowych ,

2. Ewidencja jest prowadzona przez ABI na bieżąco i starannie,

3. Ewidencja zawiera :
   - Imię i nazwisko osoby upoważnionej ,
   - Stanowisko,
   - Data nadania upoważnienia,
   - Data ustania upoważnienia,
   - Zakres upoważnienia,
   - Login/hasło użytkownika,

§ 18
ZBIORY DANYCH OSOBOWYCH – REJESTRACJA W BIURZE GIODO

1. Kierownicy komórek organizacyjnych oraz pracownicy powinni w porozumieniu z Administratorem Bezpieczeństwa Informacji współpracować w zakresie zgłaszania lub aktualizacji zbiorów danych osobowych,

2. Ostateczną decyzję o zarejestrowaniu zbioru w Krajowym Rejestrze Zbiorów prowadzonych przez GIODO podejmuje ABI,

3. ABI przygotowuje projekt zgłoszenia zbioru , powiadamia ADO o potrzebie zgłoszenia lub aktualizacji zbioru , po akceptacji ADO zgłasza zbiór do Krajowego Rejestru Zbiorów,

4. Po zgłoszeniu zbioru ABI dokonuje uzupełnień w wykazie zbiorów , który jest prowadzony przez ABI,

5. Zgłoszeniu podlegają wszystkie zbiory prowadzone w systemie informatycznym lub w sposób tradycyjny za wyjątkiem tych zbiorów , które są zawarte w art.43 ust.1 ustawy o ochronie danych osobowych,
6. Rejestracji można dokonać wypełniając wniosek w formie papierowej lub z wykorzystaniem platformy e-giodo znajdującej się na stronie www.giodo.gov.pl .

§ 19
UDOSTĘPNIANIE DANYCH OSOBOWYCH – ZASADY, PROCEDURY

1. Udostępnianie danych osobowych odbywa się na zasadzie potrzeby koniecznej,

2. Udostępnianie danych osobowych zewnętrznym podmiotom uprawnionym odbywa się na pisemny wniosek,

3. W przypadku udostępniania danych osobowych na zewnątrz Administrator Bezpieczeństwa Informacji dokonuje oceny sposobu przygotowania danych a także analizuje sposób i prawidłowość przygotowania danych do udostępnienia,

4. Dane osobowe przekazywane na zewnątrz są przekazywane listem poleconym za zwrotnym poświadczeniem odbioru lub innym bezpiecznym sposobem określonym wymogami prawa lub umową,

5. Fakt udostepnienia danych należy udokumentować pisemnie poprzez wykonanie pisma przewodniego lub notatki urzędowej,

§ 20
ODMOWA UDOSTĘPNIENIA DANYCH

1. Administrator danych odmawia osobie, której dane dotyczą, udzielenia informacji, jeżeli spowodowałoby to:

   1) ujawnienie wiadomości zawierających informacje niejawne,

   2) zagrożenie dla obronności lub bezpieczeństwa państwa, życia i zdrowia ludzi lub bezpieczeństwa i porządku publicznego,

   3) zagrożenie dla podstawowego interesu gospodarczego lub finansowego państwa,

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

§ 21
POWIERZENIE PRZETWARZANIA DANYCH OSOBOWYCH

1. Powierzenie danych osobowych odbywa się na zasadach określonych w art.31 ust.1 uodos ,

2. Powierzenie danych występuje wówczas , gdy podmiot zewnętrzny ma dostęp do danych osobowych przetwarzanych przez Urząd,

3. Administrator danych może powierzyć innemu podmiotowi współpracującemu z Urzędem na zasadzie wynikającej z umowy powierzenia,

4. Umowę powierzenia należy zawrzeć na piśmie , umowa powinna zawierać następujące warunki i zawierać:
    1) cel i zakres przetwarzania danych osobowych,
    2) sposoby zabezpieczenia danych i zasady ich przetwarzania ,
    3) zasady organizacyjne i techniczne jakie powinien spełnić podmiot , któremu powierzono przetwarzanie danych osobowych,
    4) Odpowiedzialność podmiotu , któremu powierzono dane osobowe za nieprawidłowe przetwarzanie danych osobowych,
    5) Prawo do kontroli podmiotu , któremu powierzono dane osobowe przez przedstawiciela Urzędu,

5. Projekt umowy powierzenia przygotowuje Administrator Bezpieczeństwa Informacji,

6. Administrator Bezpieczeństwa Informacji przed powierzeniem danych osobowych dokonuje kontroli stanu zabezpieczeń w jednostce , której dane osobowe będą powierzone .

§ 22

ZASADY POSTĘPOWANIA W PRZYPADKU NARUSZENIA LUB PODEJRZENIA NARUSZENIA OCHRONY DANYCH OSOBOWYCH

1. Pracownicy Urzędu są zobowiązani do szczególnej staranności przy przetwarzaniu danych osobowych,

2. Pracownicy każdorazowo przed przystąpieniem do pracy są zobowiązani do dokonania oceny i oględzin stanowiska pracy pod kątem , czy nie dokonano jakichkolwiek nieuprawnionych działań związanych z ochroną danych osobowych przez osoby nieuprawnione.

3. Sytuacje na które należy zwrócić szczególną uwagę to:

    1) próba nieuprawnionego dostępu do pomieszczenia lub dostępu do danych osobowych,

2) naruszenie lub próba naruszenia integralności, poufności lub rozliczalności danych i systemu,
3) niezamierzona zmiana lub utrata danych zapisanych na nośnikach jako kopie zapasowe,
4) próba nieuprawnionego logowania lub inny sygnał wskazujący na próbę lub działanie wskazujące na nielegalny dostęp do systemu,
5) losowe zdarzenia takie jak brak zasilania , pożar itp.,
6) stwierdzenie braku sprzętu informatycznego , jego części lub nośników zewnętrznych zawierających dane osobowe (wydruki , pamięć zewnętrzna, płyty CD, dysk twardy ,itp.).

4. W sytuacji , gdy pracownicy Urzędu stwierdza naruszenie lub próby naruszenia ochrony danych osobowych , wówczas są zobowiązani do niezwłocznego poinformowania o tym fakcie Administratora Bezpieczeństwa Informacji,

5. Przed poinformowaniem Administratora Bezpieczeństwa Informacji o naruszeniu lub próbie naruszenia ochrony danych osobowych , pracownik jest zobowiązany do :
1) wstrzymania pracy na stanowisku a także wykonywania jakichkolwiek działań , które mogłyby utrudnić ocenę i analizę stwierdzonych działań związanych z naruszeniem ochrony danych osobowych,
2) zabezpieczenia materiałów , dokumentów aby uniemożliwić dostęp osobom nieuprawnionym i dalsza stratą,
3) wykonywania wskazówek Administratora danych Osobowych.

6. Administrator Bezpieczeństwa Informacji powinien:
1) dokonać oceny sytuacji , szczególnie dokonać oględzin stanowiska pracy , pomieszczenia, stanu zabezpieczenia pomieszczenia, potencjalne skutki związane z naruszeniem ochrony danych osobowych,
2) podjąć dalsze działania stosowne do potrzeb i zaistniałej sytuacji.

7. Administrator Bezpieczeństwa Informacji jest zobowiązany do sporządzenia raportu z naruszenia ochrony danych osobowych (wzór raportu zał.nr 5 do Polityki Bezpieczeństwa).

8. Sytuacja związana z naruszeniem lub próbą naruszenia ochrony danych osobowych powinna być przedmiotem analizy i wniosków celem uniemożliwienia podobnych zdarzeń w przyszłości.

§ 23

ZBIORY DANYCH OSOBOWYCH

1. W rozumieniu ustawy o ochronie danych osobowych zbiorem danych osobowych jest każdy posiadający strukturę zestaw danych o charakterze osobowym, dostępnych według określonych kryteriów, niezależnie od tego, czy zestaw ten jest rozproszony lub podzielony funkcjonalnie.

2. Dane osobowe przetwarzane są w zbiorach z wykorzystaniem systemów informatycznych lub w kartotekach ewidencyjnych .

3. Zbiory danych osobowych są zlokalizowane w pomieszczeniach Urzędu.

4. Wykaz systemów i aplikacji związanych z przetwarzaniem danych osobowych oraz struktury zbiorów danych osobowych i opis struktur wskazujący zawartość poszczególnych pól powinien być prowadzony przez Administratora Systemów informatycznych .

5. Administrator Systemów Informatycznych prowadzi dokumentację związaną ze sposobem i zasadami współpracy i przepływu danych pomiędzy poszczególnymi systemami.

6. Administrator Bezpieczeństwa Informacji jest zobowiązany do bieżącego zgłaszania zbiorów do Krajowego Rejestru Zbiorów prowadzonego przez Generalnego Inspektora Ochrony Danych Osobowych a także ich aktualizacji w przypadku takiej potrzeby .

§ 24

OCHRONA DANYCH OSOBOWYCH W ZBIORACH NIEINFORMATYCZNYCH

1. Zbiory i dane przetwarzane w tych zbiorach to takie dane , które są przetwarzane w formie tradycyjnej bez wykorzystywania systemów informatycznych .

2. Dane osobowe w formie dokumentów i wydruków podlegają ochronie a także odpowiedniemu ich zabezpieczeniu w meblach biurowych zamykanych na klucz.

3. Dokumenty , wydruki podlegające zniszczeniu należy zniszczyć skutecznie, tak by osoba nieuprawniona nie mogła zapoznać się z treścią tych dokumentów lub wydruków.

4. W trakcie niszczenia dokumentów należy przestrzegać przepisów Ustawy o Narodowym Zasobie Archiwalnym i przepisów wykonawczych do ustawy.

§ 25

KONTROLE PROWADZONE PRZEZ GENERALNEGO INSPEKTORA OCHRONY DANYCH OSOBOWYCH

1. Zgodnie z art.12 Ustawy o Ochronie Danych Osobowych , Generalny Inspektor ochrony Danych Osobowych ma uprawnienia do kontroli przetwarzania danych osobowych z przepisami o ochronie danych osobowych, a także wydawanie decyzji administracyjnych i rozpatrywanie skarg w sprawach wykonywania przepisów o ochronie danych osobowych.

2. W celu wykonywania zadań , o których mowa w pkt.1 upoważnieni pracownicy Biura maja prawo:

1) wstępu, w godzinach od 7°° do 15°°, za okazaniem imiennego upoważnienia i legitymacji służbowej, do pomieszczenia, w którym zlokalizowany jest zbiór danych, oraz pomieszczenia, w którym przetwarzane są dane poza zbiorem danych, i przeprowadzenia niezbędnych badań lub innych czynności kontrolnych w celu oceny zgodności przetwarzania danych z ustawą,
2) żądać złożenia pisemnych lub ustnych wyjaśnień oraz wzywać i przesłuchiwać osoby w zakresie niezbędnym do ustalenia stanu faktycznego,
3) wglądu do wszelkich dokumentów i wszelkich danych mających bezpośredni związek z przedmiotem kontroli oraz sporządzania ich kopii,
4) przeprowadzania oględzin urządzeń, nośników oraz systemów informatycznych służących do przetwarzania danych,
5) zlecać sporządzanie ekspertyz i opinii

3. Administrator Danych jest zobowiązany do umożliwienia przeprowadzenia kontroli .

4. W toku kontroli kontrolujący ma prawo wglądu do zbioru danych osobowych za pośrednictwem Administratora Bezpieczeństwa Informacji.

5. Kontrolę przeprowadza się po okazaniu imiennego upoważnienia wraz z legitymacją służbową.

6. Imienne upoważnienie powinno zawierać:

1) wskazanie podstawy prawnej przeprowadzenia kontroli,
2) oznaczenie organu kontroli,
3) imię i nazwisko, stanowisko służbowe osoby upoważnionej do przeprowadzenia kontroli oraz numer jej legitymacji służbowej,
4) określenie zakresu przedmiotowego kontroli,
5) oznaczenie podmiotu objętego kontrolą albo zbioru danych, albo miejsca poddawanego kontroli,
6) wskazanie daty rozpoczęcia i przewidywanego terminu zakończenia kontroli,
7) podpis Generalnego Inspektora,
8) pouczenie kontrolowanego podmiotu o jego prawach i obowiązkach,
9) datę i miejsce wystawienia imiennego upoważnienia.

7. Z czynności kontrolnych inspektor sporządza protokół, którego jeden egzemplarz doręcza kontrolowanemu .

8. Protokół podpisują inspektor i kontrolowany Administrator Danych .

9. W razie odmowy podpisania protokołu inspektor czyni o tym wzmiankę w protokole , a wówczas można w terminie 7 dni , przedstawić swoje stanowisko na piśmie Generalnemu Inspektorowi Ochrony Danych Osobowych.

§ 26

POSTANOWIENIA KOŃCOWE

1. W sprawach nieuregulowanych w Polityce mają zastosowanie przepisy ustawy z dnia 29 sierpnia 1997r.,o ochronie danych osobowych (t.j Dz.U. z 2014 r,poz.1182 z późn.zm) oraz przepisy wykonawcze do Ustawy.

ZAŁĄCZNIKI

Załączniki do Polityki bezpieczeństwa przetwarzania danych osobowych w Urzędzie Miejskim w Krobi.

1. Załącznik nr 1 –ewidencja osób upoważnionych do przetwarzania danych osobowych,
2. Załącznik nr 2 – ewidencja zbiorów przetwarzanych danych osobowych
3. Załącznik nr 3 – upoważnienie do przetwarzania danych osobowych ,
4. Załącznik nr 4 – oświadczenie pracownika ,
5. Załącznik nr 5 – raport z naruszenia ochrony danych osobowych.

Załącznik Nr 1do Polityki Bezpieczeństwa

Ewidencja osób zatrudnionych przy przetwarzaniu danych osobowych w Urzędzie Miejskim w Krobi.

L.p.	Imię i nazwisko	Stanowisko	Komórka organizacyjna	Data przeszkolenia	Nr upoważnienia imiennego	Identyfikator	Data nadania upoważnienia	Data ustania upoważnienia	Zakres upoważnienia*

*Zakres upoważnienia:

wgląd	**D**
wprowadzanie	**W**
modyfikacja	**M**
usuwanie	**U**

Załącznik Nr 2 do Polityki Bezpieczeństwa

Ewidencja zbiorów danych przetwarzanych w URZĘDZIE MIEJSKIM W KROBI

Lp	NAZWA ZBIORU	Zakres przetwarzanych w zbiorze danych o osobach	Inne dane osobowe	System danych T-tradyc. I-inform.	Nazwa Programu 1) forma danych 2) zabezpieczenie informatyczne, 3) bazę danych chroni UPS (TAK / NIE)	Lokalizacja	Zabezpieczenie fizyczne
1.	ELEKTRONICZNY OBIEG DOKUMENTÓW, DZIENNIK KORESPONDENCJI	nazwiska i imiona adres zamieszkania lub pobytu	adres poczty elektronicznej,	I	E-SODA - PEMI 1) baza plikowa, 2) indywidualne hasło dostępu, 3) tak	- *Krobia, Rynek 1* - *Ratusz*	Kontrola dostępu przy rozpoczęciu i po zakończeniu pracy, zamki patentowe, wydruki przechowywane w szafach zamykanych na klucz, , zabezp. p.poż.
2.	REJESTR SKARG I WNIOSKÓW	nazwiska i imiona, adres zamieszkania lub pobytu, numer telefonu,		T	Nie dotyczy	- *Krobia, Rynek 1* - *Ratusz nr 10*	Kontrola dostępu przy rozpoczęciu i po zakończeniu pracy, zamki patentowe, wydruki przechowywane w szafach zamykanych na klucz, , zabezp. p.poż.
3.	SYSTEM KADROWY	nazwiska i imiona, imiona rodziców, data urodzenia, adres zamieszkania lub pobytu, numer ewidencyjny	dochody: miejsce pracy lub nauki członków rodziny, dochody członków rodziny ze wszystkich źródeł	I	KADRY - RADIX PRACOWNIKÓW JEDNOSTKI ORG. 1) baza plikowa, 2) indywidualne	- *Krobia, Rynek 1* - *Ratusz nr 3, 10, 13 (serwerownia)*	Kontrola dostępu przy rozpoczęciu i po zakończeniu pracy, zamki patentowe, wydruki przechowywane

		pesel, zawód, wykształcenie, seria i numer dowodu osobistego,			hasło dostępu, 3) tak		w szafach zamykanych na klucz, , zabezp. p.poż.
4.	SYSTEM ROZLICZEŃ Z ZUS	dane identyfikacyjne osoby ubezpieczonej: identyfikator ubezpieczonego, numer PESEL, NIP, seria i numer dokumentu tożsamości, nazwisko ubezpieczonego, pierwsze imię ubezpieczonego, data urodzenia, adres, numer telefonu,	informacje odnośnie wymiaru i wysokości składek, zasiłków chorobowych, niepełnosprawności	I	Prokom-PŁATNIK 1) baza plikowa, 2) indywidualne hasło dostępu, 3) tak	- *Krobia, Rynek 1* - *Ratusz nr 3, 13 (serwerownia)*	Kontrola dostępu przy rozpoczęciu i po zakończeniu pracy, zamki patentowe, wydruki przechowywane w szafach zamykanych na klucz, , zabezp. p.poż.
5.	SYSTEM PŁACOWY	identyfikator ubezpieczonego, pesel, nip, nazwisko i imię, data urodzenia, rodzaj dokumentu tożsamości, numer i seria dokumentu tożsamości,	dane rodzinne, informacje o niepełnosprawności, dane o składkach na ubezpieczenie społeczne, wysokość potrąconego podatku dochodowego, informacje o wynagrodzeniu i obciążeniach, absencja w pracy, wysokość zasiłku chorobowego, nazwisko rodowe, imię ojca i matki, miejsce urodzenia, stan cywilny, nagrody i kary, obowiązek wojskowy, numer konta bankowego	I	PŁACE – RADIX PRACOWNIKÓW URZĘDU 1) baza plikowa , 2) indywidualne hasło dostępu, 3) tak	- *Krobia, Rynek 1* - *Ratusz nr 3, 13 (serwerownia)*	Kontrola dostępu przy rozpoczęciu i po zakończeniu pracy, zamki patentowe, wydruki przechowywane w szafach zamykanych na klucz, , zabezp. p.poż.
6.	DANE OSOBOWE NIEZBĘDNE DO PROWADZENIA URZĘDU STANU CYWILNEGO	nazwiska i imiona, imiona rodziców, data urodzenia, adres zamieszkania lub pobytu,		I	USC-WIN firmy ARAM 1) baza plikowa , 2) indywidualne hasło dostępu,	- *Krobia, pl. Kościuszki 3*	Kontrola dostępu przy rozpoczęciu i po zakończeniu pracy, zamki patentowe, wydruki przechowywane

		numer ewidencyjny pesel, wykształcenie, seria i numer dowodu osobistego,			3) tak		w szafach zamykanych na klucz, , zabezp. p.poż.
7.	EWIDENCJA LUDNOŚCI DOWODY OSOBISTE	nazwiska i imiona, imiona rodziców, data urodzenia, adres zamieszkania lub pobytu, numer ewidencyjny pesel, wykształcenie, seria i numer dowodu osobistego,		I	SEL-WIN firmy Aram Program IDL SYSTEM 1) baza plikowa , 2) indywidualne hasło dostępu, 3) tak	- *Krobia, pl. Kościuszki 3*	Kontrola dostępu przy rozpoczęciu i po zakończeniu pracy, zamki patentowe, wydruki przechowywane w szafach zamykanych na klucz,
8.	POGRUN – NALICZANIE PODATKU OD NIERUCHOMOŚCI I ROLNEGO	nazwiska i imiona, imiona rodziców, data urodzenia, adres zamieszkania lub pobytu, numer ewidencyjny pesel, wykształcenie, seria i numer dowodu osobistego,		I	POGRUN firmy RADIX 1) baza plikowa , 2) indywidualne hasło dostępu, 3) tak	- *Krobia, Rynek 1* - *Ratusz nr 2, 13 (serwerownia)*	Kontrola dostępu przy rozpoczęciu i po zakończeniu pracy, zamki patentowe, wydruki przechowywane w szafach zamykanych na klucz,
9.	WIP – WINDYKACJA PODATKÓW LOKALNYCH	nazwiska i imiona, imiona rodziców, data urodzenia, adres zamieszkania lub pobytu, numer ewidencyjny pesel, seria i numer dowodu osobistego,		I	WIP firmy RADIX 1) baza plikowa , 2) indywidualne hasło dostępu, 3) tak	- *Krobia, Rynek 1* - *Ratusz nr 2, 13 (serwerownia)*	Kontrola dostępu przy rozpoczęciu i po zakończeniu pracy, zamki patentowe, wydruki przechowywane w szafach zamykanych na klucz, , zabezp. p.poż.

10.	DANE O NAUCZYCIELACH, WYCHOWAWCACH I INNYCH PRACOWNIKACH PEDAGOGICZNYCH GROMADZONE W SYSTEMIE INFORMACJI OŚWIATOWEJ.	nazwiska i imiona, imiona rodziców, data urodzenia, adres zamieszkania lub pobytu, numer ewidencyjny pesel, zawód, wykształcenie, seria i numer dowodu osobistego,		I	SIO MENiS 1) baza plikowa , 2) indywidualne hasło dostępu, 3) tak	- *Krobia, pl. Kościuszki 3*	Kontrola dostępu przy rozpoczęciu i po zakończeniu pracy, zamki patentowe, wydruki przechowywane w szafach zamykanych na klucz, , zabezp. p.poż.
11.	DANE KONT BANKOWYCH PRACOWNIKÓW I KONTRAHENTÓW	nazwiska i imiona, adres zamieszkania lub pobytu, numer ewidencyjny NIP, seria i numer dowodu osobistego,		I	Homebanking PKO 1) baza plikowa , 2) indywidualne hasło dostępu, 3) tak	- *Krobia, Rynek 1* - *Ratusz nr 3,*	Kontrola dostępu przy rozpoczęciu i po zakończeniu pracy, zamki patentowe, wydruki przechowywane w szafach zamykanych na klucz, , zabezp. p.poż.
12.	FAKTURA VAT - OBSŁUGA ROZRACHUNKÓW (NALEŻNOŚCI I ZOBOWIĄZAŃ)	nazwiska i imiona, adres zamieszkania lub pobytu, numer ewidencyjny NIP,		I	Subiekt GT - INSERT 1) baza plikowa , 2) indywidualne hasło dostępu, 3) tak	- *Krobia, Rynek 1* - *Ratusz nr 3, 13 (serwerownia)*	Kontrola dostępu przy rozpoczęciu i po zakończeniu pracy, zamki patentowe, wydruki przechowywane w szafach zamykanych na klucz, , zabezp. p.poż.

Załącznik Nr 3 do Polityki Bezpieczeństwa w Urzędzie Miejskim w Krobi

/nazwa jednostki/

U P O W A Ż N I E N I E *Nr .....*

Zgodnie z art. 37 ustawy z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (Dz. U. z 2014r. , poz. 1182 z późn. zm.), zgodnie z zakresem czynności i złożonego oświadczenia w sprawie znajomości przepisów dotyczących ochrony danych osobowych

U p o w a ż n i a m

Pana/Panią:

.....

imie i nazwisko

do przetwarzania danych osobowych gromadzonych w systemie informatycznym/ nie informatycznym w ..... w zbiorach :

(nazwa komórki organizacyjnej)

Lp.	PEŁNA NAZWA ZBIORU

Powyższe upoważnienie wydaje się na okres do .....

(wpisać na jaki okres lub czas zatrudnienia)

Administrator Danych Osobowych

.....

....

/miejscowość/ */data/*

Załącznik Nr 4 do Polityki Bezpieczeństwa w Urzędzie Miejskim w Krobi.

OŚWIADCZENIE

Imię i nazwisko	
Stanowisko służbowe	
Nazwa komórki organizacyjnej	

Stwierdzam własnoręcznym podpisem, że zapoznałem/am/ się z „Polityką Bezpieczeństwa w Urzędzie Miejskim w Krobi " oraz Instrukcją zarządzania systemem informatycznym służącym do przetwarzania danych osobowych w Urzędzie Miejskim w Krobi .

Jednocześnie, zgodnie z przepisami ustawy z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (Dz. U. z 2014 r. poz. 1182 z późn. zm.) zobowiązuję się do ochrony przed niepowołanym dostępem, nieuzasadnioną modyfikacją lub zniszczeniem, nielegalnym ujawnieniem lub pozyskaniem, danych osobowych przetwarzanych w Urzędzie Miejskim w Krobi oraz do zachowania ich w tajemnicy w czasie trwania jak i po ustaniu zatrudnienia.

Równocześnie oświadczam, że zostałem(am) poinformowany(a) o odpowiedzialności służbowej i karnej w przypadku naruszenia przepisów.

....

(imię, nazwisko i podpis osoby przyjmującej oświadczenie)

(data i podpis składającego oświadczenie)

Załącznik nr 5 do „Polityki bezpieczeństwa „

Raport
z naruszenia ochrony danych osobowych

w .....

1. Data: ..... Godzina: .....
(dzień, miesiąc, rok) *(00:00)*

2. Osoba powiadamiająca o zaistniałym zdarzeniu:

.....
(Imię, nazwisko, stanowisko służbowe, nazwa użytkownika (jeśli występuje))

3. Lokalizacja zdarzenia:

.....
(np. nr pokoju, nazwa pomieszczenia)

4. Rodzaj naruszenia bezpieczeństwa oraz okoliczności towarzyszące:

.....
.....

5. Podjęte działania:
.....
.....

6. Przyczyny wystąpienia zdarzenia:
.....
.....

7. Postępowanie wyjaśniające:
.....
.....

.....
/ data, podpis Administratora Bezpieczeństwa Informacji/

Załącznik Nr 2 do Zarządzenia Nr 3/W/2015 z dnia 10 lutego 2015r.

INSTRUKCJA ZARZĄDZANIA

SYSTEMEM INFORMATYCZNYM SŁUŻĄCYM

DO PRZETWARZANIA DANYCH OSOBOWYCH

w URZĘDZIE MIEJSKIM W KROBI

§ 1.

POSTANOWIENIA OGÓLNE

Instrukcja zarządzania systemem informatycznym, służącym do przetwarzania danych osobowych w Urzędzie Miejskim w Krobi , określa:

1) Instrukcja zarządzania systemem informatycznym służącym do przetwarzania danych osobowych w Urzędzie Miejskim w Krobi, zwana dalej „Instrukcją" określa zasady , tryb postępowania i zalecenia Administratora Danych Osobowych , które należy stosować w trakcie przetwarzania danych osobowych w systemach informatycznych,
2) sposób przydziału haseł dla użytkowników i częstotliwość ich zmiany oraz osoby odpowiedzialne za te czynności,
3) sposób rejestrowania i wyrejestrowywania użytkowników oraz osoby odpowiedzialne za te czynności,
4) zasady i procedury rozpoczynania i kończenia pracy,
5) zasady i częstotliwość tworzenia kopii bezpieczeństwa.
6) zasady i częstotliwość kontroli obecności wirusów komputerowych oraz metodę ich usuwania,
7) zasady i czas przechowywania nośników informacji, w tym kopii informatycznych,
8) zasady dokonywania przeglądów i konserwacji systemu i zbioru danych osobowych,
9) zasady postępowania w zakresie komunikacji w sieci komputerowej,
10) instrukcja opracowana została zgodnie z wymogami § 5 Rozporządzenia Ministra Spraw Wewnętrznych i 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 w systemach informatycznych.

§ 2.

DEFINICJE ZAWARTE W INSTRUKCJI

Ilekroć w instrukcji jest mowa o :

1) **ustawa** - rozumie się przez to ustawę z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (Dz. U. z 2014 r., poz. 1182 z późn. zm.), zwaną dalej *„ustawą"*;
2) **Jednostka** – rozumie się przez to Urząd Miejski w Krobi

3) **identyfikator użytkownika** - rozumie się przez to ciąg znaków literowych, cyfrowych lub innych jednoznacznie identyfikujący osobę upoważnioną do przetwarzania danych osobowych w systemie informatycznym;
4) **hasło** - rozumie się przez to ciąg znaków literowych, cyfrowych lub innych, znany jedynie osobie uprawnionej do pracy w systemie informatycznym;
5) **sieć telekomunikacyjna** - rozumie się przez to sieć telekomunikacyjną w rozumieniu art. 2 pkt 35 ustawy z dnia 16 lipca 2004 r. - Prawo telekomunikacyjne
6) **sieć publiczna** - rozumie się przez to sieć publiczną w rozumieniu art. 2 pkt 29 ustawy z dnia 16 lipca 2004 r. - Prawo telekomunikacyjne;
7) **teletransmisja** - rozumie się przez to przesyłanie informacji za pośrednictwem sieci telekomunikacyjnej;
8) **rozliczalność** - rozumie się przez to właściwość zapewniającą, że działania podmiotu mogą być przypisane w sposób jednoznaczny tylko temu podmiotowi;
9) **integralność danych** - rozumie się przez to właściwość zapewniającą, że dane osobowe nie zostały zmienione lub zniszczone w sposób nieautoryzowany;
10) **raport** - rozumie się przez to przygotowane przez system informatyczny zestawienia zakresu i treści przetwarzanych danych;
11) **poufność danych** - rozumie się przez to właściwość zapewniającą, że dane nie są udostępniane nieupoważnionym podmiotom;
12) **uwierzytelnianie** - rozumie się przez to działanie, którego celem jest weryfikacja deklarowanej tożsamości podmiotu,
13) **Administrator Danych (AD)** - w świetle przepisów ustawy o ochronie danych osobowych , art. 3 i 7 pkt 4 rozumie się przez to kierownika jednostki, który decyduje o celach i środkach przetwarzania danych osobowych;
14) **Administrator Bezpieczeństwa Informacji (ABI)** - rozumie się przez to osobę wyznaczoną przez Administratora Danych (kierownika jednostki), nadzorującą przestrzeganie zasad ochrony danych osobowych, w szczególności zabezpieczenia danych przed ich udostępnieniem osobom nieupoważnionym, zabraniem przez osobę nieuprawnioną, przetwarzaniem z naruszeniem ustawy oraz zmianą, utratą, uszkodzeniem lub zniszczeniem;
15) **Administrator Systemu Informatycznego (ASI), zwanego też Administratorem Systemu** - rozumie się przez to osobę zatrudnioną przez kierownika jednostki,

upoważnioną do realizacji zadań związanych z zarządzaniem systemem informatycznym;

16) **użytkownik systemu informatycznego** - rozumie się przez to upoważnioną przez kierownika jednostki , pracownika do przetwarzania danych osobowych w systemie informatycznym , który odbył stosowne szkolenie w zakresie ochrony danych.

§ 3.

ZASADY DOSTĘPU UZYTKOWNIKA DO SYSTEMU

1. Dostęp do systemu informatycznego służącego do przetwarzania danych osobowych, zwanego dalej „systemem" może uzyskać wyłącznie osoba (użytkownik) zarejestrowana w tym systemie przez Administratora Systemu na wniosek kierownika komórki organizacyjnej i po akceptacji Administratora Bezpieczeństwa Informacji.

3. Rejestracja, o której mowa w ust. l, polega na nadaniu identyfikatora i przydziale hasła oraz wprowadzeniu tych danych do bazy użytkowników systemu.

§ 4.

IDENTYFIKATOR

1. Identyfikator składa się z minimum sześciu znaków.

2. W identyfikatorze pomija się polskie znaki diakrytyczne.

3. W przypadku zbieżności nadawanego identyfikatora z identyfikatorem wcześniej zarejestrowanego użytkownika Administrator Systemu po uzgodnieniu z ABI nadaje inny identyfikator.

§ 5.

HASŁA

1. Hasło powinno składać się z unikalnego zestawu co najmniej ośmiu znaków, zawierać małe i wielkie litery oraz cyfry lub znaki specjalne.

2. Hasło nie może być identyczne z identyfikatorem użytkownika, ani z jego imieniem lub nazwiskiem.

3. Zmiana hasła powinna następować nie rzadziej niż co 30 dni z zastrzeżeniem § 6.

4. Zabrania się użytkownikom systemu udostępniania swojego identyfikatora i hasła innym osobom.

§ 6.
WYREJESTROWANIE UZYTKOWNIKA

1. Wyrejestrowania użytkownika z systemu informatycznego dokonuje Administrator Systemu na wniosek kierownika komórki organizacyjnej.

2. Wyrejestrowanie, o którym mowa w ust. 1, może mieć charakter czasowy lub trwały.

3. Wyrejestrowanie następuje poprzez:

1) zablokowanie konta użytkownika do czasu ustania przyczyny uzasadniającej blokadę (wyrejestrowanie czasowe),
2) usunięcie danych użytkownika z bazy użytkowników systemu (wyrejestrowanie trwałe).

4. Przyczyną czasowego wyrejestrowania użytkownika z systemu informatycznego jest:

3) nieobecność w pracy trwająca dłużej niż 31 dni kalendarzowych,
4) zawieszenie w pełnieniu obowiązków służbowych,
5) zwolnienie z pełnienia obowiązków służbowych.

5. Przyczyną trwałego wyrejestrowania użytkownika z systemu informatycznego jest rozwiązanie lub wygaśnięcie stosunku pracy użytkownika.

§ 7.
ROZPOCZĘCIE PRACY W SYSTEMIE

Rozpoczęcie pracy w systemie odbywa się poprzez:

1) przygotowanie stanowiska pracy,
2) włączenie stacji roboczej,
3) wprowadzenie swojego identyfikatora i hasła.

§ 8.
ZAKOŃCZENIE PRACY W SYSTEMIE

Zakończenie pracy w systemie odbywa się poprzez:

1) zamknięcie aplikacji,
2) odłączenie się od zasobów systemowych,
3) zamknięcie systemu operacyjnego,
4) wyłączenie stacji roboczej.

§ 9.
ZASADY PRACY W SYSTEMIE

1. Zabrania się użytkownikom pracującym w systemie:

1) udostępniania stacji roboczej osobom niezarejestrowanym z zastrzeżeniem pkt 2,
2) udostępniania stacji roboczej do konserwacji lub naprawy bez porozumienia z Administratorem Systemu Informatycznego,
3) używania nielicencjonowanego oprogramowania.

§ 10.
NARUSZENIE BEZPIECZEŃSTWA SYSTEMU

1. Każdy przypadek naruszenia ochrony danych osobowych, które mogą wskazywać na naruszenie bezpieczeństwa podlega zgłoszeniu do Administratora Bezpieczeństwa Informacji, a w szczególności:

1) naruszenia bezpieczeństwa systemu informatycznego,
2) stwierdzenia objawów (stanu urządzeń, sposobu działania programu lub jakości komunikacji w sieci).

2. Administratorowi Bezpieczeństwa Informacji zgłasza się w szczególności przypadki:

1) użytkowania stacji roboczej przez osobę nie będącą użytkownikiem systemu,
2) usiłowania logowania się do systemu (sieci) przez osobę nieuprawnioną,
3) usuwania, dodawania lub modyfikowania bez wiedzy i zgody użytkownika jego dokumentów (rekordów),
4) przebywania osób nieuprawnionych w obszarze, w którym przetwarzane są dane osobowe, w trakcie nieobecności osoby zatrudnionej przy przetwarzaniu tych danych

i bez zgody Administratora Danych, pozostawiania bez nadzoru otwartych pomieszczeń, w których przetwarzane są dane osobowe,

5) udostępniania osobom nieuprawnionym stacji roboczej lub komputera przenośnego, służących do przetwarzania danych osobowych,
6) niezabezpieczenia hasłem dostępu do komputera służącego do przetwarzania danych osobowych,
7) przechowywania kopii awaryjnych w tych samych pomieszczeniach, w których przechowywane są zbiory danych osobowych eksploatowane na bieżąco,
8) przechowywania nośników informacji oraz wydruków z danymi osobowymi, nieprzeznaczonymi do udostępniania, w warunkach umożliwiających do nich dostęp osobom nieuprawnionym.

3. Obowiązek dokonania zgłoszenia, o którym mowa w ust 1, spoczywa na każdym użytkowniku, który powziął wiadomość o naruszeniu ochrony danych osobowych.

4. W przypadku naruszenia integralności bezpieczeństwa sieciowego, obowiązkiem Administratora Systemu jest natychmiastowe wstrzymanie udostępniania zasobów dla użytkowników i odłączenie serwerów od sieci.

5. Użytkownik sieci i Administrator Systemu w porozumieniu z Administratorem Bezpieczeństwa Informacji ustalają przyczyny naruszenia integralności bezpieczeństwa sieciowego.

6. Przywrócenie udostępniania zasobów użytkownikom może nastąpić dopiero po ustaleniu i usunięciu przyczyny naruszenia integralności bezpieczeństwa sieciowego.

§ 11.
KOPIE ZAPASOWE

1. Kopie awaryjne tworzy się z następującą częstotliwością:
1) kopie systemu finansowo - księgowego – dwa razy w miesiącu,
2) kopie pozostałe - nie rzadziej niż raz na miesiąc.

2. Każdą kopię tworzy się na oddzielnym nośniku informatycznym.

3. Zabrania się przechowywania kopii awaryjnych w pomieszczeniach przeznaczonych
do przechowywania zbiorów danych pozostających w bieżącym użytkowaniu.

4. Administrator Systemu przegląda okresowo kopie awaryjne i ocenia ich przydatność
do odtworzenia zasobów systemu w przypadku jego awarii.

5. Stwierdzenie utraty przez kopie awaryjne waloru przydatności do celu, o którym mowa w ust. 4, upoważnia Administratora Systemu do ich zniszczenia.

§ 12.

1. Sprawdzanie obecności wirusów komputerowych w systemie oraz ich usuwanie odbywa się przy wykorzystaniu licencjonowanego oprogramowania w oparciu o serwer dystrybucji aktualnych sygnatur i wersji oprogramowania.

2. Oprogramowanie, o którym mowa w ust. 1, sprawuje ciągły nadzór (ciągła praca w tle) nad pracą systemu i jego zasobami oraz serwerami i stacjami roboczymi.

3. Niezależnie od ciągłego nadzoru, o którym mowa w ust. 2, Administrator Systemu nie rzadziej niż raz na dwa miesiące przeprowadza pełną kontrolę obecności wirusów komputerowych w systemie oraz jego zasobach, jak również w serwerach i stacjach roboczych.

4. Do obowiązków Administratora Systemu należy aktualizacja oprogramowania służącego do sprawdzania w systemie obecności wirusów komputerowych.

§ 13.

ZASILANIE AWARYJNE

1. System i urządzenia informatyczne służące do przetwarzania danych osobowych, zasilane energią elektryczną, zabezpiecza się przed utratą danych osobowych spowodowaną awarią zasilania lub zakłóceniami w sieci zasilającej.

2. Minimalne zabezpieczenie systemu i urządzeń informatycznych, o których mowa w ust. 1, polega na wyposażeniu serwera (serwerów) oraz stacji roboczych w zasilacze awaryjne .

§ 14.

NAPRAWA, SERWIS URZĄDZEŃ

1. Urządzenia informatyczne służące do przetwarzania danych osobowych można przekazać do naprawy, do likwidacji dopiero po uprzednim uzyskaniu zgody Administratora Bezpieczeństwa Informacji.

2. Urządzenia, o których mowa w ust. l przed ich przekazaniem pozbawia się zapisu danych osobowych poprzez wymontowanie dysku twardego z zastrzeżeniem ust. 3.

3. Jeżeli nie jest to możliwe, urządzenie to może być naprawiane wyłącznie pod nadzorem Administratora Systemu.

4. Jeżeli nie jest możliwe pozbawienie urządzenia przekazywanego do likwidacji zapisu danych osobowych, urządzenie - przed przekazaniem - uszkadza się w sposób uniemożliwiający odczytanie tych danych.

§ 15.

PRZEGLĄD , KONSERWACJE

1. Przeglądu i konserwacji systemu dokonuje Administrator Systemu doraźnie.

2. Przeglądu pliku zawierającego raport dotyczący działalności aplikacji bądź systemu (log systemowy) Administrator Systemu dokonuje nie rzadziej niż raz na miesiąc .

3. Przeglądu i sprawdzenia poprawności zbiorów danych zawierających dane osobowe dokonuje użytkownik przy współudziale Administratora Systemu nie rzadziej niż raz na miesiąc.

§ 16.

BEZPIECZEŃSTWO KOMUNIKACJI

1. Bezpieczeństwo komunikacji w obrębie systemów przetwarzających dane osobowe Administrator Systemu zapewnia przy użyciu narzędzi w obrębie systemu.

2. W systemach działających sieciowo, na zasadzie udostępnienia zasobów na serwerze, Administrator Systemu powinien uwzględniać dedykowane przyzwolenia dostępu.

§ 17

KOMUNIKACJA WEWNĘTRZNA

1. Przesyłanie danych osobowych w komunikacji wewnętrznej (LAN) musi być oznaczone w sposób dostępny jedynie dla uprawnionych użytkowników przy użyciu narzędzi zabezpieczeń w obrębie systemu informatycznego.

2. W sytuacji, gdy dostępne narzędzia informatyczne nie będą wystarczające do działania w komunikacji wewnętrznej, użytkownik systemu wyznacza sposób

postępowania, mając w szczególności na uwadze ochronę danych osobowych.

§ 18.

Do przesyłania danych przy połączeniach w sieci publicznej (Internet), z uwagi na przekazywane dane osobowe, powinny być wykorzystywane tylko kanały transmisji wykorzystywane przez autoryzowane programy wykorzystywane również w innych urzędach oraz instytucjach państwowych i w oparciu o przepisy prawne regulujące sposób wysyłania tych danych.

§ 19.

OZNACZANIE NOŚNIKÓW DANYCH

Nośniki informatyczne zawierające dane osobowe powinny być opisane w sposób czytelny i zrozumiały dla użytkownika, a zarazem nie powinny ułatwiać rozpoznania zawartości przez osoby nieupoważnione.

§ 20.

BEZPIECZEŃSTWO NOSNIKÓW,URZĄDZEŃ

I. Nośniki informatyczne przechowywane są w miejscach, do których dostęp mają wyłącznie osoby upoważnione.

2. W pomieszczeniach, gdzie nie jest możliwe ograniczenie dostępu osób postronnych, monitory stanowisk dostępu do danych osobowych ustawia się w taki sposób, aby uniemożliwić tym osobom wgląd w dane.

3. Ekrany monitorów stanowisk dostępu do danych osobowych są zaopatrzone w wygaszacze z ustawioną opcją wymagania hasła, które po upływie maksymalnie 20 minut nieaktywności użytkownika automatycznie wyłączają możliwość eksploracji ekranu.

§ 21.

PRZENOŚNE NOŚNIKI INFORMATYCZNE

Osoby użytkujące przenośne nośniki informatyczne, służące do przetwarzania danych osobowych, obowiązane są niezwłocznie informować na piśmie Administratora

Bezpieczeństwa Informacji o zakresie, rodzaju zbieranych danych osobowych oraz celu ich przetwarzania. Administrator Bezpieczeństwa Informacji może żądać usunięcia danych, co do których zachodzi uzasadnione podejrzenie, że nie są przetwarzane zgodnie z zasadami określonymi w przepisach o ochronie danych osobowych.

§ 22.
PRZENOSNY KOMPUTER

Osoba użytkująca przenośny komputer, służący do przetwarzania danych osobowych, obowiązana jest zachować szczególną ostrożność podczas transportu i przechowywania tego komputera poza obszarem ochrony danych w celu zapobieżenia dostępowi do tych danych osobie niepowołanej.

§ 23.
WYDRUKI

1. Użytkownik sporządzający wydruki, które zawierają dane osobowe jest odpowiedzialny za zachowanie szczególnej ostrożności przy korzystaniu z nich, a zwłaszcza za zabezpieczenie ich przed dostępem osób nie posiadających imiennego upoważnienia
oraz nieuprawnionych do wglądu.

2. Wydruki zawierające dane osobowe, które są przeznaczone do usunięcia, należy zniszczyć w stopniu uniemożliwiającym ich odczytanie.

§ 24.
DANE UŻYTKOWNIKA

System powinien umożliwić udostępnienie na piśmie, w zrozumiałej formie, treści danych o każdej osobie, której dane są przetwarzane, a w szczególności:

a) daty pierwszego wprowadzenia danych tej osoby,
b) źródła pochodzenia danych,
c) nazwy użytkownika wprowadzającego dane,
d) informacji - komu, kiedy i w jakim zakresie dane zostały udostępnione,

e) sprzeciwu, o którym mowa w art. 32 ust. I pkt 7, po jego uwzględnieniu, oraz sprzeciwu określonego w art. 32 ust. 1 pkt 8 ustawy o ochronie danych osobowych.

§ 25.
ODPOWIEDZIALNOŚĆ

Naruszenie obowiązków wynikających z niniejszej Polityki Bezpieczeństwa oraz przepisów ustawy o ochronie danych osobowych może być uznane za ciężkie naruszenie obowiązków pracowniczych, podlegające sankcjom dyscyplinarnym oraz sankcjom karnym w szczególności wynikającym z przepisów tejże ustawy.

§ 26.
OBOWIĄZKI ADMINISTRATORA BEZPIECZEŃSTWA INFORMACJI

Do obowiązków Administratora Bezpieczeństwa Informacji w zakresie ochrony danych osobowych przetwarzanych w systemach informatycznych należy w szczególności:

1) nadzór nad stosowaniem środków ochrony,

2) nadzór nad przestrzeganiem przez Administratora Systemów Informatycznych i użytkowników systemu - procedur bezpieczeństwa,

3) wskazywanie zagrożeń oraz reagowanie na naruszenia ochrony danych osobowych i usuwanie ich skutków,

4) prowadzenie ewidencji użytkowników systemów informatycznych, w których przetwarzane są dane osobowe, która jest j częścią ewidencji osób upoważnionych do przetwarzania danych osobowych oraz wszelkiej dokumentacji opisującej sposób realizacji i zasady ochrony danych osobowych w Urzędzie Miejskim w Krobi.

5) kontrolowanie nadanych w systemach informatycznych uprawnień do przetwarzania danych osobowych pod kątem ich zgodności z wpisami umieszczonymi w ewidencji osób upoważnionych do przetwarzania danych osobowych.

6) prowadzenie szkoleń dla użytkowników w zakresie stosowanych w systemach

informatycznych środków ochrony danych osobowych,

6) uzgadnianie z Administratorem Systemów Informatycznych procedur regulujących

wykonywanie czynności w systemach lub aplikacjach służących do przetwarzania danych osobowych.

§ 27.

OBOWIĄZKI ADMINISTRATORA SYSTEMÓW INFORMATYCZNYCH

Do obowiązków Administratora Systemów Informatycznych w zakresie ochrony danych osobowych przetwarzanych w systemach informatycznych należy w szczególności:

1) realizacja zadań związanych z przeszkoleniem użytkowników w zakresie obsługi sprzętu informatycznego, oprogramowania systemowego oraz oprogramowania do obsługi aplikacji , którą będą wykorzystywali,
2) zapoznanie użytkowników z treścią Instrukcji,
3) operacyjne zarządzanie systemami informatycznymi w sposób zapewniający ochronę

danych osobowych w nich przetwarzanych,

4) przestrzeganie opracowanych dla systemu procedur operacyjnych i bezpieczeństwa,
5) kontrola przepływu informacji pomiędzy systemem informatycznym a siecią publiczną oraz kontrola działań inicjowanych z sieci publicznej a systemem informatycznym,
6) zarządzanie stosowanymi w systemach informatycznym środkami uwierzytelnienia, w

tym rejestrowanie i wyrejestrowywanie użytkowników oraz dokonywanie zmiany

uprawnień ,

7) utrzymanie systemu w należytej sprawności technicznej,
8) regularne tworzenie kopii zapasowych zasobów danych osobowych oraz programów

służących do ich przetwarzania oraz okresowe sprawdzanie poprawności wykonania

kopii zapasowych,

9) Wykonywanie lub nadzór nad wykonywaniem okresowych przeglądów i konserwacji,

zgodnie z odrębnymi procedurami, sprzętu IT, systemów informatycznych, aplikacji

oraz elektronicznych nośników informacji, na których przetwarzane są dane osobowe.

PRZEPISY KOŃCOWE

W sprawach nieuregulowanych w niniejszej Instrukcji mają zastosowanie przepisy ustawy z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (Dz. U. 2014 r. poz. 1182, z późn. zm.) oraz 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 .