POLITYKA BEZPIECZEŃSTWA PRZETWARZANIA DANYCH OSOBOWYCH W URZĘDZIE GMINY KAMPINOS

Zatwierdził (data i podpis):

Wójt Gminy Kampinos

/-/ dr inż. Monika Ciurzyńska

§ 1
Postanowienia ogólne

1. Polityka bezpieczeństwa przetwarzania danych osobowych w Urzędzie Gminy Kampinos, zwana dalej „Polityką", została wydana 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 2004r. Nr 100, poz. 1024).
2. Celem Polityki jest stworzenie podstaw dla właściwego wykonania obowiązków Administratora Danych 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, ochrony i dystrybucji wewnątrz Urzędu Gminy Kampinos.
4. Polityka zawiera informacje dotyczące rozpoznawania procesów przetwarzania danych osobowych oraz wprowadzonych zabezpieczeń technicznych i organizacyjnych, zapewniających ochronę przetwarzanych danych osobowych.
5. **Niniejszą Politykę stosuje się do:**
   1) Danych osobowych:
      a. przetwarzanych w systemach informatycznych,
      b. zapisanych 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 w dokumentach powiązanych powinny być znane i stosowane przez pracowników oraz w niezbędnym zakresie przez współpracowników przetwarzających dane osobowe, których administratorem jest Gmina Kampinos.

§ 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 Administratora Danych, w zakresie ochrony danych osobowych w Urzędzie Gminy Kampinos.

1. **Administrator Danych** – Gmina Kampinos - decyduje o środkach i celach przetwarzania danych osobowych, reprezentowany przez Wójta Gminy Kampinos, wykonującego swoje zadania przy pomocy Urzędu Gminy.
2. **Administrator Bezpieczeństwa Informacji** – osoba wyznaczona przez Administratora Danych, 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** – wyznaczona przez Administratora Danych osoba, odpowiedzialna za funkcjonowanie infrastruktury informatycznej na którą składa się cały sprzęt informatyczny oraz systemów i aplikacji informatycznych, za ich przeglądy, konserwację oraz za stosowanie technicznych i organizacyjnych środków bezpieczeństwa w systemach informatycznych.
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.

5. **Dane Osobowe** – wszelkie informacje dotyczące zidentyfikowanej lub możliwej do zidentyfikowania osoby fizycznej. Osobą możliwą do zidentyfikowania jest osoba, której tożsamość można określić bezpośrednio lub pośrednio, w szczególności przez powołanie się na jeden lub kilka specyficznych czynników ją określających.
6. **GIODO** – Generalny Inspektor Ochrony Danych Osobowych.
7. **System informatyczny –** całokształt rozwiązań sprzętowo-programowych i organizacyjnych stanowiących podstawę wdrożenia i eksploatacji zaawansowanych merytorycznie i technologicznie systemów informatycznych w urzędzie.
8. **Integralność danych** – właściwość zapewniająca, że dane nie zostały zmienione lub zniszczone w sposób nieautoryzowany.
9. **Naruszenie ochrony danych osobowych** – zamierzone lub przypadkowe działanie lub zaniechanie działania, powodujące zagrożenie bezpieczeństwa danych osobowych, przetwarzanych tradycyjnie, jak również z wykorzystaniem systemów informatycznych.
10. **Osoba trzecia** – należy przez to rozumieć, osobę nie będącą pracownikiem, i współpracownikiem Urzędu Gminy Kampinos, dla której nie istnieją podstawy prawne do nadania jej upoważnienia do przetwarzania danych osobowych.
11. **Odbiorca danych** – rozumie się przez to każdego, komu udostępnia się dane osobowe, z wyłączeniem:
    a) osoby, której dane dotyczą,
    b) osoby upoważnionej do przetwarzania danych,
    c) przedstawiciela, o którym mowa w art. 31a Ustawy,
    d) podmiotu, o którym mowa w art. 31 Ustawy,
    e) organów państwowych lub organów samorządu terytorialnego, którym dane są udostępniane w związku z prowadzonym postępowaniem.
12. **Poufność** – właściwość zapewniająca, że informacja (np. dane osobowe) jest dostępna jedynie osobom upoważnionym.
13. **Przetwarzanie danych osobowych** – jakiekolwiek operacje wykonywane na danych osobowych, takie jak zbieranie, utrwalanie, przechowywanie, opracowywanie, zmienianie, udostępnianie i usuwanie, a zwłaszcza te, które wykonuje się w systemach informatycznych.
14. **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. Nr 100, poz. 1024).
15. **Rozliczalność** – właściwość zapewniająca, że działania podmiotu mogą być przypisane w sposób jednoznaczny tylko temu podmiotowi.
16. **System informatyczny** – zespół współpracujących urządzeń, programów, procedur przetwarzania informacji i narzędzi programowych zastosowanych w celu przetwarzania danych.
17. **Urząd** – Urząd Gminy Kampinos.
18. **Ustawa** – Ustawa o ochronie danych osobowych z dnia 29 sierpnia 1997 r. (Dz. U. z 2002 r. Nr 101, poz. 926 z późn. zm.).
19. **Użytkownik systemu** – osoba upoważniona do bezpośredniego dostępu do danych osobowych przetwarzanych w systemie informatycznym, która posiada ustalony identyfikator i hasło.
20. **Współpracownik** – należy przez to rozumieć osobę nie będącą pracownikiem, dla której istnieją podstawy prawne, do nadania jej upoważnienia do przetwarzania danych osobowych.
21. **Właściciel zasobów danych osobowych** – osoba kierująca komórką organizacyjną / osoba na samodzielnym stanowisku - odpowiedzialna za ochronę danych osobowych przetwarzanych w podległej komórce. Jest ona zobowiązana zastosować środki techniczne i organizacyjne zapewniające 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 o ochronie danych osobowych oraz nieautoryzowaną zmianą, utratą, uszkodzeniem lub zniszczeniem.
22. **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. Strukturę zbioru danych osobowych

charakteryzuje istnienie cechy albo cech pozwalających na odnalezienie informacji bez potrzeby przeglądania całego zestawu

23. **Zbiór nieinformatyczny** – każdy zbiór danych osobowych prowadzony poza systemem informatycznym, w szczególności w postaci papierowej - kartoteki, skorowidza, księgi, wykazu lub innego zbioru ewidencyjnego.

§ 3
Deklaracja Administratora Danych

1. Administrator Danych 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.
2. Przy przetwarzaniu danych osobowych w systemach informatycznych Urzędu Gminy Kampinos - należy stosować wysoki poziom bezpieczeństwa w rozumieniu § 6 ust. 4 Rozporządzenia.

§ 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. Przegląd Polityki ma na celu stwierdzenie, czy postanowienia Polityki odpowiadają aktualnej i planowanej działalności Urzędu oraz stanowi prawnemu aktualnemu w momencie dokonywania przeglądu.
3. Fakty wystąpienia poważnych naruszeń ochrony danych osobowych powinny skutkować zmianami w dokumencie niniejszej Polityki i dokumentach powiązanych.
4. Zmiany niniejszej Polityki wymagają przeglądu innych dokumentów obowiązujących w Urzędzie dotyczących ochrony danych osobowych.
5. Wszelkie zmiany Polityki – mające wpływ na poziom ochrony danych osobowych - powinny być zatwierdzane przez Administratora Danych.

§ 5
Zarządzanie ochroną danych osobowych

1. Realizację zamierzeń w celu zwiększenia skuteczności ochrony danych osobowych powinny zagwarantować następujące założenia:
   1) Przeszkolenie pracowników dopuszczonych do przetwarzania danych w zakresie bezpieczeństwa danych osobowych.
   2) Przypisanie użytkownikom określonych atrybutów pozwalających na ich identyfikację w systemach informatycznych (np. hasła, identyfikatory), umożliwiających im dostęp do danych osobowych - stosownie do zakresu upoważnienia i indywidualnych poziomów uprawnień.
   3) Okresowe sprawdzanie przestrzegania przez użytkowników wdrożonych metod postępowania przy przetwarzaniu danych osobowych.
   4) Podejmowanie niezbędnych działań, w celu likwidacji słabych ogniw w systemie ochrony danych osobowych.

5) Śledzenie osiągnięć w dziedzinie bezpieczeństwa fizycznego, bezpieczeństwa systemów informatycznych i - w miarę możliwości organizacyjnych i techniczno-finansowych - wdrażanie nowych narzędzi i metod pracy oraz sposobów zarządzania, służących wzmocnieniu bezpieczeństwa przetwarzanych 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 powinien być zapewniony, że pracownicy oraz współpracownicy:
   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) 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 i rolą sprawowaną w procesie przetwarzania danych.

§ 6
Dokumenty powiązane

1. Instrukcja zarządzania systemem informatycznym służącym do przetwarzania danych osobowych w Urzędzie Gminy Kampinos,

§ 7
Odpowiedzialność Administratora Danych

1. Administrator Danych 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 Ustawy oraz utratą, uszkodzeniem lub zniszczeniem.
2. Do kompetencji Administratora Danych należy w szczególności:
   1) Wyznaczenie Administratora Bezpieczeństwa Informacji.
   2) Wyznaczenie Administratora/ów Systemów Informatycznych.
   3) Określenie Właścicieli zasobów danych osobowych.
   4) Określenie celów i strategii ochrony danych osobowych.
   5) Podział zadań i obowiązków związanych z organizacją ochrony danych osobowych.
3. Do obowiązków Administratora Danych należy:
   1) Zapewnienie poufności, integralności, dostępności i rozliczalności danych przetwarzanych w systemach informatycznych.
   2) Zapewnienie szkoleń dla pracowników w zakresie przepisów o ochronie danych osobowych oraz zagrożeń związanych z ich przetwarzaniem.
   3) Przyjmowanie i zatwierdzanie niezbędnych, wymaganych przez przepisy prawa dokumentów regulujących ochronę danych osobowych w Urzędzie.
   4) Nadawanie pracownikom i współpracownikom Urzędu upoważnień do przetwarzania danych osobowych.
   5) Zapewnienie środków finansowych na ochronę fizyczną pomieszczeń, w których przetwarzane są dane osobowe.
   6) Zapewnienie środków finansowych niezbędnych do ochrony danych osobowych przetwarzanych w systemach informatycznych oraz w zbiorach nieinformatycznych.
   7) Zapewnienie środków finansowych na merytoryczne przygotowanie osób odpowiedzialnych za nadzór nad ochroną danych osobowych.

8) Zapewnienie realizacji obowiązku zgłoszenia i aktualizacji zbiorów danych osobowych do rejestracji GIODO.

§ 8
Odpowiedzialność Administratora Bezpieczeństwa Informacji

1. Administrator Danych wyznacza Administratora Bezpieczeństwa Informacji, który nadzoruje przestrzeganie zasad ochrony danych osobowych zarówno w systemach informatycznych, jak również w zbiorach danych osobowych prowadzonych w postaci 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 Administratora Bezpieczeństwa Informacji należy:
   1) Nadzór nad wdrożeniem stosownych środków organizacyjnych i technicznych w celu ochrony przetwarzanych danych osobowych.
   2) Nadawanie, zmienianie oraz cofanie uprawnień do przetwarzania danych osobowych na wniosek Właścicieli zasobów, po akceptacji Administratora Danych - dla pracowników oraz współpracowników.
   3) Nadzór nad zapewnieniem przez Właścicieli zasobów, 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 prowadzenia dokumentacji, o której mowa w § 6 w zakresie ABI
   5) Zapoznawanie pracowników oraz współpracowników z przepisami i zasadami ochrony danych osobowych oraz informowanie o zagrożeniach związanych z ich przetwarzaniem.
   6) Reprezentowanie Administratora Danych w kontaktach z Biurem GIODO.
   7) Przygotowywanie zgłoszeń zbiorów danych osobowych do rejestracji w Biurze GIODO.
   8) Reagowanie na zgłaszane incydenty (zdarzenia, zajścia lub wypadki nie będące częścią standardowych operacji lub usług, które powodują lub mogą spowodować spadek poziomu ochrony danych osobowych) związane z naruszeniem ochrony danych osobowych oraz analizowanie ich przyczyn i kierowanie wniosków dotyczących ukarania winnych naruszeń.
   9) Sprawdzanie wypełnienia obowiązków technicznych i organizacyjnych związanych z ochroną danych osobowych.
4. Administrator Bezpieczeństwa Informacji w zakresie realizacji swoich obowiązków, ma prawo żądania od pozostałych osób, bez względu na rangę ich stanowiska udzielania natychmiastowej pomocy w razie stwierdzenia, że doszło do naruszenia przepisów o ochronie danych osobowych.
5. Sprawowanie nadzoru nad przestrzeganiem zastosowanych środków technicznych i organizacyjnych zapewniających ochronę przetwarzanym danym osobowym odpowiednią do zagrożeń oraz kategorii danych objętych ochroną, powinno być głównym zadaniem Administratora Bezpieczeństwa Informacji.

§ 9
Odpowiedzialność Administratora Systemów Informatycznych

1. Rolę Administratora Systemów Informatycznych pełni pracownik (lub pracownicy) wyznaczony przez Administratora Danych.
2. Do obowiązków Administratora Systemów Informatycznych należy:
   1) Zabezpieczenie systemów przetwarzania danych osobowych zgłoszonych ASI, w zależności od kategorii przetwarzanych w tym systemie danych.
   2) Bieżący nadzór oraz zapewnianie optymalnej ciągłości działania systemu informatycznego w tym opracowanie procedur określających zarządzanie systemem informatycznym przetwarzającym dane osobowe.
   3) Reagowanie bez zbędnej zwłoki, w przypadku naruszenia bądź powstania zagrożenia bezpieczeństwa danych osobowych.

4) Przeciwdziałanie próbom naruszenia bezpieczeństwa danych osobowych
5) Analizę raportów wszelkich zdarzeń w tym incydentów związanych z bezpieczeństwem systemów przetwarzania danych
6) Zapewnienie zgodności wszystkich wdrażanych systemów przetwarzania danych osobowych z Ustawą oraz z niniejszą Polityką bezpieczeństwa i Instrukcją Zarządzania Systemem Informatycznym w Urzędzie Gminy Kampinos.
7) Instalację i konfigurację oprogramowania i sprzętu typu „stand-alone", sieciowego i serwerowego używanego do przetwarzania danych osobowych.
8) Konfigurację i administrację oprogramowaniem systemowym i sieciowym zabezpieczającym dane osobowe przed nieupoważnionym dostępem.
9) Nadzór nad czynnościami związanymi ze sprawdzaniem systemu pod kątem obecności szkodliwego oprogramowania.
10) Nadzór nad systemem komunikacji w sieci komputerowej oraz przesyłaniem danych za pośrednictwem urządzeń teletransmisji.
11) Nadzór nad naprawami, konserwacją oraz likwidacją urządzeń komputerowych, na których zapisane są dane osobowe.
12) Przyznawanie na wniosek Właściciela zasobów, za zgodą Administratora Danych i zatwierdzanego przez Administratora Bezpieczeństwa Informacji, ściśle określonych praw dostępu do danych osobowych w danym systemie.
13) Świadczenie pomocy technicznej w ramach oprogramowania a także serwis sprzętu komputerowego będącego na stanie Urzędu, służącego do przetwarzania danych osobowych.
14) Diagnozowanie i usuwanie awarii sprzętu komputerowego oraz realizacje umów z firmami świadczącymi usługi pogwarancyjnego sprzętu komputerowego.
15) Wykonywanie i zarządzanie kopiami zapasowymi oprogramowania systemowego (w tym danych osobowych oraz zasobów umożliwiających ich przetwarzanie) i sieciowego.
16) Wykonywanie i przechowywanie dokumentacji o której mowa w § 6 należącej do kompetencji Administratora Systemów Informatycznych.
17) Nadzór nad wdrożeniem i zarządzanie systemami Informatycznymi (przeglądanie, nadawanie i odbieranie uprawnień użytkownikom, itp.), w których przetwarza się dane osobowe.
18) Umożliwienie przeprowadzenia kontroli systemu informatycznego przez służby Biura Generalnego Inspektora Ochrony Danych Osobowych.

§ 10
Odpowiedzialność Właścicieli zasobów danych osobowych.

1. Administrator Danych określa 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 mieć charakter poufny.
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 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, formalnego upoważnienia do przetwarzania danych osobowych.
7) 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. Wszystkie te informacje powinny zostać przekazane do Administratora Bezpieczeństwa Informacji oraz Administratora Systemu Informatycznego.
8) Wnioskowanie do Administratora Danych o nadanie upoważnień dla pracowników podległej komórki organizacyjnej.

§ 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 współpracownika w zakresie ochrony danych osobowych.
2. Pracownicy i współpracownicy są zobowiązani do:
   1) Informowania o wszelkich podejrzeniach naruszenia lub zauważonych naruszeniach oraz słabościach systemu przetwarzającego dane osobowe bezpośrednio do Administratora Bezpieczeństwa Informacji
   2) Postępowania zgodnie z Polityką.
   3) Zachowania w tajemnicy danych osobowych oraz informacji o sposobach ich zabezpieczenia.
   4) Ochrony danych osobowych oraz środków przetwarzających dane osobowe przed nieuprawnionym dostępem, ujawnieniem, modyfikacją, zniszczeniem lub zniekształceniem. Ścisłego przestrzegania zakresu nadanego upoważnienia do przetwarzania danych osobowych
3. Pracownicy i współpracownicy - powinni mieć świadomość możliwości zaistnienia sytuacji naruszenia ochrony danych osobowych. W związku z tym powinni:
   1) Przestrzegać procedur związanych z otwieraniem i zamykaniem pomieszczeń o których mowa w § 14, a także z wejściem do obszarów przetwarzania danych osobowych osób nieupoważnionych.
   2) Informować Administratora Bezpieczeństwa Informacji o podejrzanych osobach.
   3) Pracownicy / współpracownicy powinni na podstawie dokonanej identyfikacji ewentualnych zagrożeń, przedkładać Administratorowi Bezpieczeństwa Informacji projekty i propozycje nowych rozwiązań, których celem jest zwiększenie poziomu ochrony danych osobowych.

§ 12
Szkolenia w zakresie ochrony danych osobowych

1. Przed rozpoczęciem przetwarzania danych osobowych pracownik powinien zostać przeszkolony przez Administratora Bezpieczeństwa Informacji. Szkolenie powinno obejmować następujące zagadnienia:
   1) Przepisy o ochronie danych osobowych.
   2) Zasady bezpiecznego użytkowania urządzeń i systemów informatycznych służących do przetwarzania danych osobowych.
   3) Zagrożenia na jakie może być narażone przetwarzanie danych osobowych, a w szczególności te związane z przetwarzaniem danych osobowych w systemach informatycznych.
   4) Zasady dostępu do pomieszczeń, w których przetwarzane są dane osobowe.
   5) Prawa osób, których dane osobowe dotyczą.

6) Sposób postępowania w przypadku naruszenia ochrony danych osobowych lub systemu informatycznego.
7) Odpowiedzialność z tytułu naruszenia ochrony danych osobowych.

2. Szkolenia powinny być powtarzane okresowo lub na żądanie, gdy zaistnieje taka potrzeba. Użytkownicy reprezentujący osoby trzecie (tam, gdzie jest to wskazane) powinni przechodzić przeszkolenie w zakresie:
   1) Odpowiednich zasad wynikających z Polityki.
   2) Odpowiednich procedur dotyczących bezpieczeństwa systemów informatycznych służących do przetwarzania danych osobowych.
   3) Poprawnego użytkowania urządzeń i systemów informatycznych służących do przetwarzania danych osobowych.

§ 13
Wymiana informacji dotyczących danych osobowych

1. Pracownicy i współpracownicy 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 i zniszczeniem.
   3) Zabezpieczenia i ograniczenia związane z możliwościami przekazywania wiadomości za pomocą środków komunikacji, np. automatyczne przekazywania poczty elektronicznej na zewnątrz.
   4) Zakaz pozostawiania informacji zawierających dane osobowe przy urządzeniach drukujących, np. 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 osobowych.
   6) Zachowania szczególnej ostrożności w trakcie rozmów telefonicznych, unikając podsłuchania danych osobowych przez osoby nieupoważnione.
   7) Nie pozostawianie wiadomości zawierających dane osobowe w automatycznych sekretarkach.
   8) Właściwe postępowanie z faksami i fotokopiarkami, ponieważ mają one podręczną pamięć i przechowują w niej strony zawierające np. dane osobowe na wypadek błędów transmisji.
2. Transport danych osobowych w postaci elektronicznej i papierowej pomiędzy obszarami, w których są przetwarzane dane osobowe powinien być prowadzony przez osoby upoważnione w sposób ograniczający możliwość ich pozyskanie i odczyt przez osoby nieupoważnione.

§ 14
Przetwarzanie danych osobowych w obszarach bezpiecznych

1. Dane osobowe w Urzędzie mogą być przetwarzane wyłącznie w pomieszczeniach przetwarzania danych osobowych.
2. Na pomieszczenia przetwarzania danych osobowych składają się pomieszczenia biurowe oraz części pomieszczeń, gdzie Administrator Danych 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 do przetwarzania tych danych lub za zgodą Właściciela zasobów danych osobowych.
5. Budynki lub pomieszczenia, w których przetwarzane są dane osobowe, powinny być zamykane podczas nieobecności osób upoważnionych do przetwarzania danych osobowych, w sposób ograniczający możliwość dostęp 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, np. alarmów, zamków itp.
   4) Zamykanie drzwi i okien w pomieszczeniach pozostawianych bez dozoru oraz należy rozważyć zastosowanie mechanizmów zewnętrznej ochrony dla okien, szczególnie tych położonych na poziomie gruntu.
   5) System wykrywania włamań zgodnych z normami w strefach bezpieczeństwa oraz regularne jego testowanie.
7. Obszary bezpieczne powinny być odpowiednio zabezpieczone przed skutkami pożaru.
8. Ochrona obszarów bezpiecznych powinna być zapewniona poprzez odpowiednie fizyczne zabezpieczenia wejścia zapewniające, że tylko 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 ograniczenie dostępu do obszarów, gdzie są przetwarzane dane osobowe tylko dla uprawnionego personelu.
   3) Regularne przeglądanie praw dostępu do obszarów bezpiecznych i jeśli zachodzi potrzeba, uaktualnianie ich lub odbieranie.
9. Przetwarzanie danych osobowych jest zakazane w tych pomieszczeniach, w których osoby trzecie wykonują prace techniczne.
10. Nośniki elektroniczne zawierające dane osobowe powinny być ewidencjonowane i należy przechowywać w zamykanych szafach, które znajdują się w obszarach przetwarzania danych osobowych.
11. Każdorazowe naruszenie zasad ochrony danych osobowych dane osobowe powinno być zgłaszane do Administratora Bezpieczeństwa Informacji.

§ 15
Dopuszczenie osób do przetwarzania danych osobowych

1 Pracownik i współpracownik mają prawo przetwarzać dane osobowe wyłącznie po uzyskaniu formalnego upoważnienia do przetwarzania danych osobowych, zaakceptowanego przez Administratora Danych Osobowych i wystawianego przez Administratora Bezpieczeństwa Informacji. W tym celu Właściciel zasobu danych osobowych przed dopuszczeniem do przetwarzania danych osobowych przez osoby, o których mowa powyżej:
   1) Zapoznaje pracownika / współpracownika z przepisami dotyczącymi ochrony danych osobowych oraz uregulowaniami wewnętrznymi obowiązującymi w tym zakresie w Urzędzie.
   2) Przyjmuje od pracownika / współpracownika podpisane oświadczenie o zachowaniu danych osobowych i sposobów ich zabezpieczania w tajemnicy, przetwarzania danych osobowych zgodnie z przepisami oraz oświadczenia o znajomości niniejszego dokumentu a także o znajomości „Instrukcji zarządzania systemem informatycznym służącym do przetwarzania danych osobowych”

3) Wnioskuje do Administratora Danych o formalne upoważnienie pracownika / współpracownika, do przetwarzania danych osobowych.
4) Oświadczenia i upoważnienia, o których mowa w ust. 1 przechowuje się w aktach osobowych pracownika / współpracownika lub innym stosownym miejscu oznaczonym przez Administratora Danych.

3. Właściciel zasobu danych osobowych - jest zobowiązany niezwłocznie po ustaniu potrzeby przetwarzania danych osobowych przez pracownika / współpracownika złożyć rezygnację do Administratora Bezpieczeństwa Informacji dotyczącą jego dostępu do danych osobowych.

§ 16
Ewidencja osób upoważnionych do przetwarzania danych osobowych

1. Osoby upoważnione do przetwarzania danych osobowych powinny być wpisywane do ewidencji. Ewidencja osób upoważnionych do przetwarzania danych osobowych **–** prowadzona jest przez Administratora Bezpieczeństwa Informacji.
2. Jakakolwiek zmiana w zakresie informacji zawartych w ewidencji powinna podlegać natychmiastowemu odnotowaniu.
3. Właściciele zasobów danych osobowych, przełożeni pracowników i współpracowników odpowiadają za natychmiastowe zgłoszenie do Administratora Bezpieczeństwa Informacji osób, które utraciły uprawnienia dostępu do danych osobowych.
4. Administrator Bezpieczeństwa Informacji w oparciu o informacje, o których mowa w ust. 3 powinien podjąć działania, których celem jest uniemożliwienie tym osobom dostępu do danych osobowych i wyrejestrować z ewidencji, o której mowa w ust. 1.
5. Elektroniczne nośniki informacji, na których gromadzone są wykazy zawierające ewidencję osób upoważnionych do przetwarzania danych osobowych powinny być przechowywane w szafie zamykanej, do której ma dostęp Administrator Bezpieczeństwa Informacji lub osoba przez niego upoważniona.

§ 17
Dostęp zdalny

1. Zastosowane przez Administratora Danych rozwiązania techniczne umożliwiające dostęp zdalny do danych osobowych powinny zapewniać integralność, poufność i rozliczalność przetwarzanych danych osobowych oraz ochronę kryptograficzną wobec danych służących do uwierzytelnia a przesyłanych publicznymi łączami telekomunikacyjnymi.
2. Nadawanie uprawnień w celu dostępu zdalnego do systemów informatycznych przetwarzających dane osobowe realizowane jest przez Administratora Systemów Informatycznych, po spełnieniu wymagań określonych w ust. 1 oraz po uzyskaniu akceptacji Administratora Danych.
3. Dostęp do systemów informatycznych dla współpracowników powinien być monitorowany pod kątem bezpieczeństwa przez Administratora Systemów Informatycznych w celu zapewnienia poufności, rozliczalności i integralności danych osobowych.

§ 18
Rejestracja zbiorów danych osobowych

1. Właściciele zasobów danych osobowych są zobowiązani, do zgłaszania Administratorowi Bezpieczeństwa Informacji zamiaru utworzenia nowego zbioru danych osobowych wraz z wskazaniem podstawy przetwarzania danych, uzasadnieniem celowości, zakresu i sposobu zbierania danych osobowych.
2. Administratora Bezpieczeństwa Informacji weryfikuje wniosek o utworzenie nowego zbioru danych osobowych oraz analizuje nowy zbiór danych pod kątem obowiązku zgłoszenia zasobu, jako zbioru danych do rejestracji w GIODO.
3. W sytuacji, jeżeli 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.

4. Administrator Bezpieczeństwa Informacji sprawdza opisane zgłoszeniu rejestracyjnym warunki techniczne o organizacyjne dotyczące zabezpieczeń w systemie informatycznym, a w przypadku niewystarczającego poziomu zabezpieczeń występuje z wnioskiem do Administratora Danych o podniesienie poziomu tych zabezpieczeń.
5. Sprawdzony przez Administratora Bezpieczeństwa Informacji projekt zgłoszenia zbioru danych osobowych do rejestracji w GIODO jest przedstawiany Administratorowi Danych Osobowych do podpisu.
6. Administrator Bezpieczeństwa Informacji – po akceptacji Administratora Danych Osobowych - zgłasza wniosek o rejestrację zbioru danych osobowych do GIODO i wyznacza Właściciela zasobów danych osobowych dla zarejestrowanego zbioru danych osobowych.
7. Administrator Bezpieczeństwa Informacji uzupełnia Politykę, dokumenty z nią powiązane oraz pozostałe dokumenty obowiązujące w Urzędzie w zakresie ochrony danych osobowych informacje na temat nowego zbioru.

§ 19
Udostępnianie danych osobowych

1. 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 powinny być wystosowane z zachowaniem formy pisemnej
2. Udostępniając dane osobowe należy zaznaczyć, że można je wykorzystać wyłącznie zgodnie z przeznaczeniem, dla którego zostały udostępnione.
3. Na pisemny wniosek pochodzący od osoby, której dane dotyczą, informacje o osobie powinny być udzielone w terminie 30 dni od daty złożenia wniosku.
4. Za przygotowanie danych osobowych do udostępnienia w zakresie wskazanym we wniosku jest odpowiedzialny Właściciel zasobów danych osobowych.
5. Odpowiedź na wniosek o udostępnienie danych osobowych przed wysłaniem jest akceptowana i parafowana przez Właściciela zasobów danych osobowych oraz Administratora Bezpieczeństwa Informacji a następnie podpisywana przez Administratora Danych.
6. W przypadku odpowiedzi na wniosek, o którym mowa w ust. 2, nie od osoby, której dane dotyczą, Właściciel zasobów danych osobowych przekazuje kopię odpowiedzi do Administratora Bezpieczeństwa Informacji.
7. 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 § 13 niniejszej Polityki.
   3) Innym bezpiecznym, określonym wymogiem prawnym lub umową.
8. Informacja o udostępnieniu danych osobowych podlega odnotowaniu jeśli dane osobowe udostępniane są ze zbioru danych osobowych. W takim przypadku, odnotowaniu podlega informacja o zakresie danych podlegających udostępnieniu, dacie udostępnienia odbiorcy, celu udostępnienia oraz danych osób, które ze strony Administratora Danych udostępniły dane osobowe. Nie dotyczy to sytuacji, gdy przepisy prawa zezwalają na zbieranie danych osobowych bez konieczności ujawniania adresata danych.

§ 20
Powierzanie przetwarzania danych osobowych

1. Powierzenie przetwarzania danych osobowych występuje wówczas, gdy podmioty zewnętrzne współpracujące z Urzędem Gminy Kampinos, mają dostęp do danych osobowych przetwarzanych przez Urząd.
2. Wskazane w ust. 1 powierzenie przetwarzania danych osobowych może się odbywać wyłącznie w trybie przewidzianym w art. 31 Ustawy poprzez zawarcie na piśmie umowy powierzenia przetwarzania danych osobowych, pomiędzy Administratorem Danych - 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 przetwarzania danych osobowych.
   2) Obowiązek zachowania w 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 bezterminowy.
   3) Wymagane działania w momencie zakończenia umowy.
   4) Odpowiedzialność i działania sygnatariuszy podejmowane w celu uniknięcia nieupoważnionego ujawnienia informacji.
   5) Własność informacji.
   6) Dozwolone użycie danych osobowych oraz praw sygnatariusza do jej użycia.
   7) Prawa do audytu i monitorowania działań związanych z ochroną danych osobowych.
   8) Proces powiadamiania i raportowania nieuprawnionego ujawnienia lub naruszenia poufności i integralności danych osobowych.
   9) Zasady zwrotu lub niszczenia danych osobowych przy zakończeniu umowy.
   10) Działania podejmowane w przypadku naruszenia warunków umowy..
5. Projekt umowy powierzenia przetwarzania danych osobowych innemu podmiotowi przygotowuje zespół powołany przez Administratora Bezpieczeństwa Informacji.
6. Powierzenie przetwarzania danych osobowych poza granice Rzeczpospolitej Polskiej wymaga zgody Administratora Danych i odbywa się po sprawdzeniu wymagań prawnych obowiązujących w tym zakresie.

§ 21
Postępowanie w przypadku naruszenia ochrony danych osobowych

1. Poniższe postanowienia mają zastosowanie zarówno w przypadku naruszenia lub podejrzenia naruszenia ochrony danych osobowych przetwarzanych w systemach informatycznych, jak i w zbiorach nieinformatycznych.
2. Przed przystąpieniem do pracy pracownicy / współpracownicy zobowiązani są dokonać sprawdzenia stanu urządzeń informatycznych oraz oględzin swojego stanowiska pracy, w tym zwrócić szczególną uwagę, czy nie zaszły okoliczności wskazujące na naruszenie lub próby naruszenia ochrony danych osobowych.
3. Za okoliczności, które uznaje się 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 i systemu.
   3) Niezamierzoną zmianę lub utratę danych zapisanych na kopiach zapasowych.
   4) Nieuprawniony dostęp do danych osobowych (sygnał o nielegalnym logowaniu lub inny objaw wskazujący na próbę lub działanie związane z nielegalnym dostępem do systemu).
   5) Udostępnienie osobom nieupoważnionym danych osobowych lub ich części.
   6) Inny stan systemu informatycznego lub pomieszczeń, niż pozostawiony przez użytkownika po zakończeniu pracy.
   7) Wydarzenia losowe, obniżające poziom ochrony systemu (np. brak zasilania lub pożar).

   8) Kradzież sprzętu informatycznego lub nośników zewnętrznych zawierających dane osobowe (np. wydruków komputerowych, dyskietek, płyt CD-ROM, dysków twardych, pamięci zewnętrznych, itp.).
4. W przypadku stwierdzenia naruszenia lub zaistnienia okoliczności wskazujących na naruszenia ochrony danych osobowych pracownicy zobowiązani są do bezzwłocznego powiadomienia o tym fakcie Administratora Bezpieczeństwa Informacji.
5. Do czasu przybycia Administratora Bezpieczeństwa Informacji, 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 kartotek, przede wszystkim poprzez uniemożliwienie dostępu do nich osobom nieupoważnionym.
   3) Podejmuje, stosownie do zaistniałej sytuacji, wszelkie niezbędne działania celem zapobieżenia dalszym zagrożeniom, które mogą skutkować utratą danych osobowych.
   4) Wykonuje polecenia Administratora Bezpieczeństwa Informacji.
6. W przypadku stwierdzenia naruszenia lub zaistnienia okoliczności wskazujących na naruszenia ochrony danych osobowych Administrator Bezpieczeństwa Informacji, 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 decyzje o toku dalszego postępowania, stosownie do zakresu naruszenia lub zasadności podejrzenia naruszenia ochrony danych osobowych.
7. Administrator Bezpieczeństwa Informacji sporządza raport z przebiegu zdarzenia.
8. W przypadku stwierdzenia naruszenia lub zaistnienia okoliczności wskazujących na naruszenia ochrony danych osobowych, użytkownik może kontynuować pracę dopiero po otrzymaniu pozwolenia od Administratora Bezpieczeństwa Informacji.
9. W przypadku, gdy naruszenie ochrony danych osobowych jest wynikiem uchybienia obowiązującej w Urzędzie dyscypliny pracy, Administrator Bezpieczeństwa Informacji wyjaśnia wszystkie okoliczności incydentu i podejmuje stosowne działania wobec osób, które dopuściły się wskazanego naruszenia.
10. Po zakończeniu czynności naprawczych system powinien utrzymać poziom ochrony nie niższy niż przed wystąpieniem incydentu związanego z naruszeniem ochrony danych osobowych.

§ 22
Wykaz zbiorów danych osobowych

1. Gmina Kampinos - reprezentowana przez Wójta, wykonującego swoje zadania przy pomocy Urzędu Gminy - jest Administratorem danych osobowych wymienionych ,,Ewidencji zbiorów danych osobowych", prowadzonej przez Administratora Bezpieczeństwa Informacji
2. Dane osobowe gromadzone we wskazanych zbiorach są przetwarzane w systemach informatycznych oraz w kartotekach ewidencyjnych, które są zlokalizowane w pomieszczeniach lub części pomieszczeń przetwarzania danych osobowych.
3. Administrator Systemów Informatycznych w oparciu o informacje uzyskane od Właścicieli zasobów danych osobowych, prowadzi - Ewidencję stosowanych systemów i programów (w tym licencji oprogramowania), zastosowanych do przetwarzania danych osobowych.

§ 23
Opis struktury zbiorów danych osobowych

1. Opis struktury zbiorów danych osobowych przetwarzanych w systemach informatycznych, prowadzi Administrator Systemów informatycznych.
2. Zakresy danych osobowych przetwarzanych w poszczególnych zbiorach danych osobowych w systemach informatycznych, są ustalone w oparciu o strukturę zbiorów danych osobowych prowadzonych w tych systemach oraz powiązania pól informacyjnych. Administrator Systemów Informatycznych wykonuje, na podstawie aplikacji zastosowanych do przetwarzania danych

osobowych opisy struktur zbiorów danych wskazujące zawartość poszczególnych pól informacyjnych i powiązania pomiędzy nimi.

3. Opisy wykonywane są w postaci wydruków zrzutów ekranowych lub struktur tablic bazy prezentujących zawartość pól informacyjnych i powiązań pomiędzy nimi. W przypadku braku możliwości uzyskania wydruku zrzutu ekranowego Administrator Systemów Informatycznych, sporządza inne dostępne opisy struktury zbioru.
4. Administrator Systemów Informatycznych zobowiązany jest do prowadzenia i przechowywania opisów struktur zbiorów danych oraz natychmiastowego uaktualniania w przypadku zmian.

§ 24
Sposób przepływu danych pomiędzy poszczególnymi systemami

1. Administrator Systemów Informatycznych, prowadzi dokumentację systemów informatycznych zawierającą opis współpracy pomiędzy różnymi systemami informatycznymi oraz sposób przepływu danych pomiędzy systemami, w których te dane są przetwarzane.
2. Schematy przepływu danych pomiędzy systemami informatycznymi, zastosowanymi w celu przetwarzania danych osobowych, wykonuje Administrator Systemów Informatycznych, zgodnie z relacjami występującymi w programach służących do przetwarzania danych osobowych.
3. Administrator Systemów Informatycznych zobowiązany jest do prowadzenia i przechowywania schematów oraz natychmiastowego ich uaktualniania w przypadku zmian.

§ 25
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 uprawnione osoby.
3. Na czas nie użytkowania, dokumenty i wydruki zawierające dane osobowe powinny być zamykane w szafach biurowych lub zamykanych 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.
5. Dla udokumentowania czynności dokonywanych w celu likwidacji zbiorów archiwalnych, powinny być stosowane odpowiednie przepisy dot. zasad archiwizacji i brakowania dokumentacji Urzędu.

§ 26
Sankcje za naruszenie zasad ochrony danych osobowych

1. Naruszenie zasad ochrony danych osobowych przez pracownika / współpracownika może skutkować postawieniem mu zarzutu popełnienia, jednego z przestępstw określonych w Rozdziale 8 Ustawy lub przestępstwa określonego w art. 266 Kodeksu Karnego.
2. Zgodnie z art. 100 § 2 pkt 5 Kodeksu Pracy, pracownik jest obowiązany przestrzegać tajemnicy określonej w odrębnych przepisach. Dane osobowe, którym Urząd Gminy Kampinos i 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.
3. Pracownik dopuszczający się nieuprawnionego ujawnienia lub wykorzystania danych osobowych w sposób sprzecznych z ich przeznaczeniem (np. wykorzystania danych osobowych do celów prywatnych), czy też ich przetwarzania w sposób niezgodny z przyjętymi w Urzędzie procedurami, może zostać ukarany karą upomnienia lub karą nagany.
4. W razie ciężkiego naruszenia obowiązku zachowania danych osobowych w tajemnicy lub przetwarzania ich w sposób rażąco sprzeczny z przyjętymi zasadami i procedurami, Administrator Danych może rozwiązać bez wypowiedzenia umowę o pracę z winy pracownika.

5. Sankcje dotyczące ujawnienia poufnych danych osobowych, stosuje się analogicznie do ujawnienia przez pracownika informacji dotyczących zabezpieczenia danych osobowych w Urzędzie.

§ 27
Postanowienia końcowe

1. Niezależnie od odpowiedzialności określonej w przepisach prawa powszechnie obowiązującego, naruszenie zasad określonych w niniejszej Polityce może być podstawą rozwiązania stosunku pracy bez wypowiedzenia z osobą, która dopuściła się naruszenia.
2. W sprawach nieuregulowanych w Polityce mają zastosowanie przepisy ustawy z dnia 29 sierpnia 1997 r., o ochronie danych osobowych (t.j. Dz. U. z 2002 r., Nr 101, poz. 926 z późn. zm.) oraz przepisy wykonawcze do tej Ustawy.

Zał. Nr 1 – Ewidencja osób upoważnionych przez Administratora Danych do przetwarzania danych osobowych - wzór

Lp.	Imię i nazwisko	Identyfikator użytkownika	Zakres przydzielonych uprawnień	Data przyznania uprawnień	Podpis Administratora Bezpieczeństwa Informacji	Data odebrania uprawnień	Podpis Administratora Bezpieczeństwa Informacji
1							
2							
3							
4							
5							
6							
7							
8							
9							
10							
11							
12							
13							
14							
15							
16							
17							
18							
19							
20							

Zał. Nr 2 – Ewidencja zbiorów danych osobowych ze wskazaniem programów zastosowanych do ich przetwarzania

Lp.	Referaty i samodzielne stanowiska	Nazwa zbioru danych osobowych	Nazwa programu zastosowanego do przetwarzania danych
1.	Referat ds. środowiska, gospodarki gruntami	- system ewidencji gruntów i budynków - numeracja porządkowa i adresowa - ewidencja mienia komunalnego	- Pakiet biurowy MS Office - Mienie Komunalne
2.	Samodzielne stanowisko ds. obsługi Rady Gminy	- dane osobowe radnych i Sołtysów	Pakiet biurowy MS Office
3.	Referat Finansowy	- dane finansowo – księgowe - dane przetwarzane w związku z zatrudnieniem, świadczeniem usług na podstawie umów cywilnoprawnych - zbiór danych osobowych w związku z opłatami za gospodarowanie odpadami. - zbiór danych podatkowych 0osób fizycznych i prawnych	Płatnik GOMIG AUTA JGU Kszob Płace Pakiet biurowy MS Office
4.	Referat organizacyjno - administracyjny	- dane przetwarzane w związku z zatrudnieniem, świadczeniem usług na podstawie umów cywilnoprawnych - oświadczenia majątkowe - dane zgromadzone w zbiorach danych osobowych	Pakiet biurowy MS Office Płace
5.	Kierownik Urzędu Stanu Cywilnego	- ewidencja ludności - dowody osobiste - rejestr wyborców - urząd stanu cywilnego	Selwin
6.	Samodzielne stanowisko ds. inwestycji	- system ewidencji gruntów i budynków	Pakiet biurowy MS Office

Zał. Nr 3 – Wyznaczenie Administratora Bezpieczeństwa Informacji

WYZNACZENIE
ADMINISTRATORA BEZPIECZEŃSTWA INFORMACJI

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

(tekst jednolity: Dz. U. 2002 r. Nr 101 poz. 926, ze zm.) z dniem ……..2013 r.

wyznaczam:

Panią

……

……

na ADMINISTRATORA BEZPIECZEŃSTWA INFORMACJI.

Zakres zadań, upoważnień i odpowiedzialności Administratora Bezpieczeństwa Informacji określa załącznik.

.....

data i podpis Administratora Danych

Zał. Nr 4 - Oświadczenie

……..……..
(data)

Oświadczenie

Oświadczam, że zapoznała(e)m się, rozumiem i będę przestrzegać obowiązków wynikających z przepisów ustawy z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (t.j. Dz. U. z 2002 r. Nr 101, poz. 926 z późn. zm.), aktów wykonawczych wydanych na jej podstawie oraz dokumentów przyjętych przez Urząd Gminy Kampinos w związku z przetwarzaniem danych osobowych, a w szczególności:

- Polityki bezpieczeństwa przetwarzania danych osobowych w Urzędzie Gminy Kampinos;
- Instrukcji zarządzania systemem informatycznym służącym do przetwarzania danych osobowych w Urzędzie Gminy Kampinos.

Zobowiązuję się do podejmowania działań zmierzających do zapewnienia bezpieczeństwa przetwarzania danych osobowych poprzez ich ochronę przed niepowołanym dostępem, nieuzasadnioną modyfikacją lub zniszczeniem, nielegalnym ujawnieniem lub pozyskaniem oraz unikaniem tych zachowań, które mogłyby poziom bezpieczeństwa danych osobowych obniżyć.

Zobowiązuję się do zachowania w tajemnicy danych osobowych oraz sposobów ich zabezpieczenia, do których uzyskam dostęp w trakcie zatrudnienia, również po ustaniu zatrudnienia.

Jednocześnie przyjmuje do wiadomości, że za niedopełnienie obowiązków wynikających z niniejszego oświadczenia ponoszę odpowiedzialność na podstawie przepisów Regulaminu pracy, Kodeksu pracy oraz Ustawy o ochronie danych osobowych.

.....
Imię i nazwisko pracownika / współpracownika

.....
(podpis Administratora Danych)

Potwierdzam odbiór 1 egz. oświadczenia: .....

(data i podpis pracownika / współpracownika)

Zał. Nr 5 – Upoważnienie do przetwarzania danych osobowych.

....., dnia …….....

U P O W A Ż N I E N I E NR Nr ……/……..

Na podstawie art. 37 ustawy z dnia 29 sierpnia 1997 r. o ochronie danych osobowych
(Dz. U. z 2002 r., Nr 101, poz. 926 – tekst jednolity ze zm.)

u p o w a ż n i a m

Pana /Panią ……..
zatrudnionego /zatrudnioną w Urzędzie Gminy Kampinos
na stanowisku .....

do przetwarzania danych osobowych w zakresie wynikającym z przydzielonych obowiązków pracowniczych oraz do obsługi systemu informatycznego oraz urządzeń wchodzących w jego skład, służących do przetwarzania danych osobowych.
Upoważnienie obejmuje prawo wglądu, wprowadzania, modyfikowania i usuwania danych osobowych.

Upoważnienie wydaje się na czas zatrudnienia w Urzędzie Gminy Kampinos.

Jest Pan/Pani* upoważniony/upoważniona* do przetwarzania danych osobowych wyłącznie w zakresie wynikającym z Pana/Pani* zadań służbowych oraz poleceń przełożonego.

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

……

(podpis Administratora Danych)

…….....……

(data i podpis pracownika / współpracownika)

Zał. Nr 6 – Wykaz budynków, pomieszczeń lub części pomieszczeń, tworzących obszar, w którym przetwarzane są dane osobowe.

Lp.	Budynek – dane adresowe	Pomieszczenie
1	Budynek Urzędu Gminy w Kampinosie	Pokój nr 2, 2A, 4, 5, 5A, 6, 7, 8, 10, 11,12,13

Zał. Nr 7 – Opis struktury zbiorów danych wskazujący zawartość poszczególnych pól informacyjnych i powiązania między nimi.

„Zgodnie z wymaganiami § 4 pkt 3 rozporządzenia MSWiA z dnia 29 kwietnia 2004 r. dla każdego zidentyfikowanego zbioru danych powinien być wskazany opis jego struktury i zakres informacji w nim gromadzonych.
Opisy poszczególnych pól informacyjnych w strukturze zbioru danych powinny jednoznacznie wskazywać, jakie kategorie danych są w nich przechowywane.
Opis pola danych, gdy możliwa jest niejednoznaczna interpretacja jego zawartości, powinien wskazywać nie tylko kategorię danych, ale również format jej zapisu i/lub określone w danym kontekście znaczenie.
Przykład:

- Imię i nazwisko,
- PESEL,
- Adres (Kod terytorialny, miejscowość, kod pocztowy, ulica, nr domu, nr lokalu),
- Dane meldunkowe (rodzaj zameldowania, data zameldowania, data wymeldowania),
- Płeć,
- Nazwisko rodowe,
- Dane ojca i matki (imię, nazwisko, nazwisko rodowe),
- Dane o urodzeniu (data, miejsce, numer aktu urodzenia),
- Stan cywilny (data zmiany, organ, dane małżonka, forma ustania małżeństwa),
- Dokument tożsamości (rodzaj, seria i numer, data wystawienia i ważności, organ wydający),
- Obowiązek wojskowy (seria i numer dokumentu, stopień wojskowy, kategoria przydatności do służby wojskowej),
- Obywatelstwo obce,
- Zgon (data zgonu, numer aktu zgonu),
- Uprawnienia wyborcze,
- Wykształcenie.

Jeżeli w zbiorze występuje kila zakresów danych i/lub występują relacje pomiędzy nimi, należy opisać te powiązania.
Wymóg wskazania powiązań pomiędzy polami informacyjnymi w strukturze zbiorów danych, należy rozumieć jako wymóg wskazania wszystkich tych danych znajdujących się w strukturze zbioru, które poprzez występujące relacje można skojarzyć z określoną osobą.
Przykład:
Ze struktury zbioru może wynikać, że do danych, które można skojarzyć z osobą o podanym imieniu i nazwisku, należą nie tylko dane zawarte w jednym z zakresów danych, ale również dane znajdujące się w innym obiekcie. Połączenie to, zgodnie z definicją danych osobowych, powoduje poszerzenie zakresu danych osobowych o dane zawarte w innym obiekcie.
Należy w niniejszym opisie wskazać poszczególne grupy informacji oraz istniejące między nimi relacje — identyfikując w ten sposób pełny zakres danych osobowych, jakie przetwarzane są w określonym zbiorze.
Przy opisie struktury zbiorów danych nie jest konieczne przedstawianie pełnej dokumentacji struktury bazy danych z wyszczególnieniem oryginalnych nazw poszczególnych pól informacyjnych, stosowanych kluczy czy też definicji wbudowanych obiektów funkcyjnych takich jak: procedury, funkcje, pakiety i wyzwalacze.
Opis może być przedstawiony w postaci formalnej (tabele, pola), w postaci graficznej pokazującej istniejące powiązania pomiędzy obiektami lub w formie opisu tekstowego.”

Zał. Nr 7 – Opis sposobu przepływu danych pomiędzy poszczególnymi systemami. Należy uzupełnić Politykę o w/w informacje.

Pliki typu dokumenty oraz poczta e-mail jest przechowywana na lokalnych stanowiskach, na których są edytowane przez użytkowników, zabezpieczone aktualnym oprogramowaniem antywirusowym oraz posiadające aktualne oprogramowanie Windows. Programy księgowe, płacowe, podatkowe korzystają z bazy SQL umieszczonej na serwerze. Inne systemy wymiany danych oparte są o pracę w przeglądarkach internetowych po zalogowaniu przy użyciu loginu i hasła zgodnego z obecnymi wymogami min. 8 znaków małe i duże litery oraz znaki specjalne. Dane w postaci dokumentów edytowanych edytorem tekstu oraz arkuszem kalkulacyjnym są przenoszone w szczególnych przypadkach za pomocą pendrive.