Burmistrz Zalewa

ZARZĄDZENIE NR 120-7/2012
Burmistrza Zalewa
z dnia 24 lutego 2012 r.

w sprawie: realizacji zasad bezpieczeństwa i ochrony danych osobowych przetwarzanych w Urzędzie Miejskim w Zalewie

Na podstawie art.31 i art.33 ust. 3 ustawy z dnia 8 marca 1990 r. o samorządzie gminnym (Dz. U. z 2001 r. Nr 142, poz. 1591 z późn. zm.) oraz art. 36 ustawy z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (Dz. U. z 2002 r. Nr 101, poz. 926 z późn. zm.) i § 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. Nr 100, poz.1024) zarządza się, co następuje:

§ 1.

1. Wprowadza się do użytku służbowego „Politykę bezpieczeństwa przetwarzania i ochrony danych osobowych w Urzędzie Miejskim w Zalewie" w brzmieniu stanowiącym załącznik nr 1 do zarządzenia.

§ 2.

1. Wykonanie zarządzenia powierza się Administratorowi Bezpieczeństwa Informacji.

§ 3.

Zarządzenie wchodzi w życie z dniem podpisania.

BURMISTRZ
Marek Żyliński

Załącznik Nr 1
do Zarządzenia Nr 120-7/2012
Burmistrza Zalewa
z dnia 24 lutego 2012 r.

„Polityki bezpieczeństwa przetwarzania i ochrony danych osobowych w Urzędzie Miejskim w Zalewie"

§ 1

Postanowienia ogólne

1. Polityka bezpieczeństwa przetwarzania i ochrony danych osobowych w Urzędzie Miejskim w Zalewie 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 w Urzędzie.
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 Miejskiego w Zalewie.
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 (w formie papierowej).
   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 Burmistrz Zalewa.

§ 2

Definicje

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

1. **Administrator Danych Osobowych (ADO)** – podmiot który decyduje o środkach i celach przetwarzania danych osobowych, reprezentowany przez Burmistrza Zalewa.
2. **Administrator Bezpieczeństwa Informacji (ABI)** – osoba wyznaczona przez Burmistrza Zalewa odpowiedzialna za nadzorowanie stosowania środków technicznych i organizacyjnych zapewniających ochronę przetwarzanych danych osobowych, w tym w szczególności za przeciwdziałanie dostępowi osób trzecich do systemu, w którym przetwarzane są dane osobowe oraz za podejmowanie odpowiednich działań w przypadku wykrycia naruszeń w systemie ochrony danych osobowych.

3. **Administrator Systemów Informatycznych (ASI)** – wyznaczona przez ADO 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 i niezawodność.
5. **Dane Osobowe** - każda informacja dotycząca żyjącej osoby fizycznej, która pozwala na bezpośrednią lub pośrednią identyfikację tej osoby.
6. **GIODO** – Generalny Inspektor Ochrony Danych Osobowych.
7. **Integralność danych** – właściwość zapewniająca, że dane nie zostały zmienione lub zniszczone w sposób nieautoryzowany.
8. **Naruszenie ochrony danych osobowych** – zamierzone lub przypadkowe naruszenie środków technicznych i organizacyjnych zastosowanych w celu ochrony danych osobowych. W szczególności, gdy stan urządzenia, zawartość zbioru danych osobowych, ujawnione metody pracy, sposób działania programu lub jakość komunikacji w sieci telekomunikacyjnej mogą wskazywać na naruszanie ochrony danych osobowych.
9. **Poufność** – właściwość zapewniająca, że informacja (np. dane osobowe) jest dostępna jedynie osobom upoważnionym.
10. **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.
11. **Rozporządzenie** - Rozporządzenie Ministra Spraw Wewnętrznych i Administracji z dnia 29 kwietnia 2004 r. w sprawie dokumentacji przetwarzania danych osobowych oraz warunków technicznych i organizacyjnych, jakim powinny odpowiadać urządzenia i systemy informatyczne służące do przetwarzania danych osobowych (Dz. U. Nr 100, poz. 1024, z późn. zm.).
12. **Rozliczalność** – właściwość zapewniająca, że działania podmiotu mogą być przypisane w sposób jednoznaczny tylko temu podmiotowi.
13. **System informatyczny** – zespół współpracujących urządzeń, programów, procedur przetwarzania informacji i narzędzi programowych zastosowanych w celu przetwarzania danych.
14. **Urząd** – Urząd Miejski w Zalewie, ul. Częstochowska 8 ; 14-230 Zalewo
15. **Ustawa** – Ustawa o ochronie danych osobowych z dnia 29 sierpnia 1997 r. (Dz. U. z 2002 r. Nr 101, poz. 926 z późn. zm.).
16. **Użytkownik systemu** – osoba upoważniona do bezpośredniego dostępu do danych osobowych przetwarzanych w systemie informatycznym, która posiada ustalony identyfikator i hasło.
17. **Użytkownik zewnętrzny** - osoba nie będąca pracownikiem lub stażystą Urzędu, posiadająca uprawnienia do przetwarzania informacji w związku z Polityką bezpieczeństwa przetwarzania i ochrony danych osobowych Urzędu Miejskiego w Zalewie.
18. **Właściciel zasobów danych osobowych** – kierownik komórki organizacyjnej, odpowiedzialnej za ochronę danych osobowych przetwarzanych w podległej komórce. Jest on zobowiązany 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.
19. **Zbiór danych osobowych** – każdy zestaw danych posiadający strukturę o charakterze osobowym, dostępnych według określonych kryteriów, niezależnie od tego, czy zestaw ten jest rozproszony czy podzielony funkcjonalnie

20. **Zbiór nieinformatyczny** - każdy zestaw danych posiadający strukturę o charakterze osobowym, dostępnych według określonych kryteriów, niezależnie od tego czy zestaw ten jest rozproszony lub podzielony funkcjonalnie, prowadzony poza systemem informatycznym, w szczególności w formie kartoteki, skorowidza, księgi, wykazu lub innego zbioru ewidencyjnego.

§ 3

Deklaracja Administratora Danych Osobowych

1. ADO zobowiązuje się do podjęcia odpowiednich kroków, mających na celu zapewnienie prawidłowej ochrony danych osobowych, w szczególności do zapewnienia, że przez cały okres ich przetwarzania, dane będą:
   1) przetwarzane zgodnie z prawem,
   2) zbierane dla oznaczonych, zgodnych z prawem celów i nie poddawane dalszemu przetwarzaniu niezgodnemu z tymi celami,
   3) merytorycznie poprawne i adekwatne w stosunku do celów, w jakich są przetwarzane,
   4) przechowywane w postaci umożliwiającej identyfikację osób, których dotyczą, nie dłużej niż jest to niezbędne do osiągnięcia celu przetwarzania,
   5) zabezpieczone środkami technicznymi i organizacyjnymi, które zapewniają rozliczalność, integralność oraz poufność danych,
2. Przy przetwarzaniu danych osobowych w systemach informatycznych Urzędu Miejskiego w Zalewie 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 Gminy, 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 Gminy 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 Gminie dotyczących ochrony danych osobowych.
5. Wszelkie znaczące zmiany Polityki powinny być dokonane przez ABI zatwierdzane przez Burmistrza Zalewa.

§ 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 systemów informatycznych i - w miarę możliwości organizacyjnych i techniczno-finansowych - wdrażanie nowych narzędzi i metod pracy oraz sposobów zarządzania systemami informatycznymi, 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 Osobowych powinien być zapewniony, że pracownicy, wykonawcy oraz użytkownicy zewnętrzni.
   1) są odpowiednio wprowadzani w swoje obowiązki i odpowiedzialności związane z ochroną danych osobowych i ich przetwarzaniem przed przyznaniem im dostępu do danych osobowych,
   2) otrzymali zalecenia określające wymagania w zakresie bezpieczeństwa danych osobowych związane z ich obowiązkami w Gminie,
   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 lub rolą sprawowaną w procesie przetwarzania danych.

§ 6

Dokumenty powiązane

Na dokumentacje ochrony danych osobowych w Urzędzie Miejskim w Zalewie składają się;

1. **Ewidencja osób upoważnionych przez Administratora Danych Osobowych do przetwarzania danych osobowych. (wzór Zał. Nr 1)** -prowadzona przez Administratora Bezpieczeństwa Informacji,
2. E**widencja zbiorów danych osobowych przetwarzanych w Urzędzie Miejskim w Zalewie oraz programów zastosowanych do ich przetwarzania. (wzór Zał. Nr 2)**

   prowadzona przez Administratora Bezpieczeństwa Informacji,
3. **Opisy struktur zbiorów danych osobowych**

   -prowadzone przez Administratora Systemów Informatycznych,
4. **Opisy sposobów przepływu danych pomiędzy systemami**

   - prowadzone przez Administratora Systemów Informatycznych,
5. **Oryginały i Kopie dokumentów dotyczących ochrony danych osobowych** (w tym kopie wniosków o rejestrację/aktualizacje zbiorów danych osobowych do GIODO oraz uchwały, zarządzenia, polityki itd. dotyczące ochrony danych osobowych)

   - prowadzone przez Administratora Bezpieczeństwa Informacji,

6. **Protokóły z przeprowadzonych kontroli wewnętrznych i zewnętrznych w zakresie ochrony danych osobowych**

   - prowadzone przez Administratora Bezpieczeństwa Informacji,

7. **Plany archiwizacji danych osobowych i programów służących do ich przetwarzania**

   - prowadzone przez Administratora Systemów Informatycznych,

8. **Ewidencje przenośnych nośników danych używanych w poszczególnych komórkach organizacyjnych Urzędu**

   - prowadzone przez Właścicieli zasobów.

§ 7

Odpowiedzialność Administratora Danych Osobowych

1. Administrator Danych Osobowych jest odpowiedzialny za przetwarzanie i ochronę danych osobowych zgodnie z przepisami prawa, w tym wprowadzenie do stosowania procedur postępowania zapewniających prawidłowe przetwarzanie danych osobowych, rozumiane jako ochronę danych przed ich udostępnieniem osobom nieupoważnionym, zmianą lub zabraniem przez osobę nieuprawnioną, przetwarzaniem z naruszeniem Ustawy oraz utratą, uszkodzeniem lub zniszczeniem.
2. Do kompetencji Administratora Danych Osobowych należy w szczególności:
   1) Wyznaczenie Administratora Bezpieczeństwa Informacji.
   2) Wyznaczanie Właścicieli zasobów danych osobowych.
   3) Określenie celów i strategii 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) Przyjmowanie i zatwierdzanie niezbędnych, wymaganych przez przepisy prawa dokumentów regulujących ochronę danych osobowych w Urzędzie
   3) Nadawanie upoważnień pracownikom Urzędu oraz użytkownikom zewnętrznym do przetwarzania danych osobowych.
   4) Zapewnienie środków finansowych na ochronę fizyczną pomieszczeń, w których przetwarzane są dane osobowe.
   5) Zapewnienie środków finansowych niezbędnych do ochrony danych osobowych przetwarzanych w systemach informatycznych oraz w zbiorach nieinformatycznych.
   6) Zapewnienie środków finansowych na merytoryczne przygotowanie osób odpowiedzialnych za nadzór nad ochroną danych osobowych.
   7) Zapewnienie realizacji obowiązku zgłoszenia i aktualizacji zbiorów danych osobowych do rejestracji GIODO.

§ 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 **(powołanie ABI zał. Nr 3)**
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 (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 Urzędu Gminy z przepisami i zasadami ochrony danych osobowych oraz informowanie o zagrożeniach związanych z ich przetwarzaniem.
   6) reprezentowanie Urzędu w kontaktach z Biurem GIODO,
   7) przygotowywanie zgłoszeń 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 dotyczących ukarania winnych naruszeń,
   9) sprawdzanie wypełnienia obowiązków technicznych i organizacyjnych związanych z ochroną danych osobowych.

5. 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.

6. 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 ASI pełni pracownik wyznaczony przez Administratora Danych Osobowych
2. Do kompetencji 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. Do obowiązków Administratora Systemów Informatycznych należy:
   1) bieżący nadzór oraz zapewnianie optymalnej ciągłości działania systemu informatycznego w tym opracowanie zasad określających zarządzanie systemem informatycznym przetwarzającym dane osobowe,
   2) reagowanie bez zbędnej zwłoki, w przypadku naruszenia bądź powstania zagrożenia bezpieczeństwa danych osobowych,
   3) przeciwdziałanie próbom naruszenia bezpieczeństwa danych osobowych,
   4) analizę raportów wszelkich zdarzeń w tym incydentów związanych z bezpieczeństwem systemów przetwarzania danych,
   5) zapewnienie zgodności wszystkich wdrażanych systemów przetwarzania danych osobowych z Ustawą oraz z niniejszą Polityką i Instrukcją Zarządzania Systemem Informatycznym w Urzędzie Miejskim w Zalewie,
   6) instalację i konfigurację oprogramowania i sprzętu typu „stand-alone", sieciowego i serwerowego używanego do przetwarzania danych osobowych,
   7) konfigurację i administrację oprogramowaniem systemowym i sieciowym zabezpieczającym dane osobowe przed nieupoważnionym dostępem,
   8) nadzór nad czynnościami związanymi ze sprawdzaniem systemu pod kątem obecności szkodliwego oprogramowania,
   9) nadzór nad systemem komunikacji w sieci komputerowej oraz przesyłaniem danych za pośrednictwem urządzeń teletransmisji,
   10) nadzór nad naprawami, konserwacją oraz likwidacją urządzeń komputerowych, na których zapisane są dane osobowe,
   11) przyznawanie na wniosek Właściciela zasobów, za zgodą Administratora Danych i zatwierdzeniu przez Administratora Bezpieczeństwa Informacji ściśle określonych praw dostępu do danych osobowych w danym systemie,
   12) świadczenie pomocy technicznej w ramach oprogramowania a także serwis sprzętu komputerowego będącego na stanie Urzędzie Miejskim w Zalewie, służącego do przetwarzania danych osobowych,

13) diagnozowanie i usuwanie awarii sprzętu komputerowego oraz realizacje umów z firmami świadczącymi usługi pogwarancyjnego sprzętu komputerowego,

14) wykonywanie i **zarządzanie kopiami awaryjnymi** oprogramowania systemowego (w tym danych osobowych oraz zasobów umożliwiających ich przetwarzanie) i sieciowego,

15) wykonywanie i przechowywanie dokumentacji o której mowa w § 6 należącej do kompetencji ASI,

16) nadzór nad wdrożeniem i **zarządzanie aplikacjami** (przeglądanie, nadawanie i odbieranie uprawnień użytkownikom, itp.), w których przetwarza się dane osobowe,

17) zatwierdzanie wniosków zgłoszeń do rejestracji zbiorów danych osobowych w części E i F,

18) umożliwienie przeprowadzenia kontroli systemu informatycznego przez służby Biura Generalnego Inspektora Ochrony Danych Osobowych.

§ 10

Odpowiedzialność Właścicieli zasobów danych osobowych.

1. Administrator Danych Osobowych wyznacza kierowników komórek organizacyjnych 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, cel przetwarzania oraz komu dane osobowe mają być udostępniane. Wszystkie te informacje powinny zostać przekazane do Administratora Bezpieczeństwa Informacji oraz Administratora Systemu Informatycznego.
   8) Przygotowanie wniosku do rejestracji/zmiany 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 użytkowników systemów.

1. W celu osiągnięcia i utrzymania wysokiego poziomu bezpieczeństwa przetwarzania danych osobowych konieczne jest zaangażowanie ze strony każdego pracownika i użytkownika zewnętrznego w zakresie ochrony danych osobowych.
2. Pracownicy Urzędu Miejskiego 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 konkretnych działań i procesów w celu zapewnienia ochrony danych osobowych.
4. Pracownicy / użytkownicy zewnętrzni powinni mieć świadomość możliwości zaistnienia sytuacji naruszenia ochrony danych osobowych. W tym celu powinni:
   1) przestrzegać procedur związanych z otwieraniem i zamykaniem pomieszczeń, a także z wejściem do obszarów przetwarzania danych osobowych osób nieupoważnionych,
   2) informować Administratora Bezpieczeństwa Informacji o podejrzanych osobach,
   3) pracownicy / użytkownicy zewnętrzni 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

Sankcje za naruszenie zasad ochrony danych osobowych

1. Naruszenie zasad ochrony danych osobowych przez pracownika / użytkownika zewnętrznego może skutkować postawieniem mu zarzutu popełnienia jednego z przestępstw określonych w Rozdziale 8 Ustawy 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 Miejski 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 sprzeczny 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 Osobowych 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.

§ 13

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 przetwarzania danych osobowych,
   3) procedury dotyczące bezpiecznego przetwarzania danych osobowych w systemach informatycznych ,
   4) zasady użytkowania urządzeń i systemów informatycznych służących do przetwarzania danych osobowych,
   5) zagrożenia na jakie może być narażone przetwarzanie danych osobowych, a w szczególności te związane z przetwarzaniem danych osobowych w systemach informatycznych,
   6) zasady dostępu do pomieszczeń, w których przetwarzane są dane osobowe,
   7) sposób postępowania w przypadku naruszenia ochrony danych osobowych lub systemu informatycznego,
   8) odpowiedzialność z tytułu naruszenia ochrony danych osobowych.
2. Szkolenia powinny być powtarzane okresowo lub na żądanie, gdy zaistnieje taka potrzeba.
3. 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.

§ 14

Wymiana informacji dotyczących danych osobowych

1. Pracownicy Urzędu Miejskiego oraz użytkownicy zewnętrzni w celu ochrony wymienianych informacji dotyczących danych osobowych powinni podczas przetwarzania uwzględniać następujące zasady:
   1) wykorzystywanie technik kryptograficznych do ochrony poufności, integralności i rozliczalności danych osobowych przesyłanych publicznymi sieciami telekomunikacyjnymi,
   2) ochrona wymienianych danych osobowych przed przechwyceniem, kopiowaniem, modyfikacją, błędnym wyborem drogi komunikacji 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.

3. Transport danych osobowych w formie elektronicznej i papierowej pomiędzy obszarami, w których są przetwarzane dane osobowe powinien być prowadzony przez osoby upoważnione w sposób ograniczający możliwość ich pozyskanie i odczyt przez osoby nieupoważnione.

§ 15

Przetwarzanie danych osobowych w obszarach bezpiecznych

1. Dane osobowe w Urzędzie Miejskim mogą być przetwarzane wyłącznie w pomieszczeniach przetwarzania danych osobowych.
2. Na pomieszczenia przetwarzania danych osobowych składają się pomieszczenia biurowe oraz części pomieszczeń, gdzie Urząd Miejskim 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 ABI,
   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 przechowywane w zamykanych szafach, które znajdują się w obszarach przetwarzania danych osobowych.
11. Każdorazowe uchybienie zabezpieczeń fizycznych chroniących dane osobowe powinno być zgłaszane do Administratora Bezpieczeństwa Informacji.

§ 16

Dopuszczenie osób do przetwarzania danych osobowych

1 Przetwarzanie danych osobowych jest możliwe wyłącznie po uzyskaniu przez pracownika / użytkownika zewnętrznego formalnego upoważnienia do przetwarzania danych osobowych zaakceptowanego przez Administratora Danych Osobowych i wystawianego przez Administratora Bezpieczeństwa Informacji, w tym celu przełożony pracownika / użytkownika zewnętrznego przed dopuszczeniem pracownika do pracy przy przetwarzaniu danych osobowych:

1) zapoznaje pracownika / użytkownika zewnętrznego z przepisami dotyczącymi ochrony danych osobowych oraz uregulowaniami wewnętrznymi obowiązującymi w tym zakresie w Urzędzie,

2) przyjmuje od pracownika / użytkownika zewnętrznego 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 w Urzędzie Miejskim w Zalewie", którego wzór stanowi **zał. Nr 4** niniejszej Polityki,

3) wnioskuje do Administratora Bezpieczeństwa Informacji o formalne **upoważnienie** pracownika do przetwarzania danych osobowych sporządzane wg wzoru stanowiącego **zał. Nr 6** niniejszej Polityki.

2. Oświadczenia i upoważnienia, o których mowa w ust. 1 przechowuje się w aktach osobowych pracownika.
3. Przełożony pracownika / użytkownika zewnętrznego jest zobowiązany niezwłocznie po ustaniu potrzeby przetwarzania danych osobowych przez pracownika / użytkownika zewnętrznego złożyć rezygnację do Administratora Bezpieczeństwa Informacji dotyczącą jego dostępu do danych osobowych.

§ 17

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 (ewidencja) powinna być prowadzona przez Administratora Bezpieczeństwa Informacji.
2. Jakakolwiek zmiana w zakresie informacji zawartych w ewidencji powinna podlegać natychmiastowemu odnotowaniu.
3. Właściciele zasobów danych osobowych, przełożeni pracowników / użytkowników zewnętrznych 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.

§ 18

Dostęp zdalny

1. Zastosowane przez Urząd 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 Osobowych
3. Dostęp do systemów informatycznych dla użytkowników zewnętrznych powinien być monitorowany pod kątem bezpieczeństwa przez Administratorów Systemów Informatycznych w celu zapewnienia poufności, rozliczalności i integralności danych osobowych.

§ 19

Rejestr zbiorów danych osobowych

1. Upoważnieni pracownicy są zobowiązani do wnioskowania 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 w części A-D.
4. Zgłoszenie / zmiana wniosku zgłoszenia zbioru do rejestracji przez GIODO w części E – F jest przygotowywana przez Administratora Systemów Informatycznych odpowiedzialnego za odpowiednie zabezpieczenie danych w systemie informatycznym Urzędu.
5. 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 Osobowych o podniesienie poziomu tych zabezpieczeń.
6. Sprawdzony przez Administratora Bezpieczeństwa Informacji projekt zgłoszenia zbioru danych osobowych do rejestracji w GIODO jest przedstawiany Administratorowi Danych Osobowych do podpisu.
7. Administrator Danych Osobowych zgłasza wniosek o rejestrację zbioru danych osobowych do GIODO i wyznacza Właściciela zasobów danych osobowych dla zarejestrowanego zbioru danych osobowych.
8. 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.
9. Pismo jest wysyłane przez Administratora Bezpieczeństwa Informacji do GIODO.

§ 20

Udostępnianie danych osobowych

1. Dane osobowe mogą być udostępniane podmiotom uprawnionym do ich otrzymania na mocy przepisów prawa, osobom, których dotyczą oraz w szczególnych przypadkach na podstawie art. 29 ust. 2 Ustawy.
2. Udostępnianie danych osobowych osobie nieupoważnionej do przetwarzania danych osobowych może nastąpić wyłącznie za zgodą Właściciela zasobów danych osobowych. Zgoda może dotyczyć również udostępniania danych osobowych w przyszłości. Zarówno wniosek jak i zgoda powinny być wystosowane z zachowaniem formy pisemnej
3. Udostępniając dane osobowe należy zaznaczyć, że można je wykorzystać wyłącznie zgodnie z przeznaczeniem, dla którego zostały udostępnione.
4. Na pisemny wniosek pochodzący od osoby, której dane dotyczą, informacje o osobie powinny być udzielone w terminie 30 dni od daty złożenia wniosku.
5. Za przygotowanie danych osobowych do udostępnienia w zakresie wskazanym we wniosku jest odpowiedzialny Właściciel zasobów danych osobowych.
6. Informacje zawierające dane osobowe są przekazywane uprawnionym podmiotom lub osobom za potwierdzeniem odbioru, np. w następujący sposób:
   1) listem poleconym za pokwitowaniem odbioru,
   2) teletransmisji danych zgodnie z zasadami Polityki,
   3) innym bezpiecznym, określonym wymogiem prawnym lub umową.
7. 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 Urzędu udostępniły dane osobowe. Nie dotyczy to sytuacji, gdy przepisy prawa zezwalają na zbieranie danych osobowych bez konieczności ujawniania adresata danych.

§ 21

Powierzenie przetwarzania danych osobowych

1. Powierzenie przetwarzania danych osobowych występuje wówczas, gdy podmioty zewnętrzne współpracujące z Urzędem mają dostęp do danych osobowych przetwarzanych przez Urząd.
2. Wskazane w ust. 1 powierzenie przetwarzania danych osobowych może się odbywać wyłącznie w trybie przewidzianym w art. 31 Ustawy poprzez zawarcie na piśmie umowy powierzenia przetwarzania danych osobowych, pomiędzy Urzędem a danym podmiotem, któremu zleca się czynności związane z przetwarzaniem danych osobowych lub uwzględnienie kwestii powierzenia w umowach.
3. W sytuacji powierzenia przetwarzania danych osobowych podmiotowi zewnętrznemu, w umowie powierzenia przetwarzania danych osobowych określa się przede wszystkim:
   1) Cel i zakres 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. Właściciele zasobów danych osobowych są zobowiązani do wnioskowania do Administratora Bezpieczeństwa Informacji o przygotowanie projektu umowy powierzenia danych osobowych dla zasobów danych osobowych, za które są odpowiedzialni.
6. Projekt umowy powierzenia przetwarzania danych osobowych innemu podmiotowi przygotowuje zespół powołany przez Administratora Bezpieczeństwa Informacji.
7. Powierzenie przetwarzania danych osobowych poza granice Rzeczpospolitej Polskiej wymaga zgody Administratora Danych Osobowych i odbywa się po sprawdzeniu wymagań prawnych obowiązujących w tym zakresie.

§ 22

Postępowanie w przypadku naruszenia lub podejrzenia 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 / użytkownicy zewnętrzni 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, w którym powinny się znaleźć w szczególności informacje o:
   1) Dacie i godzinie powiadomienia.
   2) Godzinie pojawienia się w pomieszczeniach, w których przetwarzane są dane.
   3) Sytuacji, jaką zastał.
   4) Podjętych działaniach i ich uzasadnieniu.
   5) Stanie systemu po podjęciu działań naprawczych.
   6) Wnioskach w sprawie ograniczenia możliwości ponownego wystąpienia naruszenia ochrony danych osobowych.
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.

§ 23
Wykaz zbiorów danych osobowych

1. Gmina Zalewo - reprezentowana przez Burmistrza Zalewa - 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 prowadzi wykaz systemów i aplikacji zastosowanych do przetwarzania danych osobowych.

§ 24

Opis struktury zbiorów danych osobowych

1. Opis struktury zbiorów danych osobowych prowadzi Administrator Systemu Informatycznego.
2. Zakresy danych osobowych przetwarzanych w poszczególnych zbiorach danych osobowych są ustalone w oparciu o strukturę zbiorów danych osobowych prowadzonych w systemach informatycznych oraz powiązania pól informacyjnych utworzonych w tych systemach.
3. Aktualny opis struktury ww. zbiorów danych osobowych wskazujący zawartość poszczególnych pól informacyjnych i powiązania między nimi powinien być prowadzony przez Administratora Systemów Informatycznych.

§ 25

Sposób przepływu danych pomiędzy poszczególnymi systemami

Administratorów 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.

§ 26

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.

§ 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 Osobowych do przetwarzania danych osobowych.

Nr upow.	Nazwisko	Imię	Stanowisko sł.	Nazwa zbioru danych osobowych	Zakres przetwarzania	Udzielone od	Udzielone do	Identyfikator

Zał. Nr 2 – Ewidencja zbiorów danych osobowych przetwarzanych w Urzędzie Miejskim w Zalewie.

Lp.	Nr ze źródłowego wykazu akt	**Właściciel zasobów**	**Nazwa zbioru**	**Forma prowadzenia**	**Data zgłoszenia**	**Data rejestracji w GIODO**	**Nr Księgi Rej. GIODO**	Program zastosowany do przetwarzania danych
1								
2								
3								
4								
5								
6								
7								
8								
9								
10								
11								
12								
13								
14								
15								

Zał. Nr 6 – Upoważnienie do przetwarzania danych osobowych.

Zalewo, ……

U P O W A Ż N I E N I E 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……

Zatrudnioną na stanowisku……..……..…… do przetwarzania danych osobowych w zbiorze o nazwie:

w systemie tradycyjnym i / lub w systemie informatycznym

identyfikator……w zakresie:……..……..

(zbierania, utrwalania, opracowywania, wprowadzania, przechowywania, zmieniania, usuwania, udostępniania, podglądu)

od dnia……..…..do dnia……..

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 Osobowych)

Przyjmuję do wiadomości i przestrzegania, zobowiązuję się do zachowania w tajemnicy tych danych oraz sposobów ich zabezpieczeń.

……

(data i podpis pracownika)

Zał. Nr 7 - Wzór wniosku o nadanie/zmianę/pozbawienie upoważnienia do przetwarzania danych osobowych.

... . Zalewo, ...
(pieczęć komórki organizacyjnej)

Burmistrz Zalewa

W N I O S E K

Zgodnie z art. 37 ustawy z dnia 29 sierpnia 1997 r. o ochronie danych osobowych

(Dz.U. z 2002 r. Nr 101, poz. 926 z późn. zm.)

w n i o s k u j ę o nadanie /pozbawienie/zmianę/*

Pani /Panu/* .....

stanowisko służbowe.....

upoważnienia do przetwarzania danych osobowych w Urzędzie Miejskim w Zalewie.

Upoważnienie wydaje się na okres: /stały/czasowy – do kiedy/* ....

1. Zakres przetwarzania danych osobowych:
   .....
   /zbieranie, utrwalanie, opracowywanie, wprowadzanie, przechowywanie, zmiana, usuwanie, udostępnianie/*
2. Nazwa zbioru danych osobowych:
   .....
3. Sposób przetwarzania danych osobowych: /papierowy/ informatyczny/*
4. Osoba została zapoznana z przepisami o ochronie danych osobowych:
   /tak/nie/*

.....
(Właściciel zasobów)

Zał. Nr 3 – Powołanie Administratora Bezpieczeństwa Informacji

Powołanie na stanowisko 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 .....2012 r. wyznaczam:

Pana/Panią

.....

ADMINISTRATORA BEZPIECZEŃSTWA INFORMACJI.

data i podpis Administratora Danych

data i podpis Administratora Bezpieczeństwa Informacji

Zał. Nr 5 – Oświadczenie o zachowaniu w poufności danych oraz sposobów ich zabezpieczeń.

.....

(imię i nazwisko)

Oświadczenie pracownika
zatrudnionego przy przetwarzaniu danych osobowych w zbiorach danych przetwarzanych przez Urząd Miejski w Zalewie.

I. Obowiązki pracownika / użytkownika zewnętrznego

Pracownik dopuszczony do przetwarzania danych osobowych zobowiązany jest do:

1. Zapoznania się i przestrzegania obowiązków wynikających z:
   a) Przepisów ustawy z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (Dz. U. z 2002 r. Nr 101, poz. 926 z późn. zm.) oraz aktów wykonawczych wydanych na jej podstawie,
   b) Dokumentów wprowadzonych przez Urząd Miejski w Zalewie w związku z przetwarzaniem danych osobowych, w szczególności:

      - Polityki Bezpieczeństwa Przetwarzania Danych Osobowych,
      - Instrukcji Zarządzania Systemem Informatycznym Służącym Do Przetwarzania Danych Osobowych.

2. Zapewnienia bezpieczeństwa przetwarzania danych osobowych poprzez ich ochronę przed niepowołanym dostępem, nieuzasadnioną modyfikacją lub zniszczeniem, nielegalnym ujawnieniem lub pozyskaniem.
3. Zachowania w tajemnicy danych oraz sposobu ich zabezpieczenia do których uzyskał dostęp w trakcie zatrudnienia, również po ustaniu zatrudnienia.

II. Odpowiedzialność pracownika

Za niedopełnienie obowiązków wynikających z niniejszego oświadczenia pracownik ponosi odpowiedzialność na podstawie przepisów Regulaminu pracy, Kodeksu pracy oraz Ustawy o ochronie danych osobowych.

Oświadczam, że treść niniejszego oświadczenia jest mi znana i zobowiązuję się do jego przestrzegania.

Potwierdzam odbiór 1 egz. oświadczenia.

Pracownik / użytkownik zewnętrzny

Administrator Bezpieczeństwa Informacji