WÓJT GMINY SŁUPNO
pow. płocki
woj. mazowieckie

OZ.0050.51.2012

ZARZĄDZENIE NR 51/2012
Wójta Gminy w Słupnie
z dnia 29 czerwca 2012 r.

w sprawie: wprowadzenia „Polityki bezpieczeństwa przetwarzania danych osobowych w Urzędzie Gminy w Słupnie"

Na podstawie art. 36 ust. 1 i 2 ustawy z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (tj. Dz. U. 2002 r. Nr 101 poz. 926, z późn. zm.) oraz § 3 i 4 rozporządzenia Ministra Spraw Wewnętrznych i Administracji z 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), zarządzam, co następuje:

§1.

Dla zapewnienia ochrony przetwarzanych danych osobowych wprowadza się „Politykę bezpieczeństwa przetwarzania danych osobowych w Urzędzie Gminy w Słupnie" zwaną dalej „Polityką", stanowiącą załącznik do niniejszego zarządzenia.

§2.

Zobowiązuję pracowników Urzędu Gminy w Słupnie do zapoznania się z treścią Polityki i stosowania zawartych w niej zasad.

§3.

Wykonanie zarządzenia powierzam Administratorowi Bezpieczeństwa Informacji.

§ 4.

Traci moc zarządzenie Nr 38/2006 Wójta Gminy w Słupnie z dnia 3 października 2006 r. w sprawie: ustalenia „Polityki bezpieczeństwa danych osobowych w Urzędzie Gminy w Słupnie" oraz „Regulaminu użytkowania oprogramowania i sprzętu komputerowego w Urzędzie Gminy w Słupnie".

§ 5

Zarządzenie wchodzi w życie z dniem 1 lipca 2012 r.

WÓJT
mgr Stefan Jakubowski

RADCA PRAWNY
mgr Danuta Jankowska

Załącznik do
zarządzenia nr 51/2012
Wójta Gminy w Słupnie
z dnia 29 czerwca 2012 r.

POLITYKA BEZPIECZEŃSTWA PRZETWARZANIA DANYCH OSOBOWYCH W URZĘDZIE GMINY W SŁUPNIE

Opracował

Administrator Bezpieczeństwa Informacji
inż. Janusz Salamon

Wydanie: 2 uaktualnione

§ 1
Zasady ogólne

1. Polityka przetwarzania danych osobowych została opracowana na podstawie ustawy z dnia 29 sierpnia 1997 roku ochronie danych osobowych (Dz. U z 2002 r.Nr 101, poz.926 z późn.zm.) w celu realizacji rozporządzenia Ministra Spraw Wewnętrznych i Administracji z dnia 29 kwietnia 2004 roku w sprawie dokumentacji przetwarzania danych osobowych oraz warunków technicznych i organizacyjnych, jakim powinny odpowiadać urządzenia i systemy informatyczne służące do przetwarzania danych osobowych (Dz. U z 2004 r. 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 w Słupnie.
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 się 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 Słupno.

§ 2
Definicje

Przez użyte w Instrukcji następujące określenia należy rozumieć:

1. **Administrator Danych Osobowych** – podmiot, który decyduje o środkach i celach przetwarzania danych osobowych - Wójt Gminy w Słupnie.
2. **Administrator Bezpieczeństwa Informacji** – osoba wyznaczona przez Wójta Gminy w Słupnie, 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 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 identyfikacje 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).
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 Gminy w Słupnie, 09-472 Słupno, ul. Miszewska 8a.
15. **Ustawa** – Ustawa o ochronie danych osobowych z dnia 29 sierpnia 1997 r. (tj. Dz. U. z 2002 r. Nr 101, poz. 926 z poźn. zm.).
16. **Użytkownik systemu** – osoba upoważniona do bezpośredniego dostępu do danych osobowych przetwarzanych w systemie informatycznym, która posiada ustalony identyfikator i hasło.
17. **Użytkowniku zewnętrznym** - należy przez to rozumieć osobę niebędącą pracownikiem lub stażystą Urzędu Gminy w Słupnie, posiadającą uprawnienia do przetwarzania informacji w związku z wykonywaniem czynności na rzecz Urzędu.
18. **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.
19. **Zbiór nieinformatyczny** - każdy posiadający strukturę zestaw danych 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. Administrator Danych Osobowych 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 niepoddawane 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 w Słupnie 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 zatwierdzane przez Wójta Gminy w Słupnie.

§ 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 Gminy w Słupnie składają się;

1 Ewidencja osób upoważnionych przez Administratora Danych Osobowych do przetwarzania danych osobowych. (wzór Zał. Nr 1)
- prowadzona przez Administratora Bezpieczeństwa Informacji

2. Ewidencja zbiorów danych osobowych przetwarzanych w Urzędzie Gminy w Słupnie - prowadzona przez Kierownika Referatu Organizacyjnego i Zarządzania Kryzysowego

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. Protokoły z przeprowadzonych kontroli wewnętrznych i zewnętrznych w zakresie ochrony danych osobowych
- prowadzone przez Administratora Bezpieczeństwa Informacji

§ 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;
   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
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) nadzór nad zapewnieniem przez Administratora Systemów Informatycznych dostosowania funkcjonalności systemów przetwarzających dane osobowe do wymagań określonych w Rozporządzeniu;
   3) 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 należącej do kompetencji 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 Gminy w kontaktach z Biurem GIODO;

7) reagowanie na zgłaszane incydenty związane z naruszeniem ochrony danych osobowych oraz analizowanie ich przyczyn i kierowanie wniosków dotyczących ukarania winnych naruszeń;

8) sprawdzanie 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 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) zapewnianie optymalnej ciągłości działania systemu informatycznego w tym opracowanie procedur 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 bezpieczeństwa i Instrukcją Zarządzania Systemem Informatycznym w Urzędzie Gminy w Słupnie;

6) instalację i konfigurację oprogramowania i sprzętu sieciowego oraz serwerowego używanego do przetwarzania danych osobowych;

7) konfigurację i administrację oprogramowaniem systemowym i sieciowym zabezpieczającym dane osobowe przed nieupoważnionym dostępem;

8) sprawdzanie 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 pracowników za zgodą Administratora Danych i po zatwierdzeniu przez Administratora Bezpieczeństwa Informacji ściśle określonych praw dostępu do danych osobowych w danym systemie oraz prowadzenie ewidencji przyznanych uprawnień;
12) świadczenie pomocy technicznej w ramach oprogramowania a także serwis sprzętu komputerowego będącego na stanie Urzędu Gminy w Słupnie, 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 odtworzenie) i sieciowego;
15) wykonywanie i przechowywanie dokumentacji, o której mowa w § 6 należącej do kompetencji ASI;
16) przygotowywanie wniosków zgłoszeń do rejestracji zbiorów danych osobowych w **części E i F.**
17) umożliwienie przeprowadzenia kontroli systemu informatycznego przez służby Biura Generalnego Inspektora Ochrony Danych Osobowych.

§ 10

Odpowiedzialność kierowników referatów i samodzielnych stanowisk pracy.

1. Kierownik referatu wykonuje czynności przetwarzania danych osobowych w ramach zbiorów, funkcjonujących w podległym referacie z upoważnienia administratora danych osobowych. Do zadań kierowników oraz samodzielnych stanowisk pracy należy w szczególności:
   1) zapewnienie aktualności, adekwatności oraz merytorycznej poprawności danych osobowych przetwarzanych w referacie;
   2) realizację obowiązku informowania o przetwarzaniu danych osobowych osób, których dane osobowe są pozyskiwane;
   3) zapewnienie na żądanie uprawnionych osób, udostępnienia informacji o przetwarzanych danych osobowych oraz podmiotach, którym zostały one udostępnione;
   4) zapewnienie uzyskania przez pracowników przetwarzających dane osobowe, formalnego upoważnienia do przetwarzania danych osobowych.
   5) 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.
   6) **przygotowanie wniosku do rejestracji/zmiany zbioru do GIODO w części A-D**
   7) wnioskowanie do Administratora Danych Osobowych o nadanie upoważnień dla pracowników podległej komórki organizacyjnej.

2. Kierownik referatu sprawuje bezpośredni nadzór nad przetwarzaniem danych osobowych w referacie i jest zobowiązany do kontroli przestrzegania zasad i sposobu wykonywania operacji przetwarzania danych osobowych przez podległych pracowników.

3. Pracownik referatu, pracownik na samodzielnym stanowisku dokonuje czynności przetwarzania danych osobowych, z upoważnienia Administratora Danych Osobowych, w zakresie indywidualnych obowiązków pracowniczych. Wzór upoważnienia stanowi załącznik **Nr 2** do polityki.

§ 11

Rejestracja 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. W sytuacji, jeśli rejestracja nowopowstałego zbioru lub zbioru wymagającego aktualizacji danych osobowych jest ustawowo wymagana, kierownik referatu 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 w zgłoszeniu rejestracyjnym warunki techniczne i organizacyjne dotyczące zabezpieczeń w systemie informatycznym, a w przypadku niewystarczającego poziomu zabezpieczeń występuje z wnioskiem do Administratora Danych Osobowych o podniesienie poziomu tych zabezpieczeń.
6. Sprawdzony przez Administratora Bezpieczeństwa Informacji projekt zgłoszenia zbioru danych osobowych do rejestracji w GIODO jest przekazywany do Kierownika Referatu Organizacyjnego i Zarządzania Kryzysowego, który przedkłada go Administratorowi Danych Osobowych do podpisu.
7. Administrator Danych Osobowych zgłasza wniosek o rejestrację zbioru danych osobowych do GIODO
8. Ewidencję zgłoszonych do GIODO zbiorów danych w Urzędzie prowadzi Kierownik Referatu Organizacyjnego i Zarządzania Kryzysowego.
9. Wzór wniosku o rejestrację zbioru danych stanowi **załącznik Nr 3** do niniejszej Polityki.

§ 12

Obszar przetwarzania danych osobowych

1.Obszar, w którym przetwarzane są dane osobowe stanowi I piętro budynku Urzędu Gminy przy ul. Miszewskiej 8a w Słupnie.
2.Dane osobowe przetwarzane są w sposób tradycyjny, a także w sieci lokalnej Urzędu Gminy.
3.Szczegółowy wykaz pomieszczeń w których przetwarzane są dane osobowe zawiera załącznik **nr 4** do polityki.

§ 13

Wykaz zbiorów danych osobowych przetwarzanych w Urzędzie

1.W skład zbiorów danych wchodzą:
   1) dokumentacja papierowa (korespondencja, wnioski, deklaracje, itd.)
   2) urządzenia i oprogramowanie komputerowe służące do przetwarzania informacji oraz procedury przetwarzania danych w tym systemie, w tym procedury awaryjne,
   3) wydruki komputerowe
2. Wykaz zbiorów danych osobowych przetwarzanych w Urzędzie stanowi załącznik **nr 5** do Polityki.
3. Kierownicy referatów, samodzielne stanowiska pracy niezwłocznie zgłaszają administratorowi bezpieczeństwa informacji wszelkie zmiany w zbiorach danych osobowych, oraz nowe zbiory danych osobowych, które podlegają zgłoszeniu Generalnemu Inspektorowi Danych Osobowych

§ 14
Struktury zbiorów danych osobowych.

1. Opis struktury zbiorów danych osobowych stanowi załącznik **nr 6** do niniejszej Polityki .
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.

§ 15
Obowiązki pracowników

1. Obowiązek przestrzegania tajemnicy danych osobowych dotyczy wszystkich pracowników, którzy mają dostęp do informacji o charakterze danych osobowych.
2. Naruszenie zasad ochrony danych osobowych, w efekcie którego nastąpiło udostępnienie danych osobie nieupoważnionej, jest ciężkim naruszeniem obowiązków pracowniczych.
3. Osoby, wymienione w ust. 1 są zobowiązane do:
   1) zapoznania się z przepisami prawa w zakresie ochrony danych osobowych,
   2) stosowania określonych przez Administratora Danych Osobowych oraz Administratora Bezpieczeństwa Informacji i Administratora Systemu zasad, procedur oraz wytycznych mających na celu właściwe i adekwatne przetwarzanie danych,
   3) należytego zabezpieczenia danych przed ich udostępnieniem osobom nie upoważnionym,
   4) zachowanie szczególnej staranności w trakcie dokonywania operacji przetwarzania danych w celu ochrony interesów osób, których dane dotyczą,

5) sygnalizowania niezgodności aktów prawnych gminy oraz innych aktów wewnętrznych Urzędu z przepisami ustawowymi w zakresie ochrony danych osobowych i przedstawienia stosownych projektów zmian, mających na celu ich dostosowanie do regulacji ustawowej,

6) zwracanie się do Administratora Bezpieczeństwa Informacji, w przypadku wątpliwości co do stosowania przepisów prawnych z zakresu ochrony danych osobowych o wiążące wytyczne.

4. Pracownik, któremu Administrator Danych Osobowych udzielił upoważnienia do przetwarzania danych osobowych jest zobowiązany do podpisania oświadczenia.
5. Wzór oświadczenia stanowi załącznik **nr 7** do Polityki.

§ 16

Procedury szczegółowe

1. W przypadku przyjęcia do pracy nowego pracownika, 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 (nie rzadziej niż raz na trzy lata) lub na żądanie, gdy zaistnieje taka potrzeba. Wzór zaświadczenia o odbyciu szkolenia stanowi załącznik **nr 8.**
3. Administrator Danych Osobowych wydaje upoważnienie do przetwarzania danych osobowych po odbyciu przeszkolenia oraz podpisaniu przez pracownika oświadczenia, o którym mowa w § 15 ust.5.
4. W przypadku zmiany stanowiska, zakresu obowiązków pracowniczych, kierownik referatu zobowiązany jest bezzwłocznie skierować wniosek o wydanie bądź cofnięcie stosownego upoważnienia do Administratora Danych Osobowych.
5. W przypadku zamiany samodzielnego stanowiska, zakresu obowiązków pracowniczych na tym stanowisku wydanie bądź cofnięcie upoważnienia dokonuje bezpośrednio Administrator Danych Osobowych.
6. Wzór pozbawienia pracownika upoważnienia do przetwarzania danych osobowych stanowi załącznik **nr 9** do niniejszej Polityki.
7. Administrator Bezpieczeństwa Informacji prowadzi wykaz pracowników pozbawionych upoważnienia do przetwarzania danych osobowych według wzoru określonego w załączniku **nr 10** do Polityki.

8. Rozwiązanie stosunku pracy w okresie obowiązywania upoważnienia powoduje jego wygaśnięcie, z zastrzeżeniem ust.9.
9. Wypowiedzenie umowy o pracę przez pracodawcę powoduje wygaśnięcie upoważnienia do przetwarzania danych z dniem wręczenia wypowiedzenia umowy o pracę.

§ 17
Udostępnianie danych osobowych

1.W obiegu zewnętrznym dane osobowe udostępnia ze zbiorów zgodnie z powszechnie obowiązującymi w tym zakresie przepisami, Administrator Danych Osobowych lub osoba przez niego upoważniona.
2. W obiegu wewnętrznym między pracownikami Urzędu, chyba że przepisy szczególne stanowią inaczej można udostępniać dane osobowe w następującym trybie: informacje zawierające dane: imię i nazwisko, adres zamieszkania i inne o charakterze podstawowym bezpośrednio identyfikujące osobę fizyczną może udostępnić pracownik przetwarzający dane w formie bezpośredniej.
3. Tryb określony w ust.2, może być w uzasadnionych przypadkach stosowany również w wymianie informacji i danych osobowych między pracownikami Urzędu a jednostkami organizacyjnymi gminy.
4. Przekazywanie danych w trybie ust.2 i 3, może odbywać się tylko i wyłącznie w przypadku toczącego się postępowania administracyjnego bądź cywilnego w stosunku do osoby, której dane dotyczą.
5. Udostępnianie danych osobowych, o których mowa w ust. 1 jest udokumentowane w prowadzonym „rejestrze".
6. W umowach zawieranych przez Wójta w przypadku zaistnienia okoliczności powierzenia danych osobowych podmiotowi zewnętrznemu w celu wykonania określonych czynności na tych danych, każdorazowo wymagany jest zapis o powierzeniu danych osobowych bądź zawarciu odrębnej umowy powierzenia.
7. W przypadkach, o których mowa w ust. 6 kierownik referatu, bądź pracownik na samodzielnym stanowisku pracy, nie później niż w ciągu 15 dni:
   1) przed podpisaniem umowy, w której został zawarty zapis o powierzeniu;
   2) przed datą planowanego powierzenia danych, na podstawie odrębnej umowy powierzenia;

przekazuje Administratorowi Danych Osobowych projekt umowy, o której mowa w pkt. 1 lub projekt umowy, o której mowa w pkt.2.

§ 18
Środki techniczne i organizacyjne niezbędne do zapewnienia poufności, integralności przetwarzanych danych

1. Budynek Urzędu jest chroniony systemem alarmowym i nadzorowany przez firmę ochroniarską Agencji Ochrony Osób i Mienia OTEL w Cekanowie ul. Płocka 23, przez całą dobę (zamykany po zakończeniu pracy).
2. Urządzenia służące do przetwarzania danych osobowych znajdują się w pomieszczeniach zamykanych na klucz.
3. Drzwi na parterze są antywłamaniowe.
4. Przebywanie osób nieuprawnionych w pomieszczeniach tworzących obszar przetwarzania danych osobowych dopuszczalne jest tylko w obecności osoby zatrudnionej przy przetwarzaniu danych lub w obecności Administratora

Bezpieczeństwa Informacji.
5. Pomieszczenia, o których mowa wyżej, powinny być zamykane na czas nieobecności pracownika zatrudnionego przy przetwarzaniu danych, w sposób uniemożliwiający dostęp do nich osób trzecich.
6. W przypadku przebywania interesantów bądź innych osób postronnych w pomieszczeniach, o których mowa wyżej, monitory stanowisk dostępu do danych osobowych powinny być ustawione w taki sposób, aby uniemożliwić tym osobom wgląd w dane.
7. Do przebywania w pomieszczeniu serwera uprawnieni są: Administrator Bezpieczeństwa Informacji, Administrator Systemu teleinformatycznego oraz Administrator Danych.
8. Dostęp do serwera osób nieuprawnionych (konserwator, elektryk, sprzątaczka) dopuszczalny jest tylko w obecności jednej z osób upoważnionych, o których mowa w ust.7
9.Każdy dokument papierowy zawierający dane osobowe przeznaczony do wyrzucenia powinien być zniszczony w sposób uniemożliwiający jego odczytanie , przy pomocy niszczarki do papieru.
10.Urządzenia wchodzące w skład systemu informatycznego zabezpieczone są UPS-em na wypadek zaniku napięcia.
11.Sieć lokalna podłączona do Internetu.
12.Na serwerze oraz w poszczególnych stacjach roboczych zainstalowano programowanie antywirusowe.
13.Zastosowano wygaszanie ekranu w przypadku dłuższej nieaktywności użytkownika.
14.Komputer, z którego możliwy jest dostęp do danych osobowych zabezpieczony jest hasłem wejściowym do systemu operacyjnego.
15.Dla każdego użytkownika systemu jest ustalony odrębny identyfikator i hasło.

§19

Postępowanie w przypadku naruszenia ochrony danych osobowych

1. W przypadku stwierdzenia naruszenia:
   1) zabezpieczenia systemu informatycznego,
   2) technicznego stanu urządzeń,
   3) zawartości zbioru danych osobowych,
   4) ujawnienia metody pracy lub sposobu działania programu,
   5) jakości transmisji danych w sieci telekomunikacyjnej mogącej wskazywać na naruszenie zabezpieczeń tych danych,
   6) innych zdarzeń mogących mieć wpływ na naruszenie danych osobowych (np. zalanie, pożar, itp.)

każda osoba zatrudniona przy przetwarzaniu danych osobowych jest obowiązana niezwłocznie powiadomić o tym fakcie Administratora Bezpieczeństwa Informacji.

2. W razie niemożliwości zawiadomienia Administratora Bezpieczeństwa Informacji lub osoby przez niego upoważnionej, należy powiadomić bezpośredniego przełożonego,
3. Do czasu przybycia na miejsce naruszenia ochrony danych osobowych Administratora Bezpieczeństwa Informacji lub innej osoby upoważnionej przez Administratora Danych Osobowych, należy:
   1) niezwłocznie podjąć czynności niezbędne dla powstrzymania niepożądanych

skutków zaistniałego naruszenia, o ile istnieje taka możliwość, a następnie uwzględnić w działaniu również ustalenie przyczyn lub sprawców,
2) rozważyć wstrzymanie bieżącej pracy na komputerze lub pracy biurowej w celu zabezpieczenia miejsca zdarzenia,
3) zaniechać - o ile to możliwe - dalszych planowanych przedsięwzięć, które wiążą się z zaistniałym naruszeniem i mogą utrudnić udokumentowanie i analizę,
4) podjąć inne działania przewidziane i określone w instrukcjach technicznych i technologicznych stosownie do objawów i komunikatów towarzyszących naruszeniu,
5) podjąć stosowne działania, jeśli zaistniały przypadek jest określony w dokumentacji systemu operacyjnego, dokumentacji bazy danych lub aplikacji użytkowej,
6) zastosować się do innych instrukcji i regulaminów, jeżeli odnoszą się one do zaistniałego przypadku,
7) udokumentować wstępnie zaistniałe naruszenie,
8) nie opuszczać bez uzasadnionej potrzeby miejsca zdarzenia do czasu przybycia Administratora Bezpieczeństwa Informacji lub osoby upoważnionej.

4. Po przybyciu na miejsce naruszenia lub ujawnienia ochrony danych osobowych, Administrator Bezpieczeństwa lub osoba go zastępująca:
1) zapoznaje się z zaistniałą sytuacją i dokonuje wyboru metody dalszego postępowania mając na uwadze ewentualne zagrożenia dla prawidłowości pracy Urzędu,
2) może żądać dokładnej relacji z zaistniałego naruszenia od osoby powiadamiającej, jak również od każdej innej osoby, która może posiadać informacje związane z zaistniałym naruszeniem,
3) rozważa celowość i potrzebę powiadamia o zaistniałym naruszeniu Administratora danych ,
4) nawiązuje bezpośredni kontakt, jeżeli zachodzi taka potrzeba, ze specjalistami spoza Urzędu.

5. Administrator Bezpieczeństwa Informacji dokumentuje zaistniały przypadek naruszenia oraz sporządza raport wg wzoru stanowiącego załącznik **nr 11**, który powinien zawierać w szczególności:
1) wskazanie osoby powiadamiającej o naruszeniu oraz innych osób odpytanych w związku z naruszeniem,
2) określenie czasu i miejsca naruszenia i powiadomienia,
3) określenie okoliczności towarzyszących i rodzaju naruszenia,
4) wyszczególnienie wziętych faktycznie pod uwagę przesłanek do wyboru metody postępowania i opis podjętego działania,
5) wstępną ocenę przyczyn wystąpienia naruszenia,
6) ocenę przeprowadzonego postępowania wyjaśniającego i naprawczego.

6. Raport, o którym mowa w ust. 5, Administrator Bezpieczeństwa Informacji niezwłocznie przekazuje Administratorowi Danych, a w przypadku jego nieobecności osobie uprawnionej.
7. Po wyczerpaniu niezbędnych środków doraźnych po zaistniałym naruszeniu Administrator Bezpieczeństwa Informacji zasięga niezbędnych opinii i proponuje postępowanie naprawcze, a w tym ustosunkowuje się do kwestii ewentualnego odtworzenia danych z zabezpieczeń oraz terminu wznowienia przetwarzania danych.
8. Zaistniałe naruszenie może stać się przedmiotem szczegółowej, zespołowej analizy prowadzonej przez Kierownictwo urzędu, Administratora Bezpieczeństwa Informacji,

Administratora Systemu teleinformatycznego, Pełnomocnika ds. Ochrony Informacji Niejawnych.
9. Analiza, o której mowa w ust. 8, powinna zawierać wszechstronną ocenę zaistniałego naruszenia, wskazanie odpowiedzialnych, wnioski co do ewentualnych przedsięwzięć proceduralnych, organizacyjnych, kadrowych i technicznych, które powinny zapobiec podobnym naruszeniom w przyszłości.

§20

Znajomość polityki bezpieczeństwa.

Do zapoznania się z niniejszym dokumentem oraz stosowania zawartych w nim zasad i procedur zobowiązani są wszyscy pracownicy Urzędu upoważnieni do przetwarzania danych osobowych.

Wykaz załączników:
Zał. Nr 1 Ewidencja osób upoważnionych przez Administratora Danych Osobowych do przetwarzania danych osobowych (wzór).
Zał. Nr 2 Upoważnienie do przetwarzania danych osobowych(wzór).
Zał. Nr 3 Wniosek o zgłoszenie zbioru danych do rejestracji GIODO (wzór)
Zał. Nr 4 Szczegółowy wykaz pomieszczeń w których przetwarzane są dane osobowe
Zał. Nr 5 Wykaz zbiorów danych osobowych przetwarzanych w Urzędzie
Zał. Nr 6 Opis struktury zbiorów danych osobowych
Zał. Nr 7 Wzór oświadczenia
Zał. Nr 8 Wzór zaświadczenia o odbyciu szkolenia
Zał. Nr 9 Pozbawienie pracownika upoważnienia do przetwarzania danych osobowych (wzór)
Zał. Nr 10 Wykaz pracowników pozbawionych upoważnienia do przetwarzania danych osobowych (wzór)
Zał. Nr 11 Raport z naruszenia bezpieczeństwa danych osobowych (wzór)

Załącznik nr 1 do polityki bezpieczeństwa

WZÓR

EWIDENCJA OSÓB
UPOWAŻNIONYCH PRZEZ ADMINISTRATORA DANYCH OSOBOWYCH
do przetwarzania danych osobowych

Lp.	Nazwisko i imię	Stanowisko	Nr upoważnienia	Nr identyfikatora	Data wydania	Data ważności
1.	2.	3.	4.	5.	6.	7.
1.						
2.						
3.						
4.						
5.						
6.						
7.						
8.						
9.						
10.						
11.						
12.						
13.						
14.						
15.						
16.						
17.						
18.						
19.						
20.						
21.						
22.						
23.						

Załącznik nr 2 do polityki bezpieczeństwa

.....
/miejscowość, data/

WZÓR

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

U p o w a ż n i a m

.....
/imię i nazwisko/

zatrudnioną na stanowisku - .....

do przetwarzania danych osobowych oraz do obsługi systemu informatycznego a także urządzeń wchodzących w jego skład, służących do przetwarzania danych osobowych w Urzędzie Gminy Słupno w zakresie - pomoc administracyjna,

i nadaję Pani identyfikator .....

Zobowiązuję Pana/Panią do zachowania tajemnicy o przetwarzanych zbiorach danych, jak i sposobach ich zabezpieczenia. Obowiązek ten istnieje również po ustaniu zatrudnienia.

Upoważnienie wydaje się na czas nieokreślony/określony do dnia ..... roku.

.....
Administrator Danych

WZÓR

ZGŁOSZENIE ZBIORU DANYCH DO REJESTRACJI GENERALNEMU INSPEKTOROWI OCHRONY DANYCH OSOBOWYCH

* ☐ — *zgłoszenie zbioru na podstawie art. 40 ustawy z dnia 29 sierpnia 1997 r. o ochronie danych osobowych* (Dz. U. z 2002 r. Nr 101, poz. 926, z późn. zm.),
* ☐ — zgłoszenie zmian na podstawie art. 41 ust. 2 ustawy z dnia 29 sierpnia 1997 r. o ochronie danych osobowych,
* ☐ — zgłoszenie zbioru, w którym będą przetwarzane dane określone w art. 27 ust. 1 ustawy z dnia 29 sierpnia 1997 r. o ochronie danych osobowych.

Nr .....
(nadaje urzędnik Biura GIODO)

Część A. Wniosek

Wnoszę o wpisanie zbioru danych osobowych o nazwie:

.....

do Rejestru Zbiorów Danych Osobowych.

Część B. Charakterystyka administratora danych

1. Wnioskodawca (administrator danych): .....
.....
.....
.....
(nazwa administratora danych i adres jego siedziby lub nazwisko, imię i adres miejsca zamieszkania wnioskodawcy oraz nr REGON)

2. Przedstawiciel wnioskodawcy, o którym mowa w art. 31a ustawy z dnia 29 sierpnia 1997 r. o ochronie danych osobowych:
.....
.....
(nazwa przedstawiciela administratora danych i adres jego siedziby lub nazwisko, imię i adres miejsca zamieszkania)

3. Powierzenie przetwarzania danych osobowych:
   * ☐ — administrator danych powierzył w drodze umowy zawartej na piśmie przetwarzanie danych innemu podmiotowi (art. 31 ustawy z dnia 29 sierpnia 1997 r. o ochronie danych osobowych),
   * ☐ — administrator danych przewiduje powierzenie przetwarzania danych innemu podmiotowi.

   W przypadku powierzenia przetwarzania danych innemu podmiotowi, należy podać nazwę i adres siedziby lub nazwisko, imię i adres miejsca zamieszkania podmiotu, któremu powierzono przetwarzanie danych osobowych:
.....
.....
..... * ☐ *ew. cd. w załączniku nr* .....

4. Podstawa prawna upoważniająca do prowadzenia zbioru danych:
   * ☐ — zgoda osoby, której dane dotyczą, na przetwarzanie danych jej dotyczących,
   * ☐ — przetwarzanie jest niezbędne do zrealizowania uprawnienia lub spełnienia obowiązku wynikającego z przepisu prawa —
.....
.....
..... * ☐ *ew. cd. w załączniku nr* .....

Część E. Opis środków technicznych i organizacyjnych zastosowanych w celach określonych w art. 36—39 ustawy z dnia 29 sierpnia 1997 r. o ochronie danych osobowych

15. Zbiór danych osobowych jest prowadzony:

a) *☐ — centralnie,
*☐ — w architekturze rozproszonej,

b) *☐ — wyłącznie w postaci papierowej,
*☐ — z użyciem systemu informatycznego,

c) *☐ — z użyciem co najmniej jednego urządzenia systemu informatycznego służącego do przetwarzania danych osobowych połączonego z siecią publiczną (np. Internetem),
*☐ — bez użycia żadnego z urządzeń systemu informatycznego służącego do przetwarzania danych osobowych połączonego z siecią publiczną (np. Internetem).

16. Zostały spełnione wymogi określone w art. 36—39 ustawy z dnia 29 sierpnia 1997 r. o ochronie danych osobowych[1]:

a) *☐ — został wyznaczony administrator bezpieczeństwa informacji nadzorujący przestrzeganie zasad ochrony przetwarzanych danych osobowych,
*☐ — administrator danych sam wykonuje czynności administratora bezpieczeństwa informacji,

b) *☐ — do przetwarzania danych zostały dopuszczone wyłącznie osoby posiadające upoważnienie nadane przez administratora danych,

c) *☐ — prowadzona jest ewidencja osób upoważnionych do przetwarzania danych,

d) *☐ — została opracowana i wdrożona polityka bezpieczeństwa,

e) *☐ — została opracowana i wdrożona instrukcja zarządzania systemem informatycznym,

f) inne środki, oprócz wymienionych w ppkt a—e, zastosowane w celu zabezpieczenia danych:

.....

.....

..... *☐ *ew. cd. w załączniku nr* .....

Część F. Informacja o sposobie wypełnienia warunków technicznych i organizacyjnych, o których mowa w rozporządzeniu 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)

17. Zastosowano środki bezpieczeństwa na poziomie[2]:

*☐ — podstawowym,
*☐ — podwyższonym,
*☐ — wysokim.

.....
(data, podpis i pieczęć wnioskodawcy)

Objaśnienia:

* W przypadku odpowiedzi twierdzącej należy zakreślić kwadrat literą „X".

[1] Administrator danych prowadzący zbiór w systemie tradycyjnym (papierowym) zobowiązany jest do zastosowania środków określonych w pkt 16 ppkt a—d, a w przypadku prowadzenia zbioru w systemie informatycznym, ponadto środka określonego w pkt 16 ppkt e.

[2] Należy wskazać odpowiedni poziom bezpieczeństwa określony w § 6 ww. rozporządzenia (UWAGA! Dotyczy wyłącznie administratorów przetwarzających dane w systemie informatycznym):
— jeżeli wnioskodawca przetwarza dane wymienione w pkt 9 zgłoszenia, należy zastosować środki bezpieczeństwa przynajmniej na poziomie podwyższonym;
— w przypadku gdy przynajmniej jedno urządzenie systemu informatycznego służącego do przetwarzania danych osobowych połączone jest z siecią publiczną, należy zastosować środki bezpieczeństwa na poziomie wysokim;
— w pozostałych przypadkach wystarczające jest zastosowanie środków bezpieczeństwa na poziomie podstawowym.

Zgłoszenia można dokonać drogą elektroniczną, za pomocą programu komputerowego umożliwiającego jego prawidłowe wypełnienie, dostępnego na stronie internetowej Generalnego Inspektora Ochrony Danych Osobowych.

10. Podstawa prawna przetwarzania danych wskazanych w pkt 9:

*☐ — osoby, których dane dotyczą, będą wyrażać na to zgodę na piśmie,

*☐ — przepis szczególny innej ustawy zezwala na przetwarzanie bez zgody osoby, której dane dotyczą, jej danych osobowych — *w przypadku odpowiedzi twierdzącej, należy podać odniesienie do przepisu tej ustawy:*

.....

.....

..... *☐ *ew. cd. w załączniku nr* .....

*☐ — przetwarzanie danych jest niezbędne do ochrony żywotnych interesów osoby, której dane dotyczą, lub innej osoby, gdy osoba, której dane dotyczą, nie jest fizycznie lub prawnie zdolna do wyrażenia zgody, do czasu ustanowienia opiekuna prawnego lub kuratora,

*☐ — przetwarzanie jest niezbędne do wykonania statutowych zadań kościoła, innego związku wyznaniowego, stowarzyszenia, fundacji lub innej niezarobkowej organizacji lub instytucji o celach politycznych, naukowych, religijnych, filozoficznych lub związkowych, a przetwarzanie danych dotyczy wyłącznie członków tej organizacji lub instytucji albo osób utrzymujących z nią stałe kontakty w związku z jej działalnością i zapewnione są pełne gwarancje ochrony przetwarzanych danych — *w przypadku odpowiedzi twierdzącej, należy podać, jakich:*

.....

.....

..... *☐ *ew. cd. w załączniku nr* .....

*☐ — przetwarzanie dotyczy danych, które są niezbędne do dochodzenia praw przed sądem,

*☐ — przetwarzanie jest niezbędne do wykonania zadań administratora danych odnoszących się do zatrudnienia pracowników i innych osób, a zakres przetwarzanych danych jest określony w ustawie,

*☐ — przetwarzanie jest prowadzone w celu ochrony stanu zdrowia, świadczenia usług medycznych lub leczenia pacjentów przez osoby trudniące się zawodowo leczeniem lub świadczeniem innych usług medycznych, zarządzania udzielaniem usług medycznych i są stworzone pełne gwarancje ochrony danych osobowych,

*☐ — przetwarzanie dotyczy danych, które zostały podane do wiadomości publicznej przez osobę, której dane dotyczą,

*☐ — przetwarzanie jest niezbędne do prowadzenia badań naukowych, w tym do przygotowania rozprawy wymaganej do uzyskania dyplomu ukończenia szkoły wyższej lub stopnia naukowego, a publikowanie wyników badań naukowych uniemożliwia identyfikację osób, których dane zostały przetworzone,

*☐ — przetwarzanie danych jest prowadzone przez stronę w celu realizacji praw i obowiązków wynikających z orzeczenia wydanego w postępowaniu sądowym lub administracyjnym.

Część D. Sposób zbierania oraz udostępniania danych

11. Dane do zbioru będą zbierane:

*☐ — od osób, których dotyczą,

*☐ — z innych źródeł niż osoba, której dane dotyczą.

12. Dane ze zbioru będą udostępniane:

*☐ — podmiotom innym niż upoważnione na podstawie przepisów prawa.

13. Odbiorcy lub kategorie odbiorców, którym dane mogą być przekazywane — *należy podać nazwę i adres siedziby lub nazwisko, imię i adres miejsca zamieszkania odbiorcy danych:*

.....

.....

..... *☐ *ew. cd. w załączniku nr* .....

14. Informacja dotycząca ewentualnego przekazywania danych do państwa trzeciego — *należy podać nazwę państwa:*

.....

.....

..... *☐ *ew. cd. w załączniku nr* .....

*☐ — przetwarzanie jest konieczne do realizacji umowy, gdy osoba, której dane dotyczą, jest jej stroną lub gdy jest to niezbędne do podjęcia działań przed zawarciem umowy na żądanie osoby, której dane dotyczą,

*☐ — przetwarzanie jest niezbędne do wykonania określonych prawem zadań realizowanych dla dobra publicznego — *w przypadku odpowiedzi twierdzącej, należy opisać te zadania:*

.....

.....

..... *☐ *ew. cd. w załączniku nr* .....

*☐ — przetwarzanie jest niezbędne do wypełnienia prawnie usprawiedliwionych celów realizowanych przez administratorów danych albo odbiorców danych, a przetwarzanie nie narusza praw i wolności osoby, której dane dotyczą.

Część C. Cel przetwarzania danych, opis kategorii osób, których dane dotyczą, oraz zakres przetwarzanych danych

5. Cel przetwarzania danych w zbiorze:

.....

.....

.....*☐ *ew. cd. w załączniku nr* .....

6. Opis kategorii osób, których dane dotyczą:

.....

.....

.....

7. Zakres przetwarzanych w zbiorze danych o osobach:

*☐ — nazwiska i imiona,
*☐ — imiona rodziców,
*☐ — data urodzenia,
*☐ — miejsce urodzenia,
*☐ — adres zamieszkania lub pobytu,
*☐ — numer ewidencyjny PESEL,
*☐ — Numer Identyfikacji Podatkowej,
*☐ — miejsce pracy,
*☐ — zawód,
*☐ — wykształcenie,
*☐ — seria i numer dowodu osobistego,
*☐ — numer telefonu.

8. Inne dane osobowe, oprócz wymienionych w pkt 7, przetwarzane w zbiorze — *należy podać, jakie:*

.....

.....

..... *☐ *ew. cd. w załączniku nr* .....

9. Dane przetwarzane w zbiorze:

a) ujawniają bezpośrednio lub w kontekście:

*☐ — pochodzenie rasowe,
*☐ — pochodzenie etniczne,
*☐ — poglądy polityczne,
*☐ — przekonania religijne,
*☐ — przekonania filozoficzne,
*☐ — przynależność wyznaniową,
*☐ — przynależność partyjną,
*☐ — przynależność związkową,
*☐ — stan zdrowia,
*☐ — kod genetyczny,
*☐ — nałogi,
*☐ — życie seksualne,

b) dotyczą:

*☐ — skazań,
*☐ — mandatów karnych,
*☐ — orzeczeń o ukaraniu,
*☐ — innych orzeczeń wydanych w postępowaniu sądowym lub administracyjnym.

Jeśli nie zakreślono żadnej odpowiedzi, należy przejść do pkt 11.

Załącznik nr 4 do polityki bezpieczeństwa

Szczegółowy wykaz pomieszczeń w którym przetwarzane są dane osobowe

Nr pomieszczenia	Osoby edytujące dane, mające wgląd do danych osobowych i ich edycji *Imię i nazwisko*
Osoby mające prawo wglądu do danych osobowych w kartotekach z uwagi na wykonywane zakresy czynności	
Administrator danych	
Pokój nr 11a	- Stefan Jakubowski
Zastępca Wójta	
Pokój nr 11b	- Leonarda Luśniewska
Administrator Bezpieczeństwa Informacji	
Pokój nr 2b	- Marek Kroczewski
Radca Prawny	
Pokój nr 11c	- Henryk Jastrzębski
Referat Organizacyjny i Zarządzania Kryzysowego	
Pokój nr 1	- Elżbieta Sarnowska - Janusz Salamon
Pokój nr 11	- Barbara Świderska
Pokój nr 11c	- Sylwia Pomianowska
Referat Rolnictwa, Budownictwa i Gospodarki Komunalnej	
Pokój nr 2	- Izabela Borowska - Małgorzata Matusiak
Pokój nr 2a	- Danuta Gierwatowska
Pokój nr 6	- Joanna Wereszczyńska - Dominika Ogieniewska
Pokój nr 7	- Teresa Majewska - Zofia Szamel
Pokój nr 10	- Michał Kolasiński
Referat Planowania i Finansów	
Pokój nr 8	- Ewa Natkowska - Sabina Lewandowska - Konrad Masiukiewicz
Pokój nr 12a	- Elżbieta Syrkowska
Pokój nr 12b	- Barbara Michałowska - Aldona Jasińska - Aleksandra Gołębiewska - Maciej Szostek
USC i referat Spraw Obywatelskich	
Pokój nr 9a	- Ala Górecka - Nina Lewandowska
Pokój nr 9b	- Barbara Malinowska
Samodzielne Stanowiska Pracy	
Pokój nr 2b	- Marek Kroczewski
Pokój nr 10	- Emilia Adamkowska
Pokój nr 11c	- Joanna Ziółkiewicz

Załącznik Nr 5 do „Polityki bezpieczeństwa"

WYKAZ ZBIORÓW DANYCH OSOBOWYCH PRZETWARZANYCH W URZĘDZIE GMINY W SŁUPNIE

Lp.	Nazwy zbiorów	Numer zgłoszenia	Nr księgi
1	REJESTR PODAŃ I ZAŚWIADCZEŃ	044038/1999	041286
2	WYKAZ ODBIORCÓW WODY	044043/1999	041272
3	REJESTR DECYZJI O WARUNKACH ZABUDOWY I ZAGOSPODAROWANIA TERENU	044060/1999	031662
4	REJESTR NAJEMCÓW LOKALI MIESZKALNYCH	044067/1999	041293
5	URZĄD STANU CYWILNEGO	044073/1999	041264
6	DOWODY OSOBISTE – KOPERTY DOWODOWE	044083/1999	041266
7	EWIDENCJA LUDNOŚCI	044090/1999	045304
8	REJESTR PODATNIKÓW ŁĄCZNEGO ZOBOWIĄZANIA PIENIĘŻNEGO	044095/1999	041256
9	REJESTR SKARG I WNIOSKÓW	044100/1999	041288
10	REJESTR PODATNIKÓW PODATKU OD ŚRODKÓW TRANSPORTOWYCH	044143/1999	041292
11	EWIDENCJA POJAZDÓW I KIEROWCÓW	044151/1999	041290
12	WNIOSKODAWCY STYPENDIÓW SZKOLNYCH	004690/2005	070942
13	INFORMACJE OŚWIATOWE	004691/2005	070960

Załącznik Nr 6 do „ Polityki bezpieczeństwa"

OPIS STRUKTUR ZBIORÓW DANYCH.

Zbiór danych REJESTR PODAŃ I ZAŚWIADCZEŃ zawiera następujące pola:

• nazwiska i imiona
• imiona rodziców
• data urodzenia
• adres zamieszkania lub pobytu

Zbiór danych WYKAZ ODBIORCÓW WODY zawiera następujące pola:

• nazwiska i imiona
• adres zamieszkania lub pobytu

Zbiór danych REJESTR DECYZJI O WARUNKACH ZABUDOWY I ZAGOSPODAROWANIA TERENU zawiera następujące pola:

• nazwiska i imiona
• adres zamieszkania lub pobytu

Zbiór danych REJESTR NAJEMCÓW LOKALI MIESZKALNYCH zawiera pola:

• nazwiska i imiona
• adres zamieszkania lub pobytu
• seria i numer dowodu osobistego

Zbiór danych URZĄD STANU CYWILNEGO zawiera następujące pola:

• imiona i nazwiska,
• imiona i nazwiska rodowe rodziców,
• nazwisko rodowe, z poprzedniego małżeństwa
• data urodzenia,
• miejsce urodzenia,
• numer PESEL,
• płeć,
• adres zamieszkania lub pobytu
• seria i numer dowodu osobistego
• stan cywilny
• numer aktu stanu cywilnego
• nazwiska i imiona świadków
• data, godzina oraz miejsce zgonu lub znalezienia zwłok
• nazwisko, imię i miejsce zamieszkania osoby zgłaszającej zgon

Zbiór danych DOWODY OSOBISTE - KOPERTY DOWODOWE zawiera pola:

• nazwiska i imiona
• imiona rodziców
• nazwiska rodowe rodziców
• nazwisko rodowe i z poprzedniego małżeństwa
• data urodzenia – miejsce urodzenia
• wzrost, kolor oczu
• numer ewidencyjny PESEL
• adres zamieszkania i pobytu
• seria i numer dowodu osobistego

Zbiór danych EWIDENCJA LUDNOŚCI zawiera następujące pola:

• nazwiska i imiona
• nazwisko rodowe i z poprzedniego małżeństwa,
• imiona rodziców, nazwisko rodowe matki
• data urodzenia, nr aktu i nazwa organu
• miejsce urodzenia,
• data zawarcia małżeństwa, nr aktu i nazwa organu
• numer ewidencyjny PESEL
• stan cywilny, imię i nazwisko rodowe małżonka
• adres zameldowania, obywatelstwo
• wykształcenie
• seria i numer dowodu osobistego
• obowiązki wojskowe

Zbiór danych REJESTR PODATNIKÓW ŁĄCZNEGO ZOBOWIĄZANIA PIENIĘŻNEGO zawiera następujące pola:

• nazwiska i imiona
• imiona rodziców
• adres zamieszkania lub pobytu
• numer telefonu
• numer ewidencyjny PESEL

Zbiór danych REJESTR SKARG I WNIOSKÓW zawiera następujące pola:

• nazwiska i imiona
• adres zamieszkania i pobytu

Zbiór danych REJESTR PODATNIKÓW PODATKU OD ŚRODKÓW TRANSPORTOWYCH zawiera następujące pola:

• nazwiska i imiona
• imiona rodziców
• data urodzenia
• adres zamieszkania lub pobytu
• numer ewidencyjny PESEL
• miejsce pracy
• zawód
• numer telefonu

Zbiór danych EWIDENCJA POJAZDÓW I KIEROWCÓW zawiera następujące pola:

• nazwiska i imiona
• data urodzenia
• miejsce urodzenia
• adres zamieszkania lub pobytu
• numer ewidencyjny PESEL
• numer dowodu rejestracyjnego
• numer prawa jazdy
• nazwisko imię współwłaścicieli pojazdu
• adres zamieszkania lub pobytu współwłaścicieli pojazdu

Zbiór danych WNIOSKODAWCY STYPENDIÓW SZKOLNYCH zawiera pola:

• nazwiska i imiona
• imiona rodziców
• data urodzenia
• miejsce urodzenia
• adres zamieszkania lub pobytu
• numer ewidencyjny PESEL
• Numer Identyfikacji Podatkowej
• miejsce pracy
• zawód
• wykształcenie
• seria i numer dowodu osobistego
• numer telefonu

Zbiór danych INFORMACJE OŚWIATOWE zawiera następujące pola:

• data urodzenia
• numer ewidencyjny PESEL
• miejsce pracy
• zawód
• wykształcenie

Załącznik nr 7 do polityki bezpieczeństwa

WZÓR

.....
(miejscowość, data)

.....
(imię i nazwisko)

.....
(stanowisko)

OŚWIADCZENIE

1. Stwierdzam własnoręcznym podpisem, że znana jest mi treść przepisów :
   a) o ochronie tajemnic prawnie chronionych stanowiących tajemnicę służbową wynikającą z Kodeksu Pracy,
   b) o ochronie danych osobowych wynikająca z ustawy o ochronie danych osobowych (tj Dz.U. 2002 r. Nr 101, poz.926 ze zm.) ,
   c) o odpowiedzialności karnej za naruszenie ochrony danych osobowych.

2. Zobowiązuję się nie ujawniać wiadomości, z którymi zapoznałem/am się w trakcie wykonywanych czynności służbowych .

.....
(podpis pracownika)

.....
(podpis złożono w obecności)

Załącznik nr 8 do polityki bezpieczeństwa

WZÓR

.....
pieczęć jednostki organizacyjnej z adresem

ZAŚWIADCZENIE Nr .....

stwierdzające odbycie przeszkolenia w zakresie ochrony danych osobowych

Stwierdza się, że Pan(i) :

- imię i nazwisko : .....
- data urodzenia : .....

Odbył(a) w URZĘDZIE GMINY W SŁUPNIE szkolenie w zakresie ochrony danych osobowych zgodnie z przepisami ustawy z dnia 29 sierpnia 1997r. o ochronie danych osobowych (tj. Dz. U. z 2002r. Nr 101, poz. 926 z późn. zm.) przeprowadzone przez administratora bezpieczeństwa informacji.

Słupno, dnia .....r.
miejscowość i data

.....
imienna pieczęć i podpis
administratora bezpieczeństwa informacji

Załącznik nr 9 polityki bezpieczeństwa

POZBAWIENIE PRACOWNIKA UPOWAŻNIENIA DO PRZETWARZANIA DANYCH OSOBOWYCH Z DNIA .....

Na podstawie art.37 ustawy z dnia 29 sierpnia 1997 roku o ochronie danych osobowych (tj. Dz.U. z 2002 r. nr 101, poz. 926 ze zm.) w związku z:

.....

.....

pozbawiam

Pana/nią.....

zatrudnionego/ą w Urzędzie Gminy Słupno

na stanowisku .....

upoważnienia nr ..... z dnia.....

do przetwarzania danych osobowych.

Administrator Danych Osobowych

.....

.....

(data i podpis pracownika)

Załącznik Nr 10 do „Polityki bezpieczeństwa"

WYKAZ PRACOWNIKÓW POZBAWIONYCH UPOWAŻNIEŃ DO PRZETWARZANIA DANYCH OSOBOWYCH W URZĘDZIE GMINY SŁUPNO

Lp.	Data cofnięcia upoważnienia	Imię i nazwisko/ stanowisko	Numer upoważnienia	Przyczyna cofnięcia upoważnienia	Podpis ABI

Załącznik Nr 11 do „Polityki bezpieczeństwa „

WZÓR

R a p o r t
z naruszenia bezpieczeństwa danych osobowych w Urzędzie.....

1. Data: ..... godzina: .....
(dd.mm.rrrr) *(00:00)*

2. Osoba powiadamiająca o zaistniałym zdarzeniu:

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

3. Lokalizacja zdarzenia:

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

4. Rodzaj naruszenia bezpieczeństwa oraz okoliczności towarzyszące:

.....
.....

5. Podjęte działania:

.....
.....

6. Przyczyny wystąpienia zdarzenia:

.....
.....

7. Postępowanie wyjaśniające:

.....
.....

.....
data, podpis Administratora Bezpieczeństwa Informacji