Zarządzenie Nr 46/2011
Wójta Gminy Białogard
z dnia 30 września 2011 r.

w sprawie ustalenia Polityki bezpieczeństwa i Instrukcji zrządzania systemem informatycznym służącym do przetwarzania danych osobowych w Urzędzie Gminy Białogard

Na podstawie art. 36 ustawy z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (Dz. U. z 2002 r. Nr 101, poz. 926 ze zm.) oraz na § 3 rozporządzenia Ministra Spraw Wewnętrznych i Administracji z dnia 29 kwietnia 2004 r. w sprawie dokumentacji przetwarzania danych osobowych oraz warunków technicznych i organizacyjnych jakim powinny odpowiadać urządzenia i systemy informatyczne służące do przetwarzania danych osobowych (Dz. U. Nr 100, poz. 1024), zarządza się co następuje:

§ 1. 1. Ustala się, Politykę bezpieczeństwa przetwarzania danych osobowych w Urzędzie Gminy Białogard, zwaną dalej „Polityką bezpieczeństwa" stanowiącą załącznik Nr 1 do niniejszego zarządzenia.
2. Ustala się Instrukcję zarządzania systemem informatycznym służącym do przetwarzania danych osobowych w Urzędzie Gminy Białogard, zwaną dalej „Instrukcją zarządzania systemem informatycznym" stanowiącą załącznik Nr 2 do niniejszego zarządzenia

§ 2. Zobowiązuje się pracowników Urzędu do stosowania zasad określonych w Polityce bezpieczeństwa i w Instrukcji zarządzania systemem informatycznym.

§ 3. 1. Wykonanie zarządzenia powierza się Administratorowi Bezpieczeństwa Informacji.
2. Nadzór nad wykonaniem zarządzenia powierza się Sekretarzowi Gminy Białogard.

§ 4. Zarządzenie wchodzi w życie z dniem podjęcia.

WÓJT
Maciej Niechciał

RADCA PRAWNY
Waldemar Bleczyc
KO 354/91

Załącznik Nr 1
do Zarządzenia Nr 46 /2011
Wójta Gminy Białogard
z dnia 30 września 2011 r.

POLITYKA BEZPIECZEŃSTWA PRZETWARZANIA DANYCH OSOBOWYCH W URZĘDZIE GMINY BIAŁOGARD

Zatwierdził (data i podpis):

WÓJT

30.09.2011

.....

Maciej Niechciał

Dokumenty powiązane:

Instrukcja zarządzania systemem informatycznym służącym do przetwarzania danych osobowych w Urzędzie Gminy Białogard.

132

SPIS TREŚCI

133

Rozdział 1
Postanowienia ogólne

§ 1. 1. Polityka bezpieczeństwa przetwarzania danych osobowych w Urzędzie Gminy Białogard, zwana dalej „Polityką", ustala reguły bezpieczeństwa danych osobowych przetwarzanych w Urzędzie Gminy Białogard.

2. Celem Polityki jest stworzenie podstaw dla właściwego wykonania obowiązków Administratora Danych Osobowych w zakresie zabezpieczenia i prawidłowej ochrony przetwarzanych danych osobowych.

3. Polityka określa zasady przetwarzania danych osobowych oraz ich zabezpieczania, jako zestaw praw, reguł i zaleceń, regulujących sposób zarządzania, ochrony i dystrybucji danych osobowych wewnątrz Urzędu Gminy Białogard.

4. Polityka zawiera informacje dotyczące rozpoznawania procesów przetwarzania danych osobowych oraz wprowadzonych zabezpieczeń technicznych i organizacyjnych, zapewniających ochronę przetwarzanych danych osobowych.

5. Politykę niniejszą stosuje się do:

1) danych osobowych:

a) przetwarzanych w systemach informatycznych,

b) zapisanych na zewnętrznych nośnikach informacji,

c) przetwarzanych tradycyjnie.

2) informacji dotyczących bezpieczeństwa przetwarzania danych osobowych:

a) służących do uwierzytelnienia w systemach informatycznych, w których są przetwarzane dane osobowe,

b) dotyczących wdrożonych zabezpieczeń technicznych i organizacyjnych.

6. Obowiązek przestrzegania zasad określonych w niniejszej Polityce oraz w dokumentach powiązanych ciąży na wszystkich - bez względu na zajmowane stanowisko, miejsce wykonywanej pracy oraz charakter stosunku pracy - pracownikach Urzędu oraz w niezbędnym zakresie na użytkownikach zewnętrznych przetwarzających dane osobowe, których administratorem jest Gmina Białogard.

7. Stosowanie zasad Polityki ma zapewnić właściwą reakcję, ocenę, udokumentowanie przypadków naruszenia bezpieczeństwa systemów i właściwy tryb działania mający na celu zapewnienie bezpieczeństwa danych przetwarzanych w systemach informatycznych Urzędu Gminy Białogard.

§ 2. Zawarte w Polityce pojęcia są wspólne dla wszystkich powiązanych z niniejszą Polityką dokumentów, które zostały przyjęte przez Urząd Gminy Białogard, w zakresie ochrony danych osobowych. Ilekroć w Polityce jest mowa o:

1) Administratorze Danych Osobowych (ADO) - rozumie się przez to podmiot, decydujący o środkach i celach przetwarzania danych osobowych - Wójta Gminy Białogard;

2) Administratorze Bezpieczeństwa Informacji (ABI) - rozumie się przez to wyznaczoną przez ADO osobę, odpowiedzialną 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) Administratorze Systemów Informatycznych (ASI)- rozumie się przez to wyznaczoną przez ADO osobę, odpowiedzialną za funkcjonowanie infrastruktury informatycznej, składającej się ze sprzętu informatycznego, systemów i aplikacji informatycznych, oraz za ich przeglądy, konserwację oraz za stosowanie technicznych i organizacyjnych środków bezpieczeństwa w systemach informatycznych;
4) bezpieczeństwie przetwarzania danych osobowych - rozumie się przez to zachowanie poufności, integralności i rozliczalności danych osobowych;
5) danych osobowych - rozumie się przez to każdą informację dotyczącą żyjącej osoby fizycznej, która pozwala na bezpośrednią lub pośrednią identyfikację tej osoby;
6) GIODO - rozumie się przez to Generalnego Inspektora Ochrony Danych Osobowych;
7) haśle (Password) – rozumie się przez to ciąg znaków literowych, cyfrowych lub innych, znany jedynie użytkownikowi - osobie uprawnionej do pracy w systemie informatycznym;
8) identyfikatorze (LOGIN) – rozumie się przez to ciąg znaków literowych, cyfrowych lub innych, jednoznacznie identyfikujący osobę upoważnioną do przetwarzania danych osobowych w systemie informatycznym;
9) integralności danych - rozumie się przez to właściwość zapewniającą, że dane nie zostały zmienione lub zniszczone w sposób nieautoryzowany;
10) naruszeniu ochrony danych osobowych - rozumie się przez to zamierzone lub przypadkowe naruszenie zastosowanych w celu ochrony danych osobowych środków technicznych i organizacyjnych;
11) poufności - rozumie się przez to właściwość zapewniającą, że informacja – dane osobowe jest dostępna jedynie osobom upoważnionym;
12) przetwarzaniu danych osobowych - rozumie się przez to jakiekolwiek operacje wykonywane na danych osobowych, takie jak zbieranie, utrwalanie, przechowywanie, opracowywanie, zmienianie, udostępnianie i usuwanie, zwłaszcza wykonywane w systemach informatycznych;
13) rozporządzeniu - rozumie się przez to 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);
14) rozliczalności - rozumie się przez to właściwość zapewniającą, że działania podmiotu mogą być przypisane w sposób jednoznaczny tylko temu podmiotowi;
15) systemie informatycznym - rozumie się przez to system przetwarzania informacji wraz ze związanymi z nim ludźmi oraz z zasobami technicznymi i finansowymi, dostarczający i rozprowadzający informacje, inaczej: zespół współpracujących urządzeń, programów, procedur przetwarzania informacji i narzędzi programowych zastosowanych w celu przetwarzania danych;
16) Urzędzie - rozumie się przez to Urząd Gminy Białogard;
17) ustawie - rozumie się przez to ustawę o ochronie danych osobowych z dnia 29 sierpnia 1997 r. (Dz. U. z 2002 r. Nr 101, poz. 926 ze zm.);
18) użytkowniku danych osobowych- rozumie się przez to pracownika upoważnionego do bezpośredniego dostępu do przetwarzanych danych osobowych, posiadającego ustalony identyfikator i hasło; odpowiedzialnego za ochronę danych osobowych przetwarzanych w podległej komórce; użytkownik zobowiązany jest do stosowania środków technicznych

i organizacyjnych zapewniających ochronę przetwarzanych danych odpowiednią do zagrożeń oraz kategorii danych objętych ochroną, w szczególności do zabezpieczenia danych przed ich udostępnieniem osobom nieupoważnionym, zabraniem przez osobę nieuprawnioną, przetwarzaniem z naruszeniem ustawy o ochronie danych osobowych oraz przed nieautoryzowaną zmianą, utratą, uszkodzeniem lub zniszczeniem;

19) użytkowniku zewnętrznym - rozumie się przez to osobę nie będącą pracownikiem lub stażystą zatrudnionym w Urzędzie Gminy Białogard, posiadającą uprawnienia do przetwarzania informacji w związku z wykonywaniem czynności na rzecz Urzędu;
20) zbiorze danych osobowych - rozumie się przez to każdy posiadający strukturę zestaw danych o charakterze osobowym, dostępnych według określonych kryteriów, niezależnie od tego, czy zestaw ten jest rozproszony czy podzielony funkcjonalnie;
21) zbiorze nieinformatycznym - rozumie się przez to 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. 1. Niniejsza Polityka i dokumenty z nią powiązane podlegają aktualizacji stosownie do zmian w przepisach prawa i zmian w ramach Urzędu Gminy, powodujących nieaktualność lub nieadekwatność ww. dokumentów.

2. ABI i ASI co najmniej jeden raz w roku dokonują przeglądu Polityki i dokumentów powiązanych w celu stwierdzenia, czy postanowienia Polityki i dokumentów odpowiadają aktualnej i planowanej działalności Gminy oraz stanowi prawnemu obowiązującemu w czasie dokonywania przeglądu.

3. Wystąpienie poważnych naruszeń ochrony danych osobowych skutkuje koniecznością wprowadzenia zmian w niniejszej Polityce i w dokumentach powiązanych.

§ 4. Dokumentacja ochrony danych osobowych w Urzędzie Gminy Białogard składa się z:

1) wykazu budynków, pomieszczeń lub części pomieszczeń tworzących obszar, w którym przetwarzane są dane osobowe (zał. Nr 1 do niniejszej instrukcji);
2) ewidencji osób upoważnionych przez ADO do przetwarzania danych osobowych. (wzór - zał. Nr 2), prowadzonej przez ABI;
3) ewidencji zbiorów danych osobowych przetwarzanych w Urzędzie Gminy Białogard oraz programów zastosowanych do ich przetwarzania (wzór - zał. Nr 3), prowadzonej przez ABI;
4) opisów struktur zbiorów danych osobowych, prowadzonych przez ASI (wzór - zał. Nr 4);
5) opisu sposobów przepływu danych pomiędzy systemami prowadzonego przez ASI (wzór - zał. Nr 5);
6) zbiorów oryginałów i kopii dokumentów dotyczących ochrony danych osobowych (w tym kopii kierowanych do GIODO wniosków o rejestrację/aktualizacje zbiorów danych osobowych, uchwał, zarządzeń, polityki itd. dotyczących ochrony danych osobowych), prowadzonych przez ABI;
7) zbioru protokołów z przeprowadzonych w zakresie ochrony danych osobowych kontroli wewnętrznych i zewnętrznych, prowadzonego przez ABI;
8) ewidencji przenośnych nośników danych używanych w poszczególnych komórkach

organizacyjnych i na stanowiskach samodzielnych, prowadzonej przez ASI (wzór - zał. Nr 6).

Rozdział 2
Zadania Administratora Danych Osobowych

§ 5. 1. Administrator Danych Osobowych jest odpowiedzialny za przetwarzanie i ochronę danych osobowych zgodnie z przepisami prawa, w tym za stosowanie procedur postępowania zapewniających prawidłowe przetwarzanie danych osobowych - rozumiane jako ochronę danych przed ich udostępnieniem osobom nieupoważnionym, zmianą lub zabraniem danych przez osobę nieuprawnioną, przetwarzaniem z naruszeniem obowiązujących przepisów oraz utratą, uszkodzeniem lub zniszczeniem.

2. Do kompetencji ADO należy w szczególności:

1) wyznaczenie ABI i ASI;
2) wyznaczanie użytkowników danych osobowych;
3) określenie celów i strategii ochrony danych osobowych;
4) podział zadań i obowiązków związanych z organizacją ochrony danych osobowych.

3. Do obowiązków ADO należy:

1) zapewnienie środków finansowych na organizowanie szkoleń dla pracowników w zakresie ochrony danych osobowych i zagrożeń związanych z ich przetwarzaniem;
2) zapewnienie prowadzenia niezbędnej, określonej przepisami prawa dokumentacji w zakresie ochrony danych osobowych;
3) nadawanie pracownikom Urzędu oraz użytkownikom zewnętrznym upoważnień 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.

Rozdział 3
Zadania Administratora Bezpieczeństwa Informacji

§ 6. 1. ADO wyznacza ABI nadzorującego przestrzeganie zasad ochrony danych osobowych w systemach informatycznych i w zbiorach danych osobowych prowadzonych w formie papierowej i elektronicznej.

2. Do kompetencji ABI należy:

1) określenie zasad ochrony danych osobowych;
2) wnioskowanie o ukaranie osób winnych naruszenia przepisów i zasad dotyczących ochrony danych osobowych.

3. Do obowiązków ABI należy:

1) nadzór nad wdrożeniem stosownych środków organizacyjnych, technicznych i fizycznych w celu ochrony przetwarzanych danych osobowych;

2) nadawanie, zmienianie oraz cofanie upoważnień do przetwarzania danych osobowych po akceptacji ADO dla pracowników oraz użytkowników zewnętrznych;
3) prowadzenie ewidencji upoważnień, o których mowa w § 4 pkt. 3;
4) nadzór nad zapewnieniem przez ASI dostosowania funkcjonalności systemów przetwarzających dane osobowe do wymagań prawem określonych;
5) prowadzenie dokumentacji zawierającej opis stosowanej ochrony danych osobowych (niniejsza Polityka oraz wynikające z niej instrukcje i procedury) w tym zapewnienie ich publikacji i dystrybucji, prowadzenia dokumentacji, o której mowa w § 4 w zakresie ABI
6) zapoznawanie pracowników oraz współpracowników Urzędu Gminy z przepisami i zasadami ochrony danych osobowych oraz informowanie o zagrożeniach związanych z ich przetwarzaniem;
7) reprezentowanie Gminy w kontaktach z GIODO;
8) reagowanie na zgłaszane incydenty związane z naruszeniem ochrony danych osobowych, analizowanie ich przyczyn, kierowanie wniosków dotyczących ukarania winnych naruszeń;
9) kontrola wypełnienia obowiązków technicznych i organizacyjnych związanych z ochroną danych osobowych.

4. Realizując powierzone obowiązki ABI ma prawo do żądania od wszystkich pracowników Urzędu, natychmiastowej pomocy w razie stwierdzenia, że doszło do naruszenia przepisów o ochronie danych osobowych.

Rozdział 4
Zadania Administratora Systemów Informatycznych

§ 7. 1. Funkcję ASI pełni pracownik wyznaczony przez ADO.
2. Do kompetencji ASI należy:
1) zabezpieczenie systemów przetwarzania danych osobowych zgłoszonych ASI, w zależności i od kategorii przetwarzanych w tym systemie danych;
2) zapewnienie poufności, integralności, dostępności i rozliczalności danych przetwarzanych w systemach informatycznych.
3. Do obowiązków ASI należy:
1) bieżący nadzór oraz zapewnianie optymalnej ciągłości działania systemu informatycznego,
2) reagowanie bez zbędnej zwłoki, w przypadku naruszenia bądź powstania zagrożenia naruszenia bezpieczeństwa danych osobowych;
3) przeciwdziałanie próbom naruszenia bezpieczeństwa danych osobowych;
4) analiza raportów wszelkich zdarzeń, w tym incydentów związanych z naruszeniem bezpieczeństwa systemów przetwarzania danych;
5) zapewnienie zgodności wszystkich wdrażanych systemów przetwarzania danych osobowych z obowiązującymi przepisami prawa, w tym z niniejszą Polityką i Instrukcją Zarządzania Systemem Informatycznym;
6) instalacja i konfiguracja lub nadzór nad instalacją i konfiguracją oprogramowania, sprzętu sieciowego i serwerowego używanego do przetwarzania danych osobowych;
7) konfiguracja i administracja oprogramowania systemowego i sieciowego zabezpieczającego dane osobowe przed nieupoważnionym dostępem;
8) wykonywanie czynnościami związanych ze sprawdzaniem systemu pod kątem obecności

szkodliwego oprogramowania;
9) nadzór nad naprawami, konserwacją oraz likwidacją urządzeń komputerowych, na których zapisane są dane osobowe;
10) przyznawanie na wniosek właściciela zasobów, za zgodą ADO i po zatwierdzeniu przez ABI ściśle określonych praw dostępu do danych osobowych w danym systemie;
11) świadczenie pomocy technicznej w ramach oprogramowania, serwis pozostającego na wyposażeniu Urzędu sprzętu komputerowego, służącego do przetwarzania danych osobowych;
12) diagnozowanie i usuwanie awarii sprzętu komputerowego, realizacja umów z firmami świadczącymi usługi napraw pogwarancyjnych sprzętu komputerowego;
13) sporządzanie, zarządzanie i archiwizacja kopii zapasowych, oprogramowania systemowego (w tym danych osobowych oraz zasobów umożliwiających ich przetwarzanie) i sieciowego;
14) przygotowywanie i przechowywanie dokumentacji, o której mowa w § 4 należącej do zakresu zadań ASI;
15) nadzór nad wdrożeniem i zarządzanie aplikacjami (przeglądanie, nadawanie i odbieranie uprawnień użytkownikom, itp.), w których przetwarzane są dane osobowe;
16) przygotowywanie zgłoszeń do rejestracji zbiorów danych osobowych w Biurze GIODO (części E i F wniosku);
17) umożliwienie przeprowadzenia kontroli systemu informatycznego przez służby Biura GIODO.

Rozdział 5
Zadania użytkowników danych osobowych i użytkowników zewnętrznych

§ 8. 1. ADO wyznacza użytkowników danych osobowych, którzy są odpowiedzialni za ochronę im przypisanych i przetwarzanych zbiorów danych osobowych.

2. Do kompetencji użytkowników 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 użytkowników danych osobowych należy:
1) określenie podstaw prawnych przetwarzania danych osobowych, od chwili zebrania danych osobowych do chwili ich usunięcia;
2) zapewnienie aktualności, adekwatności oraz merytorycznej poprawności przetwarzanych danych osobowych;
3) realizacja obowiązku informowania osób, których dane osobowe są pozyskiwane o celu przetwarzania danych osobowych;
4) udostępnianie na żądanie uprawnionych osób informacji o przetwarzanych danych osobowych oraz podmiotach, którym zostały one udostępnione;
5) realizacja obowiązku złożenia oświadczenia o znajomości przepisów o ochronie danych osobowych oraz zobowiązania do zachowania w tajemnicy danych osobowych oraz informacji na temat zabezpieczania danych osobowych;

6) realizacja obowiązku uzyskania formalnego upoważnienia do przetwarzania danych osobowych;
7) ustalenie w przypadku utworzenia nowego zbioru danych osobowych kogo dotyczą dane osobowe, jaki jest ich zakres (np. imię i nazwisko, adres zamieszkania, NIP, PESEL itp.), cel przetwarzania oraz komu
dane osobowe mają być udostępniane;
8) przekazanie informacji, o których mowa w pkt.7 ABI i ASI;
9) przygotowanie wniosku do rejestracji/zmiany zbioru do GIODO - części A-D.

§ 9. 1. Użytkownicy danych osobowych i użytkownicy zewnętrzni są zobowiązani do bezpośredniego informowania ABI o wszelkich podejrzeniach naruszenia lub zauważonych naruszeniach i słabościach systemu przetwarzającego dane osobowe.
2. Użytkownicy danych i 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;
5) przestrzegania procedur związanych z otwieraniem i zamykaniem pomieszczeń, a także z wejściem do obszarów przetwarzania danych osobowych osób nieupoważnionych;
6) informowania ABI o naruszeniach procedur, o których mowa w pkt.1.

§ 10. 1. Przed rozpoczęciem przetwarzania danych osobowych każdy użytkownik danych osobowych i użytkownik zewnętrzny podlega przeszkoleniu przez ABI. Szkolenie obejmuje 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 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 są powtarzane okresowo lub przeprowadzane na żądanie, gdy zaistnieje taka potrzeba.
3. Użytkownicy reprezentujący osoby trzecie (w przypadku zaistnienia takiej potrzeby) uczestniczą w szkoleniach 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.

§ 11. Użytkownicy danych i użytkownicy zewnętrzni w celu ochrony wymienianych informacji dotyczących danych osobowych są zobowiązani do przestrzegania w czasie przetwarzania następujących zasad:
1) zabezpieczania wymienianych danych osobowych przed przechwyceniem, kopiowaniem, modyfikacją, błędnym wyborem drogi komunikacji i zniszczeniem;
2) zabezpieczania i ograniczenia przekazywania wiadomości za pomocą środków komunikacji, np. automatycznego przekazywania poczty elektronicznej na zewnątrz;
3) nie pozostawiania informacji zawierających dane osobowe przy urządzeniach drukujących, np. kopiarkach, drukarkach, faksach, do których mogą mieć dostęp osoby nieupoważnione;
4) upewnienia się przed przekazaniem danych osobowych, czy rozmówca jest osobą upoważnioną do uzyskania określonych danych osobowych;
5) zachowania szczególnej ostrożności w czasie rozmów telefonicznych;
6) właściwego postępowania z faksami i fotokopiarkami,
7) transportowania danych osobowych w formie elektronicznej i papierowej pomiędzy obszarami, w których są przetwarzane dane osobowe przez osoby upoważnione w sposób ograniczający możliwość ich pozyskania i odczyt przez osoby nieupoważnione.

§ 12 1. Wobec użytkownika danych osobowych/użytkownika zewnętrznego, dopuszczającego 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 oraz gdy w przypadku naruszenia zabezpieczeń systemu informatycznego lub uzasadnionego domniemania takiego naruszenia nie podjął on działań określonych Polityce, a w szczególności nie powiadomił odpowiedniej osoby i nie zrealizował określonych działań, wszczyna się postępowanie dyscyplinarne.

2. Przypadki nieuzasadnionego zaniechania obowiązków wynikających z Polityki mogą być potraktowane jako ciężkie naruszenie obowiązków pracowniczych, w szczególności przez użytkownika danych, który w przypadku naruszenia zabezpieczenia systemu informatycznego lub uzasadnionego domniemania takiego naruszenia nie powiadomił o tym ABI I ASI.

3. Orzeczona kara dyscyplinarna, wobec użytkownika danych uchylającego się od powiadomienia ABI i ASI nie wyklucza odpowiedzialności karnej zgodnie z ustawą z dnia 29 sierpnia 1997 roku o ochronie danych oraz możliwości wniesienia wobec użytkownika powództwa cywilnego o zrekompensowanie poniesionych strat.

4. Sankcje dotyczące ujawnienia poufnych danych osobowych stosuje się odpowiednio do ujawnienia informacji dotyczących zabezpieczenia danych osobowych w Urzędzie.

141

Rozdział 6
Przetwarzanie danych osobowych

§ 13. 1. Dane osobowe mogą być przetwarzane wyłącznie w pomieszczeniach przetwarzania danych osobowych określonych w wykazie budynków, pomieszczeń lub części pomieszczeń tworzących obszar, w którym przetwarzane są dane osobowe.

2. Do pomieszczeń przetwarzania danych osobowych zalicza się:

1) serwerownię;
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.

3. Osoby nieuprawnione do przetwarzania danych osobowych mogą przebywać w pomieszczeniach, o których mowa w ust. 2, tylko w obecności osoby upoważnionej do przetwarzania tych danych.

4. Pomieszczenia, w których przetwarzane są dane osobowe, powinny być zamykane w czasie nieobecności osób upoważnionych do przetwarzania danych osobowych, w sposób uniemożliwiający dostęp osobom nieupoważnionym.

5. Nośniki elektroniczne zawierające dane osobowe należy przechowywać w zamykanych szafach i szufladach, znajdujących się w obszarach przetwarzania danych osobowych.

6. Każdorazowe naruszenie zabezpieczeń fizycznych chroniących dane osobowe powinno być zgłaszane do ABI.

§ 14. 1 Przetwarzanie danych osobowych jest możliwe wyłącznie po uzyskaniu przez użytkownika danych/użytkownika zewnętrznego wystawionego przez ABI formalnego upoważnienia do przetwarzania danych osobowych zatwierdzonego przez ADO.

2. Celem uzyskania upoważnienia użytkownik danych/użytkownik zewnętrzny:

1) zapoznaje się z przepisami dotyczącymi ochrony danych osobowych i uregulowaniami wewnętrznymi obowiązującymi w Urzędzie;
2) składa ABI podpisane zobowiązanie dotyczące. zachowania danych osobowych i sposobów ich zabezpieczania w tajemnicy, oświadczenie o zobowiązaniu się do przetwarzania danych osobowych zgodnie z obowiązującymi przepisami oraz oświadczenie o znajomości Polityki i „Instrukcji zarządzania systemem informatycznym służącym do przetwarzania danych osobowych w Urzędzie'(wzór - zał. Nr 7);
3) kieruje do ABI za pośrednictwem kierownika referatu lub bezpośredniego przełożonego wniosek (wzór zał. Nr 8) w sprawie udzielenia upoważnienia do przetwarzania danych osobowych (wzór- zał. Nr 9).

3. Oświadczenia i upoważnienia, o których mowa w ust. 1 przechowuje się w aktach osobowych pracownika.

4. Niezwłocznie po ustaniu potrzeby przetwarzania danych osobowych kierownik referatu lub bezpośredni przełożony kieruje do ABI wniosek w sprawie cofnięcia upoważnienia, o którym mowa w ust.1

142

§ 15. 1. ABI zobowiązany jest do prowadzenia Ewidencji osób upoważnionych do przetwarzania danych osobowych i do niezwłocznego odnotowywania zmian w zakresie danych objętych tą Ewidencją.

2. Użytkownicy danych osobowych i bezpośredni przełożeni użytkowników odpowiadają za natychmiastowe przekazanie ABI i ASI informacji o osobach, które utraciły uprawnienia dostępu do danych osobowych.

3. ABI i ASI na podstawie informacji, o których mowa w ust. 2 podejmują niezwłocznie działania, mające na celu uniemożliwienie dostępu do danych osobowych osobom, które utraciły uprawnienia.

4. Elektroniczne i papierowe nośniki informacji, na których gromadzone są wykazy zawierające ewidencję osób upoważnionych do przetwarzania danych osobowych przechowuje się w zamykanej szafie, do której ma dostęp ABI lub osoba przez niego upoważniona.

§ 16. 1. Zastosowane przez Urząd rozwiązania techniczne umożliwiające dostęp zdalny do danych osobowych powinny zapewniać integralność, poufność i rozliczalność danych osobowych przesyłanych publicznymi łączami telekomunikacyjnymi.

2. Nadawanie uprawnień w celu umożliwienia dostępu zdalnego do systemów informatycznych przetwarzających dane osobowe należy do obowiązków ASI po spełnieniu wymagań określonych w ust. 1 oraz po uzyskaniu akceptacji ADO.

3. ASI jest zobowiązany do monitorowania dostępu do systemów informatycznych umożliwionego użytkownikom zewnętrznych pod kątem bezpieczeństwa celem zapewnienia poufności, rozliczalności i integralności danych osobowych.

Rozdział 7
Rejestracja zbiorów danych osobowych

§ 17. 1. Użytkownicy danych osobowych zobowiązani są do niezwłocznego przekazywania ABI informacji o zamiarze utworzenia nowego zbioru danych osobowych łącznie ze wskazaniem podstawy przetwarzania danych, uzasadnieniem celowości, zakresu i sposobu zbierania danych osobowych.

2. ABI zobowiązany jest do weryfikacji wniosku, o którym mowa w ust. 1 i analizy nowego zbioru danych pod kątem obowiązku zgłoszenia zasobu, jako zbioru danych do rejestracji w GIODO.

3. W przypadku gdy rejestracja nowopowstałego zbioru lub zbioru wymagającego aktualizacji danych osobowych jest ustawowo wymagana, użytkownik danych osobowych przygotowuje projekt zgłoszenia zbioru danych osobowych/zgłoszenia zmian do rejestracji/zmiany w GIODO . w części A-D wniosku.

4. Część E-F zgłoszenia/zmiany zgłoszenia zbioru do rejestracji przez GIODO przygotowuje ASI odpowiedzialny za odpowiednie zabezpieczenie danych w systemie informatycznym Urzędu.

5. ASI sprawdza opisane w zgłoszeniu rejestracyjnym warunki techniczne i organizacyjne dotyczące zabezpieczeń w systemie informatycznym, a w przypadku niewystarczającego

poziomu zabezpieczeń występuje z wnioskiem do ADO o podniesienie poziomu tych zabezpieczeń.

6. Sprawdzony przez ASI projekt zgłoszenia zbioru danych osobowych do rejestracji w GIODO podpisuje ADO.

7. ADO zgłasza wniosek o rejestrację zbioru danych osobowych do GIODO i wyznacza użytkownika danych osobowych zarejestrowanego zbioru danych osobowych.

8. ABI i ASI zobowiązani są do uzupełniania Polityki, dokumentów z nią powiązanych i pozostałych dokumentów obowiązujących w Urzędzie w zakresie ochrony danych osobowych o informacje na temat nowego zbioru.

Rozdział 8
Udostępnianie danych osobowych

§ 18. 1. Dane osobowe mogą być udostępniane podmiotom uprawnionym do ich otrzymania na mocy przepisów prawa oraz osobom, których dotyczą.

2. Udostępnianie danych osobowych osobie nieupoważnionej do przetwarzania danych osobowych może nastąpić wyłącznie za zgodą ADO. Zgoda może dotyczyć udostępniania danych osobowych w przyszłości. Wniosek i zgodę sporządza się na piśmie.

3. Pracownik udostępniający dane osobowe zobowiązany jest zaznaczenia w formie pisemnej, iż 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 odpowiada użytkownik danych osobowych.

6. Informacje zawierające dane osobowe są przekazywane uprawnionym podmiotom lub osobom za potwierdzeniem odbioru:

1) listem poleconym;
2) w drodze teletransmisji danych;
3) w inny bezpieczny, prawem określony sposób.

7. W przypadku udostępniania danych osobowych ze zbioru danych osobowych, sporządza się kserokopię dokumentu zawierającego udostępniane dane. Odnotowaniu podlega: data udostępnienia odbiorcy, cel, dane pracownika, który udostępnił dane osobowe. Obowiązek ten nie dotyczy sytuacji, gdy przepisy prawa zezwalają na zbieranie danych osobowych bez konieczności ujawniania adresata danych.

Rozdział 9
Powierzanie przetwarzania danych osobowych

§ 19. 1. Powierzenie przetwarzania danych osobowych występuje w sytuacji gdy podmioty zewnętrzne współpracujące z Urzędem mają dostęp do danych osobowych przetwarzanych przez Urząd.

2. Powierzenie, o którym mowa w ust. 1 może się odbywać wyłącznie w trybie określonym w art. 31 ustawy poprzez zawarcie na piśmie umowy powierzenia przetwarzania danych

osobowych, pomiędzy Urzędem a określonym podmiotem, któremu zleca się wykonywanie czynności związanych z przetwarzaniem danych osobowych.

3. W umowie, o której mowa w ust. 2 określa się:

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 określonych w umowie;
4) wymagania bezpieczeństwa dla procesu przetwarzania danych osobowych.

4. Umowy powierzenia przetwarzania danych osobowych oraz umowy, na podstawie których dochodzi do wymiany informacji powinny zawierać następujące elementy:

1) definicję informacji, która ma być chroniona;
2) czas trwania umowy, bezterminowy obowiązek zachowania poufności;
3) związane z ochroną danych działania, wymagane w momencie zakończenia umowy;
4) odpowiedzialność i działania stron umowy podejmowane w celu uniknięcia nieupoważnionego ujawnienia informacji;
5) określenie właściciela informacji;
6) określenie dozwolonego użycia danych osobowych oraz praw do ich użycia;
7) określenie prawa do audytu i monitorowania działań związanych z ochroną danych osobowych;
8) określenie trybu powiadamiania i raportowania nieuprawnionego ujawnienia lub naruszenia poufności i integralności danych osobowych;
9) określenie zasad zwrotu lub niszczenia danych osobowych przy zakończeniu umowy;
10) określenie działań podejmowanych w przypadku naruszenia warunków umowy.

5. Użytkownicy danych osobowych są zobowiązani do kierowania do ABI wniosków dotyczących przygotowania projektu umowy powierzenia przetwarzania danych osobowych, za które są odpowiedzialni.

6. Projekt umowy powierzenia przetwarzania danych osobowych innemu podmiotowi w przypadku wystąpienia takiej potrzeby przygotowuje zespół powołany przez ABI.

7. W skład zespołu, o którym mowa w ust. 6 wchodzi ASI.

8. Powierzenie przetwarzania danych osobowych poza granice Rzeczpospolitej Polskiej wymaga zgody ADO i jest możliwe po sprawdzeniu wymagań prawnych obowiązujących w tym zakresie.

Rozdział 10
Postępowanie w przypadku naruszenia lub podejrzenia naruszenia ochrony danych osobowych

§ 20. 1. Przed przystąpieniem do pracy użytkownicy danych zobowiązani są do dokonania sprawdzenia stanu urządzeń informatycznych i oględzin stanowiska pracy, w tym do zwrócenia szczególnej uwagi, czy nie zaszły okoliczności wskazujące na naruszenie lub na próbę naruszenia ochrony danych osobowych przetwarzanych w systemach informatycznych i w zbiorach nieinformatycznych.

2. Do okoliczności, uznawanych za naruszenie, próbę 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 danych osobowych lub ich części osobom nieupoważnionym;
6) inny stan systemu informatycznego lub pomieszczeń niż pozostawiony przez użytkownika po zakończeniu pracy;
7) wydarzenia losowe, obniżające poziom ochrony systemu (np. brak zasilania, pożar);
8) kradzież sprzętu informatycznego lub nośników zewnętrznych zawierających dane osobowe (np. wydruków komputerowych, dyskietek, płyt CD-ROM, dysków twardych, pamięci zewnętrznych, itp.).

3. W przypadku stwierdzenia naruszenia lub zaistnienia okoliczności wskazujących na naruszenie ochrony danych osobowych pracownicy zobowiązani są do bezzwłocznego powiadomienia o tym fakcie ABI i ASI.

4. Do czasu przybycia ABI i ASI, pracownik powiadamiający:
1) powstrzymuje się od rozpoczęcia lub kontynuowania pracy, od podejmowania jakichkolwiek czynności, mogących spowodować zatarcie śladów naruszenia bądź innych dowodów;
2) zabezpiecza elementy systemu informatycznego lub inne dokumenty 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 ABI i ASI.

5. W przypadku stwierdzenia naruszenia lub zaistnienia okoliczności wskazujących na naruszenie ochrony danych osobowych ABI i ASI, po przybyciu na miejsce:
1) oceniają istniejącą sytuację, biorąc pod uwagę w szczególności stan pomieszczeń, w których przetwarzane są dane osobowe oraz stan urządzeń, szacują wielkość negatywnych następstw zdarzenia;
2) wysłuchują relacji osoby, która dokonała powiadomienia oraz innych osób mających związek ze zdarzeniem;
3) podejmują decyzję o trybie dalszego postępowania, stosownie do zakresu naruszenia lub zasadności podejrzenia naruszenia ochrony danych osobowych.

6. ABI i ASI sporządzają raport z przebiegu zdarzenia (wzór – zał. Nr 10), zawierający w szczególności informacje o:
1) dacie i godzinie powiadomienia o zdarzeniu;
2) godzinie przybycia do pomieszczeń, w których zdarzenie nastąpiło;
3) istniejącej w chwili przybycia sytuacji;
4) podjętych działaniach i ich zasadności;
5) stanie systemu po podjęciu działań naprawczych;

6) wnioskach w sprawie ograniczenia możliwości ponownego wystąpienia naruszenia ochrony danych osobowych.

7. Raport, o którym mowa w ust. 6 ABI przekazuje niezwłocznie ADO, a przypadku jego nieobecności osobie upoważnionej.

8. W przypadku stwierdzenia naruszenia lub zaistnienia okoliczności wskazujących na naruszenie ochrony danych osobowych, użytkownik może kontynuować pracę po otrzymaniu pozwolenia ABI.

9. W przypadku, gdy naruszenie ochrony danych osobowych jest wynikiem uchybienia obowiązującej w Urzędzie dyscypliny pracy, ABI wyjaśnia wszystkie okoliczności incydentu i podejmuje stosowne działania wobec osób, które dopuściły się wskazanego naruszenia.

10. Po zakończeniu czynności naprawczych system powinien utrzymać poziom ochrony nie niższy niż przed wystąpieniem incydentu związanego z naruszeniem ochrony danych osobowych.

Rozdział 11
Wykaz i opis struktury zbiorów danych osobowych

§ 21. 1. Gmina - reprezentowana przez Wójta Gminy - jest administratorem danych osobowych wymienionych w „Ewidencji zbiorów danych osobowych", prowadzonej przez ASI.

2. Dane osobowe gromadzone we wskazanych zbiorach są przetwarzane w systemach informatycznych oraz w kartotekach ewidencyjnych, zlokalizowanych w pomieszczeniach lub w części pomieszczeń przetwarzania danych osobowych.

3. ASI na podstawie informacji uzyskanych od użytkowników danych, prowadzi wykaz systemów i aplikacji stosowanych do przetwarzania danych osobowych.

§ 22. 1. ASI prowadzi ewidencję zawierającą aktualny opis struktury zbiorów danych osobowych wskazujący zawartość poszczególnych pól informacyjnych i powiązania między nimi.

2. Zakresy danych osobowych przetwarzanych w poszczególnych zbiorach danych osobowych ustalane są w oparciu o strukturę zbiorów danych osobowych prowadzonych w systemach informatycznych i powiązania pól informacyjnych utworzonych w tych systemach.

§ 23. ASI prowadzi dokumentację systemów informatycznych, zawierającą opis współpracy pomiędzy różnymi systemami informatycznymi oraz opis sposobu przepływu danych pomiędzy systemami, w których te dane są przetwarzane.

Rozdział 12
Zasady ochrony danych osobowych w zbiorach nieinformatycznych

§ 24. 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. Nie użytkowane, 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. Celem udokumentowania czynności mających na celu likwidację zbiorów archiwalnych, stosuje się odpowiednie przepisy dot. zasad archiwizacji i brakowania dokumentacji Urzędu.

Rozdział 13
Kontrola przestrzegania zasad bezpieczeństwa danych osobowych

§ 25. 1. ADO lub na jego polecenie ABI I ASI sprawują nadzór nad przestrzeganiem zasad ochrony danych osobowych wynikających z obowiązujących przepisów prawa, w tym: ustawy o ochronie danych osobowych oraz zasad ustanowionych w Polityce i Instrukcji zarządzania systemem informatycznym.

2. ABI i ASI przeprowadzają 1 raz w roku kontrolę w zakresie, o którym mowa w ust.1 i dokonują oceny stanu bezpieczeństwa danych osobowych.

3. Na podstawie zgromadzonych materiałów, ABI i ASI sporządzają roczne sprawozdanie i przedstawiają ADO.

§ 26. W sprawach nieuregulowanych w Polityce mają zastosowanie przepisy ustawy z dnia 29 sierpnia 1997 r. o ochronie danych osobowych i przepisy wykonawcze.

Załącznik Nr 1
do Polityki bezpieczeństwa
przetwarzania danych osobowych
w Urzędzie Gminy Białogard

Wykaz budynków, pomieszczeń lub części pomieszczeń, tworzących obszar, w którym przetwarzane są dane osobowe

1) Budynek Urzędu Gminy Białogard, mieszczący się przy ul. Wileńskiej 8, 78-200 Białogard.
2) Pomieszczenia budynku, o którym mowa w pkt.1, tj. :
a) piwnica - serwerownia, pokój informatyka;
b) pierwsze piętro – pokój nr 8, pokój nr 9, pokój nr 10, pokój nr 11, pokój nr 12, pokój nr 13, pokój nr 14;
3) drugie piętro - pokój nr 16, pokój nr 17, pokój nr 18, pokój nr 19,
4) trzecie piętro - pokój nr 21, pokój nr 22, pokój nr 23.

Załącznik Nr 2
do Polityki bezpieczeństwa
przetwarzania danych osobowych
w Urzędzie Gminy Białogard

Wzór

Ewidencja osób upoważnionych przez Administratora Danych Osobowych do przetwarzania danych osobowych.

Nr upoważnienia	Nazwisko i imię	Stanowisko służbowe	Nazwa zbioru danych osobowych	Zakres przetwarzania	Udzielone od	Udzielone do	Identyfikator

Załącznik Nr 3
do Polityki bezpieczeństwa
przetwarzania danych osobowych
w Urzędzie Gminy Białogard

Wzór

Ewidencja zbiorów danych osobowych przetwarzanych w Urzędzie Gminy Białogard

Lp.	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						

Załącznik Nr 4
do Polityki bezpieczeństwa
przetwarzania danych osobowych
w Urzędzie Gminy Białogard

Wzór

Wykaz zbiorów danych osobowych wraz ze wskazaniem programów zastosowanych do przetwarzania tych danych.

W Urzędzie Gminy Białogard dane osobowe przetwarzane są w zbiorach zawierających pola informacyjne:

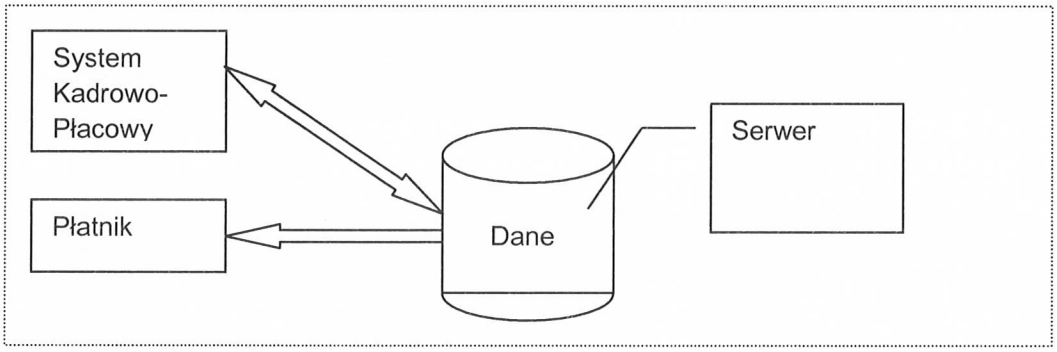
1. **Akta osobowe pracowników** - imię i nazwisko, data urodzenia, PESEL, imię ojca i matki, nr NIP, miejsce urodzenia, miejsce zamieszkania, nr dowodu osobistego, wykształcenie / nazwa szkoły i rok ukończenia/, wykształcenie uzupełniające, zawód, specjalność, stopień, tytuł zawodowy, kursy /w tym podyplomowe/, przebieg zatrudnienia, dodatkowe uprawnienia, badania lekarskie, powszechny obowiązek wojskowy, oświadczenie o dodatkowym zatrudnieniu, oświadczeniu o prowadzeniu działalności gospodarczej, oświadczenie o posiadaniu na utrzymaniu dzieci do 14 roku życia,
2. **Oświadczenia majątkowe pracowników wydających decyzje w imieniu Wójta Gminy Białogard, oraz osób zajmujących kierownicze stanowiska** - imię, nazwisko, data i miejsce urodzenia, miejsce pracy, stanowisko, zasoby pieniężne, posiadane nieruchomości, posiadane udziały w spółkach handlowych, posiadane akcje w spółkach handlowych, forma nabycia majątku, prowadzenie działalności gospodarczej , przynależność do spółek handlowych, spółdzielni, fundacji, inne dochody z tytułu zatrudnienia, dochody żony, zobowiązania pieniężne powyżej 10.000 zł , zaciągnięte kredyty i pożyczki,
3. .....

Załącznik Nr 5
do Polityki bezpieczeństwa
przetwarzania danych osobowych
w Urzędzie Gminy Białogard

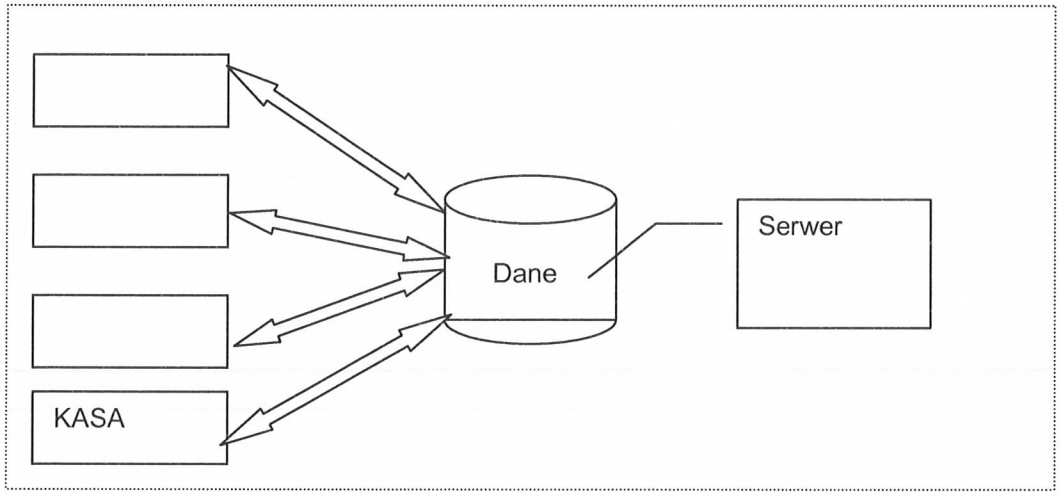
Wzór

Sposób przepływu danych pomiędzy poszczególnymi systemami:

a. System Kadrowo- Płacowy a Płatnik



b. System .....



Załącznik Nr 6
do Polityki bezpieczeństwa
przetwarzania danych osobowych
w Urzędzie Gminy Białogard

Wzór

Ewidencja przenośnych nośników danych używanych w Urzędzie Gminy Białogard

Lp.	Imię i nazwisko	Rodzaj nośnika (nazwa, pojemność)	Data przekazania, podpis użytkownika			Data zwrotu, podpis użytkownika		
			Data	Przekazujący	Odbierający	Data	Przekazujący	Odbierający
1								
2								
3								
4								
5								
6								
7								
8								
9								
10								
11								
12								
13								
14								
15								
16								

Załącznik Nr 7
do Polityki bezpieczeństwa
przetwarzania danych osobowych
w Urzędzie Gminy Białogard

Wzór

Oświadczenie o zachowaniu w poufności danych oraz sposobów ich zabezpieczeń.

Oświadczenie pracownika / użytkownika zewnętrznego zatrudnionego przy przetwarzaniu danych osobowych zawartych w zbiorach danych przetwarzanych przez Urząd Gminy Białogard

Ja niżej podpisana/y oświadczam, że:

1) zapoznałam/zapoznałem się z obowiązkami wynikającymi z:
a) ustawy z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (Dz. U. z 2002 r. Nr 101, poz. 926 ze zm.) oraz aktami wykonawczymi wydanymi na podstawie tej ustawy,
b) Polityką bezpieczeństwa przetwarzania danych osobowych w Urzędzie Gminy Białogard,
c) Instrukcją zarządzania systemem informatycznym służącym do przetwarzania danych osobowych w Urzędzie Gminy;
2) zobowiązuję się do zapewnienia bezpieczeństwa przetwarzanych danych osobowych poprzez ich ochronę przed niepowołanym dostępem, nieuzasadnioną modyfikacją lub zniszczeniem, nielegalnym ujawnieniem lub pozyskaniem;
3) zobowiązuję się do zachowania w tajemnicy danych osobowych i informacji o sposobie ich zabezpieczenia - do których uzyskałam/uzyskałem dostęp - w trakcie zatrudnienia i po ustaniu zatrudnienia;
4) posiadam znajomość przepisów określających zasady odpowiedzialności pracownika za niedopełnienie obowiązków wynikających z niniejszego oświadczenia

....

(data, podpis składającego oświadczenie) (data, podpis przyjmującego oświadczenie)

Załącznik Nr 8
do Polityki bezpieczeństwa
przetwarzania danych osobowych
w Urzędzie Gminy Białogard

Wzór

Wniosek o nadanie/zmianę/pozbawienie upoważnienia do przetwarzania danych osobowych.

..... Białogard, dnia .....
(pieczęć komórki organizacyjnej)

Wójt Gminy Białogard

WNIOSEK

Na podstawie art. 37 ustawy z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (Dz. U. z 2002 r. Nr 101, poz. 926 ze zm.) wnoszę o nadanie /pozbawienie/zmianę/* Pani /Panu/ Pana*

.....zatrudnionej/ zatrudnionemu/ zatrudnionego na stanowisku

....upoważnienia do przetwarzania danych osobowych w Urzędzie Gminy Białogard 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. Pracownik został zapoznany z przepisami o ochronie danych osobowych: /tak/nie/*

.....
(data, podpis)

/* niepotrzebne proszę skreślić

Załącznik Nr 9
do Polityki bezpieczeństwa
przetwarzania danych osobowych
w Urzędzie Gminy Białogard

Wzór

Upoważnienie do przetwarzania danych osobowych.

Białogard, ...

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 ze zm.) upoważniam Panią/Pana .....

zatrudnioną/zatrudnionego 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..... na czas zatrudnienia w Urzędzie Gminy Bialogard.

Jednocześnie zobowiązuję Panią/Pana do przestrzegania przepisów, dotyczących ochrony danych osobowych zawartych w ustawie o ochronie danych osobowych.

.....
(podpis Administratora Danych Osobowych)

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

.....
(data i podpis pracownika)

Załącznik Nr 10
do Polityki bezpieczeństwa
przetwarzania danych osobowych
w Urzędzie Gminy Białogard

Wzór

Raport z przebiegu zdarzenia naruszenia lub zaistnienia okoliczności wskazujących na naruszenie ochrony danych osobowych w Urzędzie Gminy Białogard

1. Data: ..... Godzina: (00: 00)
(dd.mm.rrrr)

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, podpisy ABI i ASI)

158

Załącznik Nr 2
do zarządzenia Nr 46/ 2011
Wójta Gminy Białogard
z dnia 30 września 2011 r.

INSTRUKCJA ZARZĄDZANIA SYSTEMEM INFORMATYCZNYM SŁUŻĄCYM DO PRZETWARZANIA DANYCH OSOBOWYCH w URZĘDZIE GMINY BIAŁOGARD

Zatwierdził (data i podpis):
30.09.2011
.....
Maciej Niechciał

Dokument powiązany z Polityką bezpieczeństwa przetwarzania danych osobowych w Urzędzie Gminy Białogard

159

SPIS TREŚCI:

160

Rozdział 1
Postanowienia ogólne

§ 1. 1. Instrukcja niniejsza, zwana dalej „Instrukcją" określa sposób zarządzania systemem informatycznym wykorzystywanym do przetwarzania danych osobowych, przez Administratora Danych Osobowych (ADO) w celu zabezpieczenia danych osobowych przed zagrożeniami, w tym przed ich udostępnieniem osobom nieupoważnionym, nieautoryzowaną zmianą, utratą, uszkodzeniem lub zniszczeniem. Celem instrukcji jest zagwarantowanie zgromadzonym danym osobowym, przez cały okres ich przetwarzania poufnego charakteru z zachowaniem ich integralności i rozliczalności.

2. Instrukcję opracowano zgodnie z wymogami § 5 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).

3. Podstawowym celem zabezpieczenia systemów informatycznych służących do przetwarzania danych osobowych, jest zapewnienie jak najwyższego poziomu bezpieczeństwa przetwarzanych danych osobowych w systemach informatycznych.

4. Uwzględniając kategorie danych osobowych oraz konieczność zachowania bezpieczeństwa ich przetwarzania w systemie informatycznym połączonym z siecią publiczną wprowadza się „poziom wysoki" bezpieczeństwa w rozumieniu § 6 rozporządzenia, o którym mowa w ust. 2.

Rozdział 2
Obowiązki w zakresie ochrony danych osobowych

§ 2. 1. Do obowiązków osób zaangażowanych w przetwarzanie danych osobowych w systemach informatycznych należy:

1) podejmowanie współpracy przy ustaleniu przyczyn naruszenia ochrony danych osobowych, usuwaniu skutków tych naruszeń oraz zapobieganie ich ewentualnemu ponownemu wystąpieniu;
2) przetwarzanie danych osobowych wyłącznie w celach prawem określonych.

2. Do obowiązków kierowników referatów lub bezpośrednich przełożonych należy w szczególności wnioskowanie do ADO o nadanie, zmianę lub cofnięcie uprawnień do przetwarzania danych w systemach informatycznych dla bezpośrednio podległych pracowników.

3. Użytkownicy danych osobowych podlegają okresowym szkoleniom, stosownie do potrzeb wynikających ze zmian w systemie informatycznym (wymiana sprzętu na nowszej generacji, zmiana oprogramowania) oraz w związku ze zmianą przepisów o ochronie danych osobowych lub zmianą wewnętrznych regulacji.

Rozdział 3
Obowiązki Administratora Bezpieczeństwa Informacji

§ 3. Do obowiązków ABI w zakresie ochrony danych osobowych przetwarzanych w systemach informatycznych należy w szczególności:

1) nadzór nad stosowaniem środków ochrony systemów;
2) nadzór nad przestrzeganiem przez ASI i użytkowników systemu – procedur

bezpieczeństwa;
3) wskazywanie zagrożeń oraz reagowanie na naruszenia ochrony danych osobowych i usuwanie ich skutków;
4) prowadzenie szkoleń dla użytkowników w zakresie stosowanych w systemach informatycznych środków ochrony danych osobowych;
5) doradztwo w zakresie przestrzegania przez użytkowników zewnętrznych zasad ochrony danych osobowych przyjętych w Urzędzie.

Rozdział 4
Obowiązki Administratora Systemów Informatycznych

§ 4. Do obowiązków Administratora Systemów Informatycznych w zakresie ochrony danych osobowych przetwarzanych w systemach informatycznych należy w szczególności:
1) realizacja zadań określonych w Polityce bezpieczeństwa przetwarzania danych osobowych w Urzędzie Gminy Białogard;
2) prowadzenie ewidencji użytkowników systemów informatycznych, w których przetwarzane są dane osobowe;
3) kontrolowanie nadanych w systemach informatycznych uprawnień do przetwarzania danych osobowych pod kątem ich zgodności z wpisami umieszczonymi w ewidencji osób upoważnionych do przetwarzania danych osobowych;
4) zarządzanie systemami informatycznymi w sposób zapewniający ochronę danych osobowych w nich przetwarzanych;
5) przestrzeganie opracowanych dla systemu procedur operacyjnych i bezpieczeństwa;
6) kontrola przepływu informacji pomiędzy systemem informatycznym a siecią publiczną oraz kontrola działań inicjowanych z sieci publicznej;
7) zarządzanie stosowanymi w systemach informatycznych środkami uwierzytelnienia, w tym rejestrowanie i wyrejestrowywanie użytkowników oraz dokonywanie zmiany upoważnień na podstawie wniosków zaakceptowanych przez ADO;
8) utrzymywanie systemu w należytej sprawności technicznej;
9) regularne tworzenie kopii zapasowych zasobów danych osobowych oraz programów służących do ich przetwarzania;
10) wykonywanie lub nadzór nad wykonywaniem okresowych przeglądów i konserwacji sprzętu informatycznego, systemów informatycznych, aplikacji oraz elektronicznych nośników informacji, na których zapisane są dane osobowe.

Rozdział 5
Obowiązki użytkowników danych osobowych

§ 5. Do obowiązków użytkowników danych osobowych w zakresie ochrony danych osobowych przetwarzanych w systemach informatycznych należy w szczególności:
1) zapewnienie właściwego poziomu ochrony danych osobowych w systemach, dla danych za które są odpowiedzialni;
2) informowanie ABI o zmianie celu przetwarzania danych osobowych w systemie lub o poszerzeniu zakresu zbieranych danych osobowych;
3) przestrzeganie opracowanych dla systemu zasad przetwarzania danych osobowych, w tym opracowanych dla systemu procedur operacyjnych i bezpieczeństwa;
4) uniemożliwienie dostępu lub podglądu danych osobowych osobom nieupoważnionym;
5) udostępnianie danych osobowych wyłącznie osobom upoważnionym lub uprawnionym do ich uzyskania;
6) informowanie ABI i ASI o wszelkich naruszeniach, podejrzeniach naruszenia

i nieprawidłowościach w sposobie przetwarzania i ochrony danych osobowych;
7) wykonywania bez zbędnej zwłoki poleceń ABI i ASI w zakresie ochrony danych osobowych jeśli są one zgodne z przepisami prawa.

Rozdział 6
Bezpieczna eksploatacja systemów informatycznych

§ 6. Celem zapewnienia bezpiecznej eksploatacji systemów informatycznych przetwarzających dane osobowe:
1) użytkownikom zabrania się, wprowadzania zmian do oprogramowania, sprzętu informatycznego poprzez jego samodzielne konfigurowanie i wyposażanie;
2) użytkownikom zabrania się, umożliwiania stronom trzecim uzyskiwania nieupoważnionego dostępu do systemów informatycznych;
3) użytkownikom zabrania się instalowania nowego i dokonywania aktualizacji już zainstalowanego oprogramowania;
4) użytkownikom zabrania się wykorzystywania systemów informatycznych do celów innych niż związane z wykonywaniem obowiązków służbowych;
5) użytkownikom zabrania się korzystania z prywatnego sprzętu informatycznego, w tym oprogramowania oraz nośników pamięci;
6) użytkownikom zabrania się podejmowania prób testowania, modyfikacji i naruszenia zabezpieczeń systemów informatycznych lub jakichkolwiek działań noszących takie znamiona;
7) informacje przetwarzane przy użyciu współdzielonych aplikacji sieciowych na stacjach roboczych muszą być zapisywane na dyskach serwera;
8) wszystkie aplikacje sieciowe, współdzielone zasoby użytkowe muszą być ulokowane na przeznaczonych do tego celu serwerach;
9) zabrania się dokonywania nieautoryzowanych podłączeń innych niż stanowiące własność Gminy urządzeń teleinformatycznych do systemu informatycznego Urzędu.

Rozdział 7
Nadawanie uprawnień do przetwarzania danych osobowych

§ 7. 1. Użytkownicy systemu przetwarzającego dane osobowe przed przystąpieniem do przetwarzania danych osobowych w tym systemie informatycznym, zobowiązani są zapoznać się z:
1) ustawą z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (Dz. U. z 2002 Nr 101, poz. 926 ze zm.);
2) Polityką bezpieczeństwa przetwarzania danych osobowych w Urzędzie Gminy Białogard.

2. Przed dopuszczeniem do obsługi systemu informatycznego, w którym przetwarzane są dane osobowe użytkownicy podlegają przeszkoleniu w zakresie obsługi sprzętu informatycznego, oprogramowania systemowego oraz oprogramowania do obsługi aplikacji, którą będą wykorzystywali. Szkolenie przeprowadza ASI lub właściwa firma zewnętrzna.

3. Przed pierwszym zarejestrowaniem użytkownika w systemie i nadaniem uprawnień umożliwiających pracę w systemie przetwarzającym dane osobowe użytkownik składa oświadczenia o:
1) zachowaniu w tajemnicy danych osobowych i sposobów ich zabezpieczania oraz o przetwarzaniu danych osobowych zgodnie z przepisami;
2) uzyskaniu formalnego upoważnienia do przetwarzania danych osobowych

4. Rejestrowanie użytkowników i nadawanie uprawnień w systemach informatycznych dokonywane jest zgodnie z procedurą określoną w § 14 Polityki bezpieczeństwa przetwarzania danych osobowych w Urzędzie Gminy Białogard. Rejestracja polega na nadaniu identyfikatora i przydzieleniu hasła oraz wprowadzeniu tych danych do bazy użytkowników systemu.

5. Identyfikator oraz zakres dostępu użytkownika podlegają rejestracji w ewidencji osób upoważnionych do przetwarzania danych osobowych, określonej w § 15 Polityki bezpieczeństwa przetwarzania danych osobowych w Urzędzie Gminy Białogard.

6. ASI przekazuje użytkownikom tymczasowe hasła dostępowe w sposób bezpieczny.

7. Procedurę nadawania uprawnień do przetwarzania danych osobowych w systemach stosuje się odpowiednio, w przypadku zmiany i odebrania uprawnień w systemach.

8. Zmiany dotyczące użytkownika: rozwiązanie umowy o pracę, utrata upoważnienia, stanowią przesłankę do natychmiastowego wyrejestrowania użytkownika z systemu oraz do unieważnienia hasła i odnotowania tego faktu w ewidencji osób upoważnionych do przetwarzania danych osobowych, o której mowa w ust. 5.

9. Informację o zaistnieniu zmian dot. użytkownika, o których mowa w ust. 8 przekazuje niezwłocznie pracownik zatrudniony na stanowisku ds. kadrowych.

10. Prawa dostępu przyznane użytkownikom zewnętrznym mają charakter czasowy i mogą być przyznawane na okres odpowiadający wykonywanemu zadaniu.

11. Dostęp do systemu informatycznego, do poszczególnych aplikacji i baz danych przetwarzających dane osobowe jest możliwy tylko po podaniu identyfikatora odrębnego dla każdego użytkownika i poufnego hasła.

Rozdział 8
Metody i środki uwierzytelniania w systemie

§ 8. 1. Identyfikatory i hasła są sposobem zagwarantowania rozliczalności, poufności i integralności danych osobowych przetwarzanych w systemach informatycznych. Służą do weryfikowania tożsamości użytkownika, uzyskania dostępu do określonych zasobów, kont uprzywilejowanych lub uruchomienia określonej funkcji.

2. Celem zagwarantowania wysokiego poziomu bezpieczeństwa przetwarzania danych osobowych oraz zagwarantowania użytkownikom pełnej rozliczalności wykonywanych przez nich operacji w systemach informatycznych stosuje się następujące zasady:

1) użytkownicy przy uwierzytelnianiu do systemów informatycznych posiadają unikalne identyfikatory do osobistego i wyłącznego użytku;
2) hasła dostępu do systemów informatycznych są tworzone przez użytkownika i stanowią tajemnicę służbową, znaną wyłącznie temu użytkownikowi z zastrzeżeniem § 7 ust. 6;
3) użytkownik ponosi pełną odpowiedzialność za utworzenie hasła dostępu oraz jego przechowywanie;
4) hasła nie mogą być ujawniane lub przekazywane komukolwiek, bez względu na okoliczności.

3. Użytkownicy ponoszą odpowiedzialność za wszelkie działania w systemach informatycznych prowadzone z użyciem ich identyfikatora i hasła.

4. ASI ponosi odpowiedzialność za okresowe sprawdzanie, usuwanie lub blokowanie zbędnych identyfikatorów użytkowników oraz kont w systemach, za które są odpowiedzialni.

§ 9. 1. Wszystkie konta dostępowe (identyfikatory) do systemów informatycznych powinny być chronione hasłem.

2. Identyfikator i nadane uprawnienia powinny umożliwiać wykonywanie czynności wyłącznie zgodnych z zakresem powierzonych obowiązków.
3. Identyfikator użytkownika powinien być niepowtarzalny, po wyrejestrowaniu się z systemu informatycznego nie powinien być przydzielany innej osobie.
4. Identyfikator, który utracił ważność nie może być ponownie przydzielony innemu użytkownikowi.
5. Użytkownicy są zobowiązani do wybierania haseł dobrej jakości, składających się co najmniej z 8 znaków, zawierających małe i wielkie litery oraz cyfry lub znaki specjalne.
6. Hasła nie mogą być takie same jak identyfikator użytkownika, nie mogą być zapisywane w systemach w postaci jawnej.
7. Hasła powinny być utrzymywane w tajemnicy także po upływie ich ważności.
8. Należy unikać ponownego lub cyklicznego używania starych haseł.
9. Hasła dla użytkowników o wysokich uprawnieniach (np. root, administrator) mogą być wykorzystywane tylko w uzasadnionych przypadkach.
10. Hasła użytkowników o wysokich uprawnieniach powinny być przechowywane w uzgodnionym z ABI I ASI, zabezpieczonym przed dostępem osób nieupoważnionych miejscu.
11. Udostępnienie hasła osobie postronnej należy traktować jako poważny incydent naruszenia ochrony danych osobowych.

Rozdział 9
Wymogi dotyczące zmiany haseł i bezpiecznego uwierzytelniania

§ 10 1.Użytkownik zobowiązany jest do zmiany posiadanego hasła:
1) okresowo, zgodnie z wymaganiami dla danego systemu informatycznego (przed upływem terminu ważności hasła), nie rzadziej niż co 30 dni;
2) w przypadku ujawnienia lub podejrzenia ujawnienia hasła.
2. W przypadku braku dostępu do konta chronionego posiadanym hasłem, tj:
1) zapomnienia/zgubienia hasła;
2) wygaśnięcia ważności hasła;
3) zablokowania konta spowodowanego nieprawidłowym wprowadzeniem hasła;
4) braku uprawnień/interfejsu umożliwiających samodzielną zmianę hasła;
użytkownik zobowiązany jest wystąpić o zmianę hasła do ASI.

§ 11. 1. Procedura bezpiecznego uwierzytelniania w systemie informatycznym zapewnia minimalizowanie możliwości nieautoryzowanego dostępu do systemu. Procedura powinna ujawniać minimum informacji o systemie informatycznym tak, aby uniemożliwić nieuprawnionemu użytkownikowi uzyskanie dodatkowych wskazówek w celu ich wykorzystania w sposób niedozwolony. Celem realizacji powyższego należy zapewnić zatwierdzanie jedynie kompletnych informacji wejściowych, niezbędnych przy logowaniu; jeżeli wystąpi błąd, system nie powinien wskazywać, która część danych jest poprawna, a która niepoprawna

Rozdział 10
Wymagania dotyczące sprzętu i oprogramowania

§ 12. 1. Wygaszacz stacji roboczej konfiguruje się w sposób umożliwiający automatyczne aktywowanie się po upływie 20 minut od ostatniego użycia stacji roboczej, uruchamiając blokadę stacji roboczej, wymuszającą ponowne zalogowanie.
2. Ekrany monitorów należy ustawić w sposób, uniemożliwiający osobom postronnym wgląd lub spisanie informacji wyświetlanej na ekranie monitora.

3. Programy zainstalowane na stacjach roboczych stacjonarnych i na komputerach przenośnych obsługujących przetwarzanie danych osobowych muszą być użytkowane z zachowaniem praw autorskich i posiadać licencje.

4. Oprogramowanie może być używane tylko zgodnie z prawami licencji Oprogramowanie typu Freeware, Shareware lub inne oprogramowanie dostarczane bez opłat jest uznawane jako nieautoryzowane, jeżeli nie otrzyma stosownej aprobaty ASI.

5. Przed zainstalowaniem nowego oprogramowania ASI zobowiązany jest sprawdzić działanie programu pod kątem bezpieczeństwa całego systemu.

6. Sieć teleinformatyczna wykorzystywana do przetwarzania danych osobowych powinna mieć zapewnione prawidłowe zasilanie energetyczne gwarantujące właściwe i zgodne z wymaganiami producenta działanie sprzętu informatycznego.

7. Serwer systemu przetwarzającego dane osobowe powinien być zasilany przez UPS o odpowiednich parametrach, pozwalających na podtrzymanie zasilania przez co najmniej 15 minut oraz na wykonanie, bezpiecznego wyłączenia serwera, tak aby przed ostatecznym zanikiem zasilania zostały prawidłowo zakończone operacje rozpoczęte na zbiorze danych osobowych.

8. Infrastruktura techniczna związana z siecią teleinformatyczną i jej zasilaniem (rozdzielnie elektryczne, skrzynki z bezpiecznikami) powinna być zabezpieczona przed dostępem osób nieupoważnionych.

Rozdział 11
Procedury rozpoczęcia, zawieszenia i zakończenia pracy w systemie

§ 13. 1. Przed przystąpieniem do pracy w systemie, użytkownik zobowiązany jest do dokonania kontroli stanu urządzeń informatycznych, oględzin stanowiska pracy, ze zwróceniem szczególnej uwagi, czy nie zaszły okoliczności wskazujące na naruszenie ochrony danych osobowych.

2. W przypadku stwierdzenia bądź podejrzenia, iż miało miejsce naruszenie ochrony danych osobowych, użytkownik systemu zobowiązany jest do postępowania zgodnego z procedurą opisaną w § 20 Polityki bezpieczeństwa przetwarzania danych osobowych w Urzędzie Gminy Białogard.

3. Przed opuszczeniem stanowiska pracy, użytkownik obowiązany jest zablokować swoją stację roboczą poprzez wciśnięcie klawiszy "ctrl+alt+delete" i wybranie opcji "Zablokuj stację roboczą".

4. Kończąc pracę, użytkownik obowiązany jest do wylogowania się z systemu informatycznego i zabezpieczenia stanowiska pracy, w szczególności wszelkiej dokumentacji, wydruków oraz wymiennych nośników informacji, na których znajdują się dane osobowe i umieszczenia ich zamykanych szafkach.

Rozdział 12
Przetwarzanie, udostępnianie i likwidacja danych osobowych

§ 14. 1. W przypadku przekazywania urządzeń lub nośników zawierających dane osobowe, poza obszar przetwarzania danych osobowych, zabezpiecza się je w sposób zapewniający poufność, integralność i rozliczalność tych danych, przez co rozumie się:

1) ograniczenie dostępu do danych osobowych hasłem zabezpieczającym dane przed osobami nieupoważnionymi;
2) stosowanie odpowiednich zabezpieczeń fizycznych;
3) stosowanie odpowiednich zabezpieczeń organizacyjnych;

2. W zależności od stopnia zagrożenia stosuje się kombinacje zabezpieczeń wymienionych w pkt.1, 2, 3.

3. Zabronione jest kopiowanie przez użytkowników plików z serwerów na stacje robocze użytkowników i na elektroniczne nośniki informacji bez uprzedniego uzyskania zgody ABI.

4. Dla udokumentowania czynności dokonywanych w celu likwidacji nie podlegających archiwizacji w odrębnym trybie zbiorów danych osobowych w systemie informatycznym, dla których cel przetwarzania ustał, ABI lub osoby upoważnione sporządzają protokół, zawierający następujące informacje:

1) datę dokonania likwidacji;
2) przedmiot likwidacji (aplikacja, baza);
3) podpisy osób dokonujących i obecnych przy likwidacji zbiorów danych osobowych.

5. Decyzję o likwidacji zbiorów danych osobowych, przetwarzanych w systemach informatycznych podejmują użytkownicy zasobów danych osobowych.

6. W przypadku likwidacji elektronicznych nośników informacji, należy uprzednio skutecznie usunąć dane z likwidowanych nośników. W przypadku gdy usunięcie danych nie jest możliwe, należy uszkodzić nośniki w sposób uniemożliwiający odczyt tych danych.

7. Przed przekazaniem elektronicznego nośnika informacji osobie nieuprawnionej, należy usunąć z nośnika dane osobowe.

Rozdział 13
Kopie zapasowe

§ 15. 1. ASI lub użytkownicy wykonują jeden raz w tygodniu zapasowe kopie zbiorów danych osobowych, programów i narzędzi programowych służących do ich przetwarzania.

2. Kopie zapasowe tworzy się na nośnikach magnetycznych, odpowiednio opisanych, oznakowanych i ewidencjonowanych.

3. Kopie zapasowe opisuje się w sposób umożliwiający szybką i jednoznaczną identyfikację zawartych w nich danych.

4. ASI odpowiedzialny za tworzenie kopi zapasowych, zobowiązany jest do przestrzegania terminów sporządzania kopii zapasowych.

5. Kopie zapasowe przechowuje się przez okres trzech miesięcy. Dane z kopii zapasowych powinny być odtwarzane wyłącznie przez ASI.

6. Kopie zapasowe, które uległy uszkodzeniu podlegają natychmiastowemu zniszczeniu.

7. Niszczenia kopii zapasowych, na nośnikach magnetycznych dokonuje ASI. Proces niszczenia kopi zapasowych odbywa się komisyjnie i jest dokumentowany poprzez sporządzenie protokołu.

Rozdział 14
Przechowywanie nośników elektronicznych zawierających dane osobowe

§ 16. 1. Dane osobowe mogą być przechowywane:

1) na serwerach zlokalizowanych w obszarach wyznaczonych do przetwarzania danych osobowych;
2) na wymiennych nośnikach elektronicznych;
3) na poszczególnych stacjach roboczych.

2. Po wykorzystaniu dane osobowe w postaci elektronicznej należy niezwłocznie usunąć z nośnika elektronicznego, w sposób uniemożliwiający ich ponowne odtworzenie.
3. Nie użytkowane wymienne nośniki elektroniczne, przechowuje się w zamykanych szafkach, szufladach.
4. Nośniki zawierające kopie zapasowe powinny być przechowywane w innym pomieszczeniu niż to, w którym umieszczony jest serwer przetwarzający dane osobowe.
6. Kopie zapasowe przechowuje się w wyznaczonym pomieszczeniu, w kasetce metalowej zamykanej na klucz przeznaczonej wyłącznie do przechowywania kopii zapasowych. Szafa jest zamykana na klucz, a klucze od kasetki i od szafy przechowywane są oddzielnie. Dostęp do kopii posiadają wyłącznie ABI i ASI.
7. Każde wydanie i przyjęcie lub jakiekolwiek użycie kopii jest odnotowywane w ewidencji kopii zapasowych (wzór - zał.) .

Rozdział 15
Ochrona systemu informatycznego przed działaniem szkodliwego oprogramowania

§ 17. 1. Na każdej stacji roboczej w sieci oraz na serwerze przetwarzającym dane osobowe powinno być zainstalowane oprogramowanie antywirusowe skanujące na bieżąco system informatyczny.
2. Skaner poczty elektronicznej powinien być stale włączony.
3. Kontrola antywirusowa powinna być przeprowadzana na nośnikach służących zarówno do przetwarzania danych osobowych w systemie, jak i do celów instalacyjnych.
4. Należy stosować wersje programów antywirusowych z aktualną bazą sygnatur wirusów.
5. Nowe wersje oprogramowania antywirusowego oraz uaktualnienia bazy sygnatur wirusów instaluje się automatycznie.
6. W przypadku zainfekowania systemu ASI odpowiada za usunięcie wirusa.
8. ASI ma prawo odłączyć od sieci stację roboczą, na której został zlokalizowany wirus, jeśli uzna, że dalsze pozostawienie go w sieci zagraża innym stacjom roboczym.

Rozdział 16
Zasady komunikacji w sieci teleinformatycznej

§ 18. 1. Przesyłanie danych osobowych drogą teletransmisji może odbywać się wyłącznie przy wykorzystaniu wymaganych zabezpieczeń logicznych chroniących przed nieuprawnionym dostępem.
2. Dopuszcza się przetwarzanie danych osobowych w plikach (MS Word, MS Excel) na stacjach roboczych użytkowników, poza bazą danych, znajdującą się w określonym systemie informatycznym.
3. ASI jest zobowiązany do chronienia systemu informatycznego służącego do przetwarzania danych osobowych przed zagrożeniami pochodzącymi z sieci publicznej poprzez wdrożenie zabezpieczeń chroniących przed nieuprawnionym dostępem.
4. Zabezpieczenia, o których mowa w ust. 3 powyżej, obejmują:
1) kontrolę przepływu informacji pomiędzy systemem informatycznym a siecią publiczną;
2) kontrolę działań inicjowanych z sieci publicznej i systemu informatycznego.
5. Wynik kontroli jest dokumentowany przez ASI raportem kontroli.

Rozdział 17
Zasady monitorowania, przeglądu i konserwacji systemu informatycznego

§ 19. 1. Przeglądy, naprawy i konserwacje systemu informatycznego przeprowadzane w miejscu użytkowania systemu odbywają się w obecności ASI, który odpowiada za prawidłowość przeprowadzanych przeglądów, zapewnienie należytej jakości przeglądów, konserwację systemów.

2. W przypadku konieczności dokonania przeglądu, naprawy lub konserwacji systemu informatycznego poza miejscem jego użytkowania, z urządzenia należy wymontować element, na którym zapisane są dane osobowe, o ile jest to możliwe. W przeciwnym wypadku należy zawrzeć z podmiotem dokonującym naprawy umowę powierzenia w rozumieniu art. 31 ustawy o ochronie danych osobowych.

3. ASI codziennie przeprowadza kontrolę logów zdarzeń zachodzących w systemie oraz każdorazowo po wykryciu naruszenia zasad bezpieczeństwa.

4. Jeden raz w roku należy przeprowadzać weryfikację całego oprogramowania użytkowego eksploatowanego na wszystkich stacjach roboczych podłączonych do systemu informatycznego pod kątem spełnienia wymogów bezpieczeństwa.

5. Kontrole i testy przeprowadzane przez ASI powinny obejmować zarówno dostęp do zasobów systemu, jak i profile oraz uprawnienia poszczególnych użytkowników.

Rozdział 18
Zasady postępowania z komputerami przenośnymi

§ 20. 1. O ile to możliwe, przy przetwarzaniu danych osobowych na komputerach przenośnych obowiązują procedury określone w niniejszej instrukcji, dotyczące pracy na komputerach stacjonarnych.

2. Pracownik używający przenośnego komputera zawierającego dane osobowe zobowiązany jest do zachowania szczególnej ostrożności podczas jego transportu, przechowywania i użytkowania poza obszarem przetwarzania danych osobowych. Ponadto zobowiązany jest do:

1) zabezpieczenia dostępu do komputera na poziomie systemu operacyjnego - identyfikator i hasło;
2) zabezpieczenia komputera przed dostępem osób nieupoważnionych;
3) przestrzegania zakazu korzystania z komputera do przetwarzania danych osobowych w obszarach użyteczności publicznej;
4) zachowania szczególnej ostrożności przy podłączaniu do sieci publicznych poza obszarem przetwarzania danych osobowych.

3. W przypadku podłączania komputera przenośnego do sieci publicznej poza siecią Urzędu należy zastosować firewall zainstalowany bezpośrednio na tym komputerze oraz system antywirusowy.

4. Użytkownik jest zobowiązany do zachowania szczególnej ostrożności w czasie korzystania z zasobów sieci publicznej.

5. Za wszelkie działania wykonywane na komputerze przenośnym odpowiada jego formalny użytkownik.

6. Obowiązuje zakaz samodzielnej modernizacji oprogramowania i sprzętu w powierzonych komputerach przenośnych. Wszelkie zmiany mogą być dokonywane tylko pod nadzorem ASI, stosownie do wymagań niniejszej instrukcji. Wystąpienie usterek w pracy komputerów przenośnych, konieczność aktualizacji ich oprogramowania należy zgłosić ASI.

7. Komputery przenośne wyposażone są w odpowiednie programy ochrony

antywirusowej, których aktualizację sugeruje automatycznie system.
8. Użytkownicy, którym zostały powierzone komputery przenośne podpisują umowę przekazania do użytku służbowego.

Rozdział 19
Postanowienia końcowe

§ 21. ABI i ASI są zobowiązani do zapoznania z treścią Instrukcji każdego użytkownika systemu informatycznego służącego do przetwarzania danych osobowych.

2. W sprawach nieuregulowanych w Instrukcji mają zastosowanie przepisy ustawy z dnia 29 sierpnia 1997 r., o ochronie danych osobowych (Dz. U. z 2002 r., Nr 101, poz. 926 ze zm.) i inne przepisy obowiązujące w zakresie ochrony danych osobowych.

Załącznik do
Instrukcji zarządzania systemem informatycznym
służącym do przetwarzania danych osobowych
w Urzędzie Gminy Białogard

Wzór

Ewidencja wydawania kopii zapasowych Urzędu Gminy Białogard

Lp.	Nazwa kopii zapasowej - rodzaj nośnika, cel wydania	Imię i nazwisko	Data przekazania, podpis użytkownika			Data zwrotu, podpis użytkownika		
			data	przekazujący	odbierający	data	przekazujący	odbierający
1								
2								
3								
4								
5								
6								
7								
8								
9								
10								
11								
12								
13								
14								
15								