Zarządzenie Nr 10/08
Wójta Gminy w Małkini Górnej
z dnia 1 kwietnia 2008 roku

w sprawie dokumentacji opisującej sposób przetwarzania danych osobowych oraz środki techniczne i organizacyjne zapewniające ochronę przetwarzania danych osobowych w Urzędzie Gminy w Małkini Górnej.

Na podstawie art. 36 ust. 1 i 2 ustawy z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (Dz. U. z 2002 r. Nr 101, poz. 926, Nr 153, poz. 1271; z 2004 r. Nr 25, poz. 219, Nr 33, poz. 285; z 2006 r. Nr 104, poz. 708 i 711) oraz § 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.

Wprowadza się następującą dokumentację opisującą sposób przetwarzania danych osobowych oraz środki techniczne i organizacyjne zapewniające ochronę przetwarzanych danych osobowych w Urzędzie Gminy w Małkini Górnej:

1) politykę bezpieczeństwa przetwarzania danych osobowych, stanowiącą załącznik Nr 1 do niniejszego zarządzenia;
2) instrukcję zarządzania systemem informatycznym służącym do przetwarzania danych osobowych, stanowiącą załącznik Nr 2 do niniejszego zarządzenia.

§ 2.

Obowiązki „Administratora Bezpieczeństwa Informacji" w systemie informatycznym Urzędu powierza się Panu Piotrowi Konferowiczowi zatrudnionemu na stanowisku do spraw obsługi informatycznej Urzędu.

§ 3.

Traci moc zarządzenie Nr 82/2004 Wójta Gminy w Małkini Górnej z dnia 27 października 2004 roku w sprawie wykonania ustawy o ochronie danych osobowych w Urzędzie Gminy w Małkini Górnej.

§ 4.

Wykonanie zarządzenia powierza się Administartorowi Bezpieczeństwa Informacji i Kierownikowi Referatu Organizacyjnego Spraw Obywatelskich i Kadr.

Załącznik Nr 1
do zarządzania Nr 10/08
Wójta Gminy w Małkini Górnej

POLITYKA BEZPIECZEŃSTWA

Wstęp

Wójt Gminy w Małkini Górnej, świadomy wagi zagrożeń prywatności, w tym zwłaszcza zagrożeń danych osobowych przetwarzanych w związku z wykonywaniem zadań Administratora danych, deklaruje podejmowanie wszelkich możliwych działań koniecznych do zapobiegania m. in. takim zagrożeniom, jak:

3) sytuacje losowe lub nieprzewidziane oddziaływanie czynników zewnętrznych na zasoby systemu, jak np. pożar, zalanie pomieszczeń, katastrofa budowlana, napad, kardzież, włamanie, działania terrorystyczne, niepożądana ingerencja ekipy remontowej,
4) niewłaściwe parametry środowiska zakółcające pracę urządzeń komputerowych (nadmierna wilgotność lub bardzo wysoka temperatura, oddziaływanie pola elektromagnetycznego i inne),
5) awarie sprzętu lub oprogramowania, które wyraźnie wskazują na umyślne naruszenia ochrony danych, niewłaściwe działanie serwisantów, w tym pozotawienie serwisantów bez nadzoru, a także przyzwolenie na naprawę sprzętu zawierającego danego osobowe poza siedzibą Administratora danych,
6) naruszenie bezpieczeństwa danych przez nieautoryzowane ich przetwarzanie; ujawnienie osobom nieupoważnionym procedur ochrony danych stosowanych przez Administratora danych,
7) ujawnienie osobom nieupoważnionym danych przetwarzanych przez Administratora danych, w tym także nieumyślne ujawnienie danych osobom postronnym, przebywającym bez nadzoru lub niedostatecznie nadzorowanym w pomieszczeniach Administratora danych,
8) podejmowanie pracy w systemie z przełamaniem lub zaniechaniem stosowania procedur danych np. praca osoby, która nie jest upoważniona do przetwarzania, próby stosowania nie swojego hasła i identyfikatora przez osoby upoważnione,
9) celowe lub przypadkowe rozproszenie danych w internecie z ominięciem zabezpieczeń systemu lub wykorzystaniem błędów projektu systemu informatycznego Administratora danych,
10) ataki z internetu,
11) naruszenia zasad i procedur określonych w dokumentacji z zakresu ochrony danych osobowych przez osoby upoważnione do przetwarzania danych osobowych związane z nieprzestrzeganiem procedur ochrony danych, w tym zwłaszcza;

    a) niezgodne z procedurami zakończenie pracy lub opuszczenie stanowiska pracy (nieprawidłowe wyłączenie komputera, niezablokowanie wyświetlenia

treści pracy na ekranie komputera przed tymczasowym opuszczeniem stanowiska pracy, pozostawienie po zakończeniu pracy nieschowanych do zamykania na klucz szaf dokumentów zawierających dane osobowe, niezamknięcie na klucz pokoju po jego opuszczeniu, nieprzekazanie klucza do zabezpieczonego pomieszczenia);
b) niewykonywanie stosownych kopii zapasowych;
c) przetwarzanie danych osobowych w celach prywatnych;
d) wprowadzanie zmian do systemu informatycznego Administratora danych i wgrywanie programów bez zgody Administratora bezpieczeństwa informacji.

Postanowienia ogólne

1. Definicje

Ilekroć w polityce bezpieczeństwa jest mowa o:

1) ustawie – rozumie się przez to ustawę z 29 sierpnia 1997 r. o ochronie danych osobowych (tekst jedn. Dz. U. z 2002 r. Nr 101, poz. 926 ze zm.);
2) rozporządzeniu – rozumie się przez to rozporządzenie Ministra Spraw Wewnętrznych i Administracji z 29 kwietnia 2004 roku w sprawie warunków technicznych i organizacyjnych, jakim powinny odpowiadać urządzenia i systemy informatyczne służące do przetwarzania danych osobowych (Dz. U. Nr 100, poz. 1024);
3) administratorze danych rozumie się przez to Urząd Gminy reprezentowany przez Wójta;
4) administratorze systemu – rozumie się przez to stanowisko pracy ds. Obsługi informatycznej Urzędu;
5) osobie upoważnionej do przetwarzania danych osobowych – rozumie się przez to osobę, ktora upoważniona została na piśmie przez Wójta do przetwarzania danych osobowych;
6) użytkowniku – rozumie się przez to osobę upoważnioną do przetwarzania danych osobowych, której nadano identyfikator i przyznano hasło;
7) przetwarzającym – rozumie się przez to podmiot, któremu zostało powierzone przetwarzanie danych osobowych na podstawie umowy zawieranej zgodnie z art. 31 ustawy;
8) odbiorcy danych – rozumie się przez to każdego, komu udostępnia się dane osobowe, z wyłączeniem:
   a) osoby, której dane dotyczą,
   b) osoby upoważnionej do przetwarzania danych,
   c) przedstawiciela, o którym mowa w art. 31 a ustawy,
   d) podmiotu, o którym mowa w art. 31 ustawy,
   e) organów państwowych lub organów samorządu terytorialnego, którym dane są udostępniane w związku z prowadzonym postępowaniem;
9) identyfikatorze – rozumie się przez to ciąg znaków literowych, cyfrowych lub innych jednoznacznie identyfikujących osobę upoważnioną do przetwarzania

danych osobowych w systemie informatycznym;
10) haśle – rozumie się przez to ciąg znaków literowych, cyfrowych lub innych, znany jedynie osobie uprawnionej do pracy w systemie informatycznym,
11) sieci telekomunikacyjnej – rozumie się przez to sieć telekomunikacyjną w rozumieniu art. 2 pkt. 32 ustawy z 16 lipca 2004 r. - Prawo telekomunikacyjne (Dz. U. Nr 171, poz. 1800 ze zm.);
12) sieci publicznej – rozumie się przez to publiczną sieć telekomunikacyjną w rozumieniu art. 2 pkt 29 ustawy z 16 lipca 2004 r. - Prawo telekomunikacyjne;
13) teletransmisji – rozumie się przez to przesyłanie informacji za pośrednictwem sieci telekomunikacyjnej;
14) rozliczalności – rozumie się przez to właściwość zapewniającą, że działania podmiotu mogą być przypisane w sposób jednoznaczny tylko temu podmiotowi;
15) integralności danych – rozumie się przez to właściwość zapewniającą, że dane osobowe nie zostały zmienione lub zniszczone w sposób nieautoryzowany;
16) poufności danych – rozumie się przez to właściwość zapewniającą, że dane nie są udostępnianie nieupoważnionym podmiotom;
17) raporcie – rozumie się przez to przygotowane przez system informatyczny zestawienia zakresu i treści przetwarzanych danych;
18) uwierzytelnianiu – rozumie się przez to działanie, którego celem jest weryfikacja deklarowanej tożsamości podmiotu.

2. Cel

Wdrożenie polityki bezpieczeństwa ma na celu zabezpieczenie przetwarzanych w Urzędzie Gminy danych osobowych, w tym bezpieczeństwa danych przetwarzanych w systemie informatycznym i poza nim. Niniejszy dokument opisuje niezbędny do uzyskania bezpieczeństwa danych osobowych zbiór procedur i zasad dotyczących przetwarzania danych osobowych oraz ich zabezpieczenia.

3. Zakres stosowania

Polityka bezpieczeństwa administratora danych dotyczy zarówno danych osobowych przetwarzanych w sposób tradycyjny w księgach, wykazach i innych zbiorach ewidencyjnych, jak i w systemach informatycznych.

Procedury i zasady określone w niniejszym dokumencie stosuje się do wszystkich osób upoważnionych do przetwarzania danych osobowych, zarówno zatrudnionych, jak i innych np. stażystów, praktykantów.

II. Organizacja przetwarzania danych osobowych

1.Administrator danych osobowych

Administrator danych osobowych reprezentowany przez Wójta Gminy w Małkini Górnej realizuje zadania w zakresie ochrony danych osobowych, w tym zwłaszcza:

1) upoważnia poszczególne osoby do przetwarzania danych osobowych (wzór upoważnienia w zał. Nr 1) w stosownym, indywidualnie określonym zakresie;
2) wyznacza „Administratora Bezpieczeństwa Informacji" oraz określa zakres jego zadań w zakresie czynności;
3) wyznacza Kierownika Referatu Organizacyjnego Spraw Obywatelskich i Kadr jako właściwego do prowadzenia ewidencji osób upoważnionych do przetwarzania danych osobowych oraz pozostałej dokumentacji z zakresu ochrony danych, jeżeli jako właściwy do jej prowadzenia nie zostanie wskazany w niniejszym dokumencie inny podmiot;
4) podjemuje odpowiednie działania w przypadku naruszenia lub podejrzenia naruszenia procedur bezpiecznego przetwarzania danych osobowych;
5) zleca Kierownikowi Referatu Organizacyjnego Spraw Obywatelskich i Kadr, aby we współpracy z administratorem systemu oraz administratorem bezpieczeństwa informacji zapewnił użytkownikom odpowiednie stanowiska pracy umożliwiające bezpieczne przetwarzanie danych;
6) podejmuje decyzje o celach i środkach przetwarzania danych osobowych, zwłaszcza z uwzględnieniem zmian w obowiązującym prawie, organizacji administratora danych oraz technik zabezpieczenia danych osobowych.

2. Administrator bezpieczeństwa informacji w szczególności:

1) sprawuje nadzór nad wdrożeniem stosownych środków organizacyjnych, technicznych i fizycznych w celu zapewnienia bezpieczeństwa danych;
2) sprawuje nadzór nad funkcjonowaniem systemu zabezpieczeń, w tym także nad prowadzeniem ewidencji z zakresu ochrony danych osobowych;
3) nadzoruje udostępnianie danych osobowych odbiorcom danych i innym podmiotom;
4) przygotowuje wnioski zgłoszeń rejestracyjnych i aktualizacyjnych zbiorów danych oraz prowadzi inną korespondencję z Generalnym Ionspektorem;
5) zatwierdza wzory dokumentów (odpowiednie klauzule na dokumentach) dotyczących ochrony danych osobowych przygotowywane przez komórki organizacyjne administratora danych;
6) nadzoruje prowadzenie ewidencji i innej dokumentacji z zakresu ochrony danych osobowych przez Kierownika Referatu Organizacyjnego Spraw Obywatelskich i Kadr;
7) prowadzi oraz aktualizuje dokumentację opisującą sposób przetwarzania danych osobowych oraz środki techniczne i organizacyjne zapewniające ochronę przetwarzanych danych osobowych;
8) podejmuje odpowiednie działania w wypadku naruszenia lub podejrzenia naruszenia systemu informatycznego;
9) przygotowuje wyciągi z polityki bezpieczeństwa dostosowane do zakresów

obowiązków osób upoważnionych do przetwarzania danych osobowych;
10) przygotowuje materiały szkoleniowe z zakresu ochrony danych osobowych i prowadzi szkolenia osób upoważnionych do przetwarzania danych osobowych;
11) w porozumieniu z administatorem danych osobowych oraz Kierownikiem Referatu Organizacyjnego Spraw Obywatelskich i Kadr na czas nieobecności (urlop, choroba) wyznacza swojego zastępcę.

3. Administator sytemu w szczególności:

1) zarządza systemem informatycznym, w którym przetwarzane są dane osobowe, posługując się hasłem dostępu do wszystkich stacji roboczych z pozycji administratora;
2) przeciwdziała dostępowi osób niepowołanych do systemu informatycznego, w którym przetwarzane są dane osobowe;
3) na wniosek Kierownika Referatu Organizacyjnego Spraw Obywatelskich i Kadr przydziela każdemu użytkownikowi identyfikator i hasło do systemu informatycznego oraz na polecenie administratora danych dokonuje ewentualnych modyfikacji uprawnień;
4) nadzoruje działanie mechanizmów uwierzytelnienia użytkowników oraz kontroli dostępu do danych osobowych;
5) podejmuje działania w zakresie ustalania i kontroli identyfikatorów dostępu do systemu informatycznego;
6) wyrejestrowuje użytkowników na polecenie administratora danych lub Kierownika Referatu Organizacyjnego Spraw Obywatelskich i Kadr;
7) zmienia w poszczególnych stacjach roboczych hasła dostępu, ujawniając je wyłącznie danemu użytkownikowi;
8) w stytuacji naruszenia zabezpieczeń systemu usuwa skutki naruszenia;
9) prowadzi szczegółową dokumentację naruszeń bezpieczeństwa danych osobowych przetwarzanych w systemie informatycznym;
10) nadzoruje wykonywanie napraw, konserwację oraz likwidację urządzeń komputerowych, na których zapisane sa dane osobowe, sprawuje nadzór nad wykonywaniem kopii zapasowych, ich przechowywaniem oraz okresowym sprawdzaniem pod kątem ich dalszej przydatności do odtwarzania danych w przypadku awarii systemu informatycznego;
11) podejmuje działania służące zapewnieniu niezawodności zasilania komputerów, innych urządzeń mających wpływ na bezpieczeństwo przetwarzania danych oraz zapewnieniu bezpiecznej wymiany danych w sieci wewnętrznej i bezpiecznej teletransmisji.

4. Kierownik Referatu Organizacyjnego, Spraw Obywatelskich i Kadr w szczególności:

1) prowadzi ewidencję osób upoważnionych do przetwarzania danych osobowych;
2) występuje z wnioskiem do administratora systemu o nadanie identyfikatora i

przyznanie hasła osobie upoważnionej do przetwarzania danych osobowych;
3) występuje z wnioskiem do administratora danych o nadanie upoważnienia do przetwarzania danych osobowych;
4) występuje z wnioskiem o odwołanie upoważnienia do przetwarzania danych osobowych i/lub wyrejestrowania użytkownika z systemu informatycznego.

5. Osoba upoważniona do przetwarzania danych osobowych

Użytkownik może przetwarzać dane osobowe wyłącznie w zakresie ustalonym indywidualnie przez administratora danych i tylko w celu wykonywania nałożonych na niego obowiązków. Zakres dostępu do danych przypisany jest do niepowtarzalnego identyfikatora użytkownika, niezbędnego do rozpoczęcia pracy w systemie. Rozwiązanie stosunku pracy, odwołanie z pełnionej funkcji powoduje wygaśnięcie upoważnienia do przetwarzania danych osobowych.

Użytkownicy danych pisemnie oświadczają, że zobowiązują się do zachowania tajemnicy danych osobowych oraz przestrzegania procedur ich bezpiecznego przetwarzania (wzór oświadczenia w zał. Nr 2). Przestrzeganie tajemnicy danych osobowych obowiązuje przez cały okres zatrudnienia u administratora danych, a także po ustaniu stosunku pracy lub odwołaniu z pełnionej funkcji.

Naruszenie przez użytkowników danych osobowych procedur bezpiecznego przetwarzania tych danych, w szczególności świadome udostępnienie danych osobie niepowołanej, jest ciężkim naruszeniem obowiązków pracowniczych i może uzasadnić rozwiązanie umowy o pracę bez wypowiedzenia.

Wszyscy użytkownicy danych zobowiązani są do:

1) zapoznania się z przepisami prawa w zakresie ochrony danych osobowych, w tym przepisami niniejszej polityki i instrukcji zarządzania systemem informatycznym służącym do przetwarzania danych osobowych,
2) stosowania określonych przez administratora danych oraz administratora bezpieczeństwa informacji procedur oraz wytycznych mających na celu zgodne z prawem, w tym zwłaszcza adekwatne przetwarzanie danych,
3) odpowiedniego zabezpieczenia danych przed ich udostępnieniem osobom nieupoważnionym.

III. Infrastruktura przetwarzania danych osobowych

Administrator przetwarza dane osobowe w dwóch budynkach: w budynku Nr 1 w Małkini Górnej przy ul. Przedszkolnej i w budynku Nr 3 przy ul. Biegańskiego 3 w Małkini Górnej.

1. Obszar przetwarzania danych osobowych obejmuje:

Wykaz zbiorów danych wraz ze wskazaniem
programów zastosowanych do przetwarzania tych danych
w budynku w Małkini Górnej ul. Przedszkolna 1

Lp.	Zbiór danych	Programy zastosowane przy przetwarzaniu nazwa zasobu	Lokalizacja zbioru/zasobu	Miejsce przetwarzania danych
1.	„Urząd Stanu Cywilnego”	PB – USC Komputerowy System Rejestracji Aktów Stanu Cywilnego	parter – pokój Nr 7	parter – pokój Nr 7
2.	„Dowody osobiste”	SWDO	parter – pokój Nr 7	parter – pokój Nr 7
3.	„Ewidencja ludności”	Elud +	Piętro – pokój Nr 14	Piętro – pokój Nr 14
4.	„Ewidencja podatków i opłat”	„Podatek”	Piętro – pokój Nr 8	Piętro – pokój Nr 8
5.	„Ewidencja podatków i opłat”	„JGU”	„Piętro – pokój Nr 8	Piętro – pokój Nr 8
6.	„Ewidencja podatków i opłat”	„AUTA”	Piętro – pokój Nr 12	Piętro – pokój Nr 12
7.	„Ewidencja podatków i opłat”	„KASA”	Piętro – pokój Nr 11	Piętro – pokój Nr 11
8.	„Rejestr wniosków o zwrot podatku akcyzowego zawartego w ceniu oleju napędowego wykorzystywanego do produkcji rolnej”	„Podatek”	Piętro – pokój Nr 8	Piętro – pokoj Nr 8
9.	„Płace”	„Kadri i płace”	Piętro – pokój Nr 12	Piętro – pokój Nr 12

Wykaz zbiorów ewidencyjnych (dane osobowe przetwarzane tylko tradycyjnie)
budynek zlokalizowany w Małkini Górnej ul. Przedszkolna 1

Lp.	Zbiór	Lokalizacja zbioru ewidencyjnego
1.	„Wykaz osób ubiegających się o przydział mieszkania”	parter – pokój Nr 1
2.	„Rejestr decyzji o warunkach zabudowy i zagospodarowania terenu”	parter – pokój Nr 1
3.	„Dodatki mieszkaniowe”	parter – pokój Nr 1
4.	„Numeracja porządkowa nieruchomości”	parter – pokój Nr 1
5.	„Rejestr rolników dotkniętych suszą”	parter – pokój Nr 3
6.	„Rejestr spraw dotyczących usuwania drzew”	parter – pokój Nr 3
7.	„Zezwolenia na wykonywanie krajowego zarobkowego przewozu osób taksówką bagażową”	parter – pokój Nr 3
8.	„Ewidencja zezwoleń na sprzedaż napojów alkoholowych”	parter – pokój Nr 3
9.	„Podział nieruchomości”	parter – pokój Nr 3
10.	„Rejestr ras psów uznanych za agresywne”	parter – pokój Nr 3
11.	„Decyzje środowiskowe”	parter – pokój Nr 3
12.	„Zajęcie pasa drogowego”	parter – pokój Nr 3
13.	„Rozgraniczenie nieruchomości”	parter – pokój Nr 3
14.	„Opłaty za wieczyste użytkowanie”	parter – pokój Nr 4
15.	„Nabycie, zbycie, dzierżawa lub użytkowanie wieczyste”	parter – pokój Nr 4
16.	„Rejestr zaświadczeń”	piętro – pokój Nr 8
17.	„Rejestr skarg i wniosków”	piętro – pokój Nr 8
18.	„Wybory ławników”	piętro – pokój Nr 9
19.	„Wykaz sołtysów”	piętro – pokój Nr 9
20.	„Oświadczenia majątkowe”	piętro – pokój Nr 14
21.	'Zamówienia publiczne”	arter – pokój Nr 1 i piętro – pokój Nr 10
22.	„Ewidencja formacji obrony cywilnej”	piętro – pokój Nr 14
23.	„Ewidencja przedpoborowych”	piętro – pokój Nr 14
24.	„Świadczenia osobiste i rzeczowe na rzecz obrony kraju”	piętro – pokój Nr 14

25. „Kadry” piętro – pokój Nr 9
26.

Wykaz zbiorów ewidencyjnych (dane osobowe przetwarzane tylko tradycyjnie)
w budynku zlokalizowanym w Małkini Górnej
ul. Biegańskiego 3

Lp.	Zbiór	Lokalizacja zbioru ewidencyjnego
1.	„Zbiór danych przetwarzanych przez Straż Gminną”	Małkinia Górna ul. Biegańskiego 3

3. Ewidencje

Kierownik Referatu Organizacyjnego Spraw Obywatelskich i Kadr prowadzi: ewidencję osób upoważnionych do przetwarzania danych.

Administrator danych prowadzi ewidencję udostępnień danych odbiorcom danych oraz innym podmiotom.

Administrator systemu prowadzi przechowywaną w kasie pancernej ewidencję haseł do stanowisk roboczych poszczególnych użytkowników danych oraz ich identyfikatorów.

IV. Struktuta zbiorów danych, sposób przepływu danych w systemie i zakres przetwarzania.

1. Zbiór danych „Urząd Stanu Cywilnego”

Zbiór „Urząd Stanu Cywilnego” obejmuje: nazwiska i imiona, imiona rodziców, datę urodzenia, miejsce urodzenia, adres zamieszkania lub pobytu, numer ewidencyjny PESEL, zawód, wykształcenie, nazwisko panieńskie, nazwisko z poprzedniego małżeństwa, nazwisko rodowe, datę i numer aktu małżeństwa, imię i nazwisko ojca, imię i nazwisko matki, imię i nazwisko wpółmałżonka, płeć, stan cywilny, datę i miejsce zawarcia małżeństwa; datę, godzinę, miejsce zgonu lub odnalezienia zwłok, datę zgonu męża matki; nazwisko, imię, adres osoby zgłaszającej zgon, numer aktu zgonu żony lub męża, nazwisko i imię rodowe małżonka, nazwisko rodowe matki i ojca mężczyzny, nazwisko rodowe matki i ojca kobiety, adnotacje o rozwodzie, nazwisko po zawarciu małżeństwa mężczyzny, kobiety, dzieci; numer dowodu i miejsce wydania dowodu kobiety, mężczyzny; data unieważnienia aktu małżeństwa, urodzenia, zgonu; imię nadane z urzędu, zmiana nazwiska dziecka, data i numer orzeczenia sądu ustalającego ojcostwo, zaprzeczającego ojcostwo, przysposabiającego dziecko, imię i nazwisko osoby przysposabiającej dziecko, data rozwiązania poprzedniego małżeństwa.

Dane osobowe wprowadzane są do systemu informatycznego niezwłocznie po

otrzymaniu sprawy. Dostęp do oprogramowania komputerowego posiadają tylko użytkownicy uprawnieni przez administratora . Posiadają własny login i hasło zmieniane co 30 dni. Kopie awaryjne wykonywane są raz w miesiącu na płyty CD. Kontrola dotępu rejestracji operacji na rekordach i szyfrowanie jest realizowane przez system użytkowy MSQL. Zainstalowano oprogramowanie antywirusowe. Wszystkie operacje logowania i przetwarzania danych są przechowywane w plikach rejestru systemu. Po upływie ustalonego czasu przerwy w pracy systemu monitor zostaje wygaszony.
Dane osobowe przetwarzane w tym zbiorze mogą być udostępniane wyłącznie podmiotom upoważnionym na podstawie przepisów prawa – między innymi: Policji, Sądom , Komornikom. Mogą być także przekazywane do ambasad i polskich konsulatów za granicą.

2. Zbiór danych „Dowody osobiste".

Zbiór danych „ Dowody osobiste" obejmuje: nazwisko i imię, imiona rodziców, datę urodzenia, miejsce urodzenia, adres zamieszkania lub pobytu, numer ewidencyjny PESEL, serię i numer dowodu osobistego, stan cywilny, nazwiska rodziców, nazwiska rodowe, dane dotyczące obywatelstwa. Dostęp do komputera jest możliwy wyłącznie po włożeniu unikatowego klucza i wpisaniu loginu i hasła. Kopie awaryjne wykonywane są raz w miesiącu. Dane do Departamentu Rejestrów Państwowych przesyłane są przy wykorzystaniu tunelu VPN poprzez łącze GSM. Baza danych oprata jest o system SQL Serwer. Kontrola dostępu, rejestracja operacji na rekordach i szyfrowanie reazlizowane jest przez system użytkowy. Zainstalowane zostało oprogramowanie antywirusowe i fajerłol programowy.
Dane osobowe mogą być udostępniane wyłącznie podmiotom upoważnionym na podstawie przepisów prawa między innymi: sądom, prokuraturze, urzędom skarbowym i policji.

3. Zbiór danych „Ewidencja podatków i opłat".

Zbiór danych „Ewidencja podatków i opłat" obejmuje: nazwisko i imiona, imiona rodziców, adres zamieszkania lub pobytu, numer ewidencyjny PESEL.
Dostęp do komputera jest możliwy wyłącznie po podaniu identyfikatora i hasła. Kopie awaryjne wykonywane są raz w miesiącu na płytu CD. Hasło zmieniane jest co 30 dni. Kontrola dostępu rejestracji operacji na rekordach i szyfrowanie jest realizowane przez system bazodanowy FIRE BRID. Zainstalowano oprogramowanie antywirusowe. Wszystkie operacje logowania i przetwarzania danych są przechowywane w plikach rejestru systemu. Po upływie ustalonego czasu przerwy w pracy systemu monitor zostaje wygaszony. Dane ze zbioru mogą być udostępniane wyłącznie podmiotom upoważnionym na podstawie przepisów prawa.

4. **Zbiór danych „ Rejestr wniosków o zwrot podatku akcyzowego zawartego w cenie oleju napędowego wykorzystywanego do produkcji rolnej”.**

Zbiór danych „rejestr wniosków o zwrot podatku akcyzowego zawartego w cenie oleju napędowego wykorzystywanego do produkcji rolnej” obejmuje: nazwisko i imiona, adres zamieszkania lub pobytu, numer ewidencyjny PESEL, Numer Indetyfikacji Podatkowej, serię i numer dowodu osobistego.
Dostęp do komputera jest możliwy wyłącznie po podaniu identyfikatora i właściwego hasła. Kopie awaryjne wykonywane są raz w miesiącu na płyty CD. Hasło jest zmieniane co 30 dni. Kontrola dostępu rejestracji operacji na rekordach i szyfrowanie jest realizowane przez system bazodanowy FIRE BRID. Zainstalowano oprogramowanie antywirusowe. Dane ze zbioru mogą być udostępniane wyłącznie podmiotom upoważnionym na podstawie przepisów prawa.

W odniesieniu do wszystkich zbiorów przetwarzanych w systemie informatycznym zastosowano środki bezpieczeństwa na poziomie podstawowym.

Zbiory danych osobowych przetwarzanych w systemie tradycyjnym są zabezpieczone w zamykanych szafach. W czasie nieobecności pracowników pomieszczenia są zamykane. Budynek Urzędu Gminy zabezpieczony jest alarmem antywłamaniowym. Dane z tych zbiorów udostępniane są wyłącznie podmiotom upoważnionym na podstawie przepisów prawa.

V. Srategia zabezpieczenia danych osobowych (działania niezbędne do zapewnienia poufności, integralności i rozliczalności przetwarznych danych).

1. Bezpieczeństwo osobowe

Administrator danych, zgodnie z ustawą z 22 marca 1990 r. o pracownikach samorządowych (tekst jedn. Dz. U. z 2001 r. Nr 142, poz. 1593 ze zm.), prowadzi nabór na stanowiska urzędnicze w drodze konkursu. Jednym z kryteriów oceny kandydatów jest przedstawienie przez nich zaświadczenia o niekaralności.
Wszyscy pracownicy są dobierani z uwględnieniem ich kompetencji merytorycznych, a także kwalifikacji moralnych. Zwraca się uwagę na takie cechy kandydata, jak: uczciwość, odpowiedzialność, przewidywalność zachowań.

Ryzyko utraty bezpieczeństwa danych przetwarzanych przez administratora danych ze strony osób trzecich jest minimalne. Osoby sprzątające pomieszczenia nie mają dostępu do komputerów i do danych osobowych przetwarzanych w systemie tradycyjnym.

3. Zabezpieczenie sprzętu.

Serwer jest zlokalizowany w odrębnym, klimatyzowanym pomieszczeniu. W pokoju tym może przebywać tylko osoba do spraw obsługi informatycznej, inne osoby upoważnione do przetwarzania danych tylko w towarzystwie osoby prowadzącej obsługę informatyczną , a osoby postronne w ogóle nie mają dostępu.

Wszystkie urządzenia systemu informatycznego administratora danych są zasilane za pośrednictwem zasilaczy awaryjnych (tzw. UPS-ów). Dodatkowo planuje się zastosowanie generatora awaryjnego do zasilania serwera.

Okablowanie sieciowe zostało zaprojektowane w ten sposob, że dostęp do linii teletransmisyjnych jest możliwy tylko z pomieszczeń zamykanych na klucz.

Bieżąca konserwacja sprzętu wykorzystywanego przez administratora danych do ich przetwarzania prowadzona jest tylko przez pracownika do spraw obsługi informatycznej. Natomiast poważne naprawy wykonywane przez personel zewnętrzny realizowane są w siedzibie administratora danych po zawarciu z podmiotem wykonującym naprawę umowy o powierzenie przetwarzania danych osobowych, określającej kary umowne za naruszenie bezpieczeństwa danych.
Wszystkie awarie, działania konserwacyjne i naprawy systemu informatycznego są opisywane w stosownych protokołach podpisywanych przez osoby w nich uczestniczące, a także przez administratora bezpieczeństwa informacji.

Administator systemu dopuszcza konserwowanie i naprawę sprzętu poza siedzibą administratora danych jedynie po trwałym usunięciu danych osobowych. Zużyty sprzęt służący do przetwarzania danych osobowych może być zbywany dopiero po trwałym usunięciu danych osobowych, a urządzenia uszkodzone powinny być przekazywane właściwym podmiotom w celu utylizacji. Zawiera się z nimi umowy powierzenia przetwarzania danych.

Pracownik prowadzący obsługę informatyczną Urzędu wskazuje użytkownikom, jak postępować, aby zapewnić:

1) ochornę elektromagnetyczną nośników danych – dyskietek z danymi, a szczególnie nośników danych, na których przechowywane są kopie zapasowe (należy je przechowywać z dala od magnesów oraz urządzeń wytwarzających pole magnetyczne, a więc nie wprost na urządzeniach komputerowych),
2) prawidłową lokalizację komputerów.

4. Zabezpieczenia we własnym zakresie

Niezwykle ważne dla bezpieczeństwa danych jest wyrobienie przez każdą osobę upoważnioną do przetwarzania danych lub użytkownika nawyku:

1) kasowania po wykorzystaniu danych na dyskach przenośnych,
2) nieużywania powtórnego jednostronnie zadrukowanych dokumentów,

3) niepodawania w rozdzielniku do decyzji do wiadomości stronom informacji o adresach innych (stosowanie załączników do deczyji),
4) zachowania tajemnicy danych, w tym także wobec najbliższych,
5) pilnego strzeżenia akt, dyskietek, pamięci przenośnych i komputerów przenośnych,
6) niepozostawiania bez kontroli dokumentów, nośników danych i sprzętu w hotelach i innych miejscach publicznych ani też w samochodach,
7) ustawiania ekranów komputerowych tak, aby osoby niepowołane nie mogły oglądać ich zawartości, a zwłaszcza nie naprzeciwko wejścia do pomieszczenia,
8) niezapisywania hasła wymaganego do uwierzytelnienia się w systemie na papierze lub innym nośniku,
9) niepodłączania do listew podtrzymujących napięcie, przeznaczonych do sprzętu komputerowego, innych urządzeń, szczególnie tych łatwo powodujących spęcia (np. grzejników, czajników, wentylatorów),
10) dbania o prawidłową wentylację komputerów (nie można zasłaniać im kratek wentylatorów meblami, zasłonami lub stawiać tuż przy ścianie),
11) powstrzymywania się przez osoby upoważnione do przetwarzania danych osobowych od samodzielnej ingerencji w oprogramowanie i konfigurację powierzonego sprzętu (szczególnie komputerów przenośnych), nawet gdy z pozoru mogłoby to usprawnić pracę lub podnieść poziom bezpieczeństwea danych,
12) przestrzegania przez osoby upoważnione do przetwarzania danych osobowych swoich uprawnień w systemie, tj. właściwego korzystania z baz danych, używania tylko własnego identyfikatora i hasła oraz stosowania się do zaleceń administratora bezpieczeństwa informacji,
13) niepozostawiania osób postronnych w pomieszczeniu, w którym przetwarza się dane osobowe, bez obecności osoby upoważnionej do przetwarzania danych osobowych,
14) opuszczania stanowiska pracy dopiero po aktywizowaniu wygaszacza ekranu lub po zablokowaniu stacji roboczej w inny sposób,
15) kopiowania tylko jednostkowych danych (pojedynczych plików), obowiązuje zakaz robienia kopii całych zbiorów danych lub takich ich części, które nie są konieczne do wykonywania obowiązków przez pracownika; jednostkowe dane mogą być kopiowane na nośniki magnetyczne, optyczne i inne po ich zaszyfrowaniu i przechowywane w zamkniętych na klucz szafach; po ustaniu przydatności tych kopii dane należy trwale skasować lub fizycznie zniszczyć nośniki, na których są przechowywane,
16) udostępniania danych osobowych pocztą elektroniczną tylko w postaci zaszyfrowanej,
17) niewynoszenia na jakichkolwiek nośnikach całych zbiorów danych oraz szerokich z nich wypisów, nawet w postaci zaszyfrowanej,
18) wykonywania kopii roboczych danych, na których się właśnie pracuje, tak często, aby zapobiec ich utracie,
19) kończenia pracy na stacji roboczej po wprowadzeniu danych przetwarzanych

tego dnia w odpowiednie obszary serwera, a następnie prawidłowym wylogowaniu się użytkownika i wyłączeniu komputera oraz odcięciu w UPS i listwie,

20) niszczenia w niszczarce lub chowania dokumentów do szaf zamykanych na klucz wszelkich wydruków zawierających dane osobowe, przed opuszczeniem miejsca pracy po zakończeniu dnia pracy,
21) chowania do zamykanych na klucz szaf wszelkich akt zawierających dane osobowe, przed opuszczeniem miejsca pracy po zakończeniu dania pracy,
22) umieszczania kluczy do szaf w ustalonym, przeznaczonym do tego miejscu po zakończeniu dania pracy,
23) zamykania okien w razie opadów lub innych zjawisk atmosferycznych, które mogą zagrozić bezpieczeństwu danych osobowych,
24) zamykania okien w razie opuszczenia pomieszczenia, w tym zwłaszcza po zakończeniu dnia pracy,
25) zamykania drzwi na klucz po zakończeniu pracy w danym dniu i umieszcznia klucza w skrzynce na klucze w pokoju Nr 14.

5. Postępowanie z nośnikami i ich bezpieczeństwo

Osoby upoważnione do przetwarzania danych osobowych powinny pamiętać zwłaszcza, że:

1) dane z nośników po wprowadzeniu ich do systemu informatycznego administratora danych powinny być trwale usuwane z tych nośników przez fizyczne zniszczenie (np. płyty CD – ROM) lub skasowanie danych programem usuwającym trwale pliki; jeśli istnieje uzasdaniona konieczność, to dane pojednyczych osób (a nie całe zbiory czy obszerne wypisy ze zbiorów) mogą być przechowywane w zamkniętych na klucz szafach, nie mogą być udostępniane osobom postronnym; po ustaniu przydatności tych danych nośniki powinny być trwale kasowane lub niszczone,
2) uszkodzone nośniki przed ich wyrzuceniem należy zniszczyć fizycznie (przeciąć, przełamać),
3) po wykorzystaniu wydruki zawierające dane osobowe należy codziennie przed zakończeniem pracy zniszczyć w niszczrce; jeżeli to możliwe, nie należy przchowywać takich wydruków na biurku ani wynosić poza siedzibę administratora danych,
4) zabrania się powtórnego używania do sporządzania brudnopisów pism jednostronnie zadrukowanych kart, jeśli zawierają one chronione dane; zaleca się natomiast dwustronne drukowanie brudnopisów pism i sporządzanie dwustronnych dokumentów.

6. Wymiana danych i ich bezpieczeństwo

Bezpieczeństwo danych, a w szczególności ich integralność i dostępność w dużym stopniu zależy od zdyscyplinowanego, codziennego umieszczania danych w

wyznaczonych zasobach serwera. Pozwala to – przynajmniej w pewnym stopniu – uniknąć wielokrotnego wprowadzania tych samych danych do sytemu informtycznego administratora danych.

Sporządzanie kopii zapasowych odbywa się przynajmniej raz w miesiącu na nośniku DVD. Kopie zapasowe przechowywane są w kasie pancernej w innym pomieszczeniu niż te, w którym przetwarza się dane osobowe.

Inne wymogi bezpieczeństwa systemowego określają instrukcje obsługi producentów sprzętu i używanych programów, wskazówki administratora bezpieczeństwa informacji oraz „Instrukcja zarządzania systemem informatycznym służącym do przetwarzania danych osobowych".

Przed atakami z sieci zewnętrznej wszystkie komputery administratora danych chronione są środkami dobranymi przez administratora systemu i administartora bezpieczeństwa informacji. Ważne jest, aby użytkownicy zwracali uwagę na to, czy urządzenie, na którym pracują, domaga się aktualizacji tych zabezpieczeń. O wszystkich takich przypadkach należy informować administratora bezpieczeństwa inrormacji oraz umożliwić mu monitorowanie oraz aktualizację środków (urządzeń, programów) bezpieczeństwa.

Administrator bezpieczeństwa informacji dobiera elektroniczne środki ochrony przed atakami z sieci stosownie do pojawienia się nowych zagrożeń (nowe wirusy, robaki, trojany, inne możliwości wdarcia się do systemu), a także stosownie do rozbudowy systemu informatycznego administratora danych i powiększenia bazy danych. Jednocześnie należy zwracać uwagę, czy rozwijający się system zabezpieczeń sam nie powoduje nowych zagrożeń.

7. Kontrola dostępu do systemu

Poszczególnym osobom upoważnionym do przetwarzania danych osobowych przydziela się konta opatrzone niepowtarzalnym identyfikatorem umożliwiające dostęp do danych, zgodnie z zakresem upoważnienia do przetwarzania danych osobowych. Administrator systemu po uprzednim przedłożeniu upoważnienia do przetwarzania danych osobowych, stosownie do wniosku Kierownika Referatu Organizacyjnego Spraw Obywatelskich i Kadr przydziela pracownikowi upoważnionemu do przetwarzania danych konto w systemie informatycznym dostępne po wprowadzeniu prawidłowego identyfikatora i uwierzytelnieniu hasłem. System wymusza zmianę hasła przy pierwszym logowaniu.

W razie potrzeby administrator systemu może przydzielić konto opatrzone identyfikatorem osobie upoważnionej do przetwarzania danych osobowych niemającej statusu pracownika.

Pierwsze hasło wymagane do uwierzytelnienia się w systemie przydzielane jest przez administratora systemu po odebraniu od osoby upoważnionej do przetwarzania danych oświadczenia zawierającego zobowiązanie do zachowania w tejemnicy pierwszego i następnych haseł oraz potwierdzenie odbioru pierwszego hasła.

Do zagwarantowania poufności i integralności danych osobowych konieczne jest przestrzeganie przez użytkowników swoich uprawnień w systemie, tj.

właściwego korzystania z baz danych, używania tylko własnego identyfikatora i hasła oraz stosowanie się do zaleceń administratora bezpieczeństwa informacji.

8. Kontrola dostępu do sieci.

System informatyczny posiada szerokopasmowe połączenie z internetem. Dostęp do niego jest jednak ograniczony. Na poszczególnych stacjach roboczych można przeglądać tylko wyznaczone strony www.

Korzystanie z zasobów sieci wewnętrznej (intranet) jest możliwe tylko w zakresie uprawnień przypisanych do danego konta osoby upoważnionej do przetwarzania danych osobowych.

Osoba prowadząca obsługę informatyczną w Urzędzie Gminy z własnej inicjatywy lub na wniosek Administratora danych dokonuje zmian ustawień systemu w celu uniemożliwiania przeglądania wybranych stron www.

10. Przeglądy okresowe zapobiegające naruszeniom obowiązku szczególnej staranności administratora danych.

Administrator bezpieczeństwa informacji przeprowadza raz w roku przegląd przetwarzanych danych osobowych pod kątem celowości ich dalszego przetwarzania. Osoby upoważnione do przetwarzania danych osobowych, w tym zwłaszcza kierownicy poszczególnych referatów, są obowiązane współpracować z administratorem bezpieczeństwa informacji w tym zakresie przez wypełnienie kwestionariuszy przeglądu i w razie potrzeby udzielenie innych koniecznych informacji.

Administrator bezpieczeństwa informacji może zarządzić przeprowadzenie dodatkowego przeglądu w wyżej określonym zakresie w razie zmian w obowiązującym prawie, ograniczających dopuszczalny zakres przetwarzanych danych osobowych. Dodatkowy przegląd może być konieczny także w sytuacji zmian organizacyjnych administratora danych.

Z porzebiegu usuwania danych osobowych należy sporządzić protokoł podpisany przez administratora bezpieczeństwa informacji i kierownika referatu, w którym usunięto dane osobowe.

11. Szkolenia osób upoważnionych do przetwarzania danych

Administrator bezpieczeństwa informacji przyjmuje plan szkoleń. Zgodnie z planem szkoli się każdą osobę, która ma zostać upoważniona do przetwarzania danych osobowych. Szkolenia wewnętrzne wszystkich osób upoważnionych do przetwarzania danych osobowych przeprowadzane są w wypadku każdej zmiany zasad lub procedur ochrony danych osobowych.

Tematyka szkoleń obejmuje:

1) przepisy i instrukcje dotyczące ochrony danych osobowych, sporządzania i przechowywania ich kopii, niszczenia wydruków i zapisów na nośnikach,
2) sposoby ochrony danych przed osobami postronnymi i procedury udostępniania danych osobm, których one dotyczą,
3) obowiązki osób upoważnionych do przetwarzania danych osobowych,
4) zasady i procedury określone w polityce bezpieczeństwa.

12. Odpowiedzialność osób upoważnionych do przetwarzania danych osobowych.

Niezastosowanie się do prowadzonej przez administratora danych polityki bezpieczeństwa przetwarzanych danych osobowych, której założenia określa niniejszy dokument i naruszenie procedur ochrony danych przez pracowników upoważnionych do przetwarzania danych osobowych może być potraktowane jako ciężkie naruszenie obowiązków pracowniczych, podlegające sankcjom dyscyplinarnym oraz sankcjom karnym, w szczególności wynikającym z art. 51 – 52 ustawy oraz art. 266 Kodeksu karnego.

VI. Przeglądy polityki bezpieczeństwa i audyty systemu

Polityka bezpieczeństwa powinna być poddawana przeglądowi przynajmniej raz na rok. W razie istotnych zmian dotyczących przetwarzania danych osobowych administrator bezpieczeństwa informacji może zarządzić przegląd polityki bezpieczeństwa stosownie do potrzeb.

Administrator bezpieczeństwa informacji analizuje, czy polityka bezpieczeństwa i pozostała dokumentacja jest adekwatna do zmian:
1) w budowie systemu informatycznego,
2) zmian organizacyjnych administratora danych, w tym również zmian statutsu osób upoważnionych do przetwarzania danych osobowych,
3) zmian w obowiązującym prawie.

Administrator bezpieczeństwa informacji po uzgodnieniu z Wójtem może, stosownie do potrzeb, przeprowadzić audyt18 systemu informatycznego. Przeprowadzenie audytu wymaga uzgodnienia jego zakresu z administratorem systemu. Zakres, przebieg i rezulataty audytu dokumentowane są na piśmie w protokole podpisywanym zarówno przez administratora bezpieczeństwa informacji i osobę prowadzącą obsługę informatyczną.

Wójt, w razie konieczności, może zlecić przeprowadzenie audytu zewnętrznego przez wyspecjalizowany podmiot.

VII. Postanowienia końcowe

Każda osoba upoważniona do przetwarzania danych osobowych zobowiązana

jest zapoznać się przed dopuszczeniem do przetwarzania danych z niniejszym dokumentem oraz złożyć stosowne oświadczenie potwierdzające znajomość jego treści.

Polityka bezpieczeństwa wchodzi w życie z dniem 1 kwietnia 2008 r.

Załącznik Nr 1

....
(pieczęć administratora danych) (miejscowość data)

U P O W A Ż N I E N I E

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

Panią/Pana .....
(imię i nazwisko, stanowisko)

do przetwarzania danych osobowych w w zbiorze danych/zbiorach danych*

.....

.....

.....

.....

.....

w następującym zakresie:

1. .....

.....

2. .....

.....

3. .....

.....

.....

4. .....

.....

5. .....

.....

wyłącznie w związku z wykonywaniem obowiązków pracowniczych (służbowych) zleceniobiorcy*

Upoważnienie jest udzielone na czas trwania zatrudnienia (do odwołania) od .....
do .....*

....
(podpis osoby reperezentującej administratora danych)

Wnoszę/nie wnoszę* o nadanie identyfikatora użytkownika i przyznanie hasła

.....
(podpis Kierownika Ref. Organizacyjnego
Spraw Obywatelskich i Kadr)

.....
(data i podpis osoby upoważnionej)

Pouczenie: osoba upoważniona do przetwarzania danych jest zgodnie z art. 39 ust. 2 ustawy o ochronie danych osobowych obowiązana zachować w tajemnicy dane osobowe oraz sposoby ich zabezpieczenia, w tym także po ustaniu zatrudnienia (odwołaniu upoważnienia) upływie jego ważności. Ponadto podlega odpowiedzialności karnej wynikającej z art. 51 – 52 ustawy o ochronie danych osobowych, a także art. 266 Kodeksu karnego.

- niepotrzebne skreślić

Załącznik Nr 2

ZOBOWIĄZANIE

Oświadczam, że zapoznałem(am) się z dokumentem polityki bezpieczeństwa oraz instrukcją zarządzania systemem informatycznym służącym do przetwarzania danych osobowych ustalonymi w załączniku do zarządzenia Wójta Gminy w Małkini Górnej Nr 10/08 z dnia 1 kwietnia 2008 r.

Zobowiązuję się przestrzegać zasad i procedur ochrony danych osobowych określonych w ww. dokumentach oraz nie ujawniać informacji zawartych w tych dokumentach, a także danych osobowych, które przetwarzam u administratora danych.

Powyższe informacje zobowiązuję się zachować w tajemnicy przez cały okres zatrudnienia u administratora danych, a także po jego ustaniu.

Oświadczam, że jestem świadomy (świadoma) odpowiedzialności karnej, wynikającej z art. 51 – 52 ustawy o ochronie danych osobowych oraz art. 266 Kodeksu karnego.

Małkinia Górna, dnia .....

.....
(czytelny podpis)

Załącznik Nr 2

do zarządzenia Nr 10/08
Wójta Gminy w Małkini Górnej

INSTRUKCJA ZARZĄDZANIA SYSTEMEM INFORMATYCZNYM SŁUŻĄCYM DO PRZETWARZANIA DANYCH OSOBOWYCH

12)Cel instrukcji

Instrukcja określa sposób zarządzania systemem informatycznym wykorzystywanym do przetwarzania danych osobowych przez administratora danych w celu zabezpieczenia danych osobowych przed zagrożeniami a zwłaszcza przed ich udostępnieniem osobom nieupoważnionym, nieautoryzowana zmianą, utratą, uszkodzeniem lub zniszczeniem.

Definicje

Ilekroć w Instrukcji jest mowa o:

2. ustawie – rozumie się przez to ustawę z 29 sierpnia 1997 r. o ochronie danych osobowych (tekst jedn. Dz. U. z 2002 r. Nr 101, poz. 926 ze zm.),
3. rozporządzeniu – rozumie się przez to rozporządzenie 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),
4. administratorze danych – rozumie się przez to Urząd Gminy reprezentowany przez Wójta,
5. administratorze bezpieczeństwa informacji – rozumie się przez to osobę, której administrator danych powierzył pełnienie obowiązków administratora bezpieczeństwa informacji,
6. administratorze systemu – rozumie się przez to osobę zatrudnioną na stanowisku ds. Obsługi informatycznej zatrudnionej w administratora danych,
7. osobie upoważnionej do przetwarzania danych osobowych – rozumie się przez to osobę zatrudnioną na podstawie umowy o pracę, umowy zlecenia lub innej umowy, osobę odbywającą u administratora danych staż absolwencki, praktykę studencką, wolontariat, której nadane zostało przez administratora danych upoważnienie do przetwarzania danych osobowych,
8. użytkowniku – rozumie się prze to osobę upoważnioną do przetwarzania danych osobowych, której nadano uprawnienia do przetwarzania danych w systemie informatycznym,
9. systemie informatycznym administratora danych – rozumie się przez to sprzęt komputerowy, oprogramowanie, dane eksploatowane w zespole

współpracujących ze sobą urządzeń, programów procedur przetwarzania informacji i narzędzi programowych; w systemie tym pracuje co najmniej jeden komputer centralny i system ten tworzy sieć teleiformatyczną administratora danych,

10. identyfikatorze użytkownika – rozumie się przez to ciag znaków literowych, cyfrowych lub innych jednoznacznie identyfikujący osobę upoważnioną do przetwarzania danych osobowych w wyznaczonych przez administratora danych osobowych obszarach systemu informatycznego administratora danych,
11. haśle – rozumie się przez to ośmioznakowy ciąg znaków literowych, cyfrowych zawierający duże i małe litery oraz znaki specjalne, znany jedynie osobie, które nadano identyfikator użytkownika,
12. odbiorcy danych – rozumie się przez to każdego, komu udostępnia się dane osobowe, z wyłączeniem:
    a) osoby, której dane dotyczą,
    b) osoby, upoważnionej do przetwarzania danych,
    c) przedstawiciela, o którym mowa w art. 31 a ustawy,
    d) podmiotu, o którym mowa w art. 31 ustawy,
    e) organów państwowych lub organów samorządu terytorialnego, którym dane są udostępniane w związku z prowadzonym postępowaniem,
13. serwisancie – rozumie się przez to firmę lub pracownika firmy zajmującej się sprzedażą, instalacją, naprawą i konserwacją sprzętu komputerowego

19) Poziom bezpieczeństwa

Uwzględniając kategorie danych osobowych oraz konieczność zachowania bezpieczeństwa ich przetwarzania w systemie informatycznym połączonym z siecią publiczną, wprowadza się „poziom podstawowy” bezpieczeństwa w rozumieniu § 6 rozp.

3. Nadawanie i rejestrowanie (wyrejestrowywanie) uprawnień do przetwarzania danych w systemie informatycznym

4. Dostęp do systemu informatycznego służącego do przetwarzania danych osobowych może uzyskać wyłącznie osoba upoważniona do przetwarzania danych osobowych zarejestrowana jako użytkownik w tym systemie przez administratora systemu na wniosek Kierownika Referatu Organizacyjnego, Spraw Obywatelskich i Kadr.
5. Rejestracja użytkownika, o której mowa w pkt 1, polega na nadaniu identyfikatora i przydzieleniu hasła oraz wprowadzeniu tych danych do bazy użytkowników systemu.
6. Rejestracja użytkownika, o której mowa w pkt. 1, polega na nadaniu identyfikatora i przydzieleniu hasła oraz wprowadzeniu tych danych do bazy użytkowników systemu.
7. Administrator systemu przekazuje do Referatu Organizacyjnego Spraw

Obywatelkich i Kadr informację o identyfikatorze, który został nadany użytkownikowi.

III. Metody i środki uwierzytelnienia oraz procedury związane z ich zarządzaniem i użytkowaniem

7) Identyfikator składa się z minimum sześciu znaków, z których pierwszy odpowiada pierwszej literze imienia użytkownika, a reszta znaków składa się z nazwiska.
8) W wypadku zbieżności nadawanego identyfikatora z identyfikatorem wcześniej zarejestrowanego użytkownika administrator systemu, nadaje inny identyfikator odstępując od zasady określonej w pkt 1.
9) Hasło powinno składać się z niepowtarzalnego zestawu co najmniej ośmiu znaków, zawierać małe i wielkie litery oraz cyfry lub znaki cpecjalne. Hasło nie może być identyczne z identyfikatorem użytkownika ani z jego imieniem lub nazwiskiem.
10) System informatyczny wymusza zmianę hasła co 30 dni. Administrator bezpieczeństwa informacji może, w uzsadnionych sytuacjach polecić dokonanie zmiany hasła przez użytkownika.
11) Zabrania się użytkownikom systemu udostępniania swojego identyfikatora i hasła innym osobom oraz korzystania przez osoby upoważnione do przetwarzania danych osobowych z identyfikatora lub hasła innego użytkownika.
12) Wyrejestrowania użytkownika z systemu informatycznego dokonuje administrator systemu na wniosek kierownika Referatu Organizacyjnego, Spraw Obywatelskich i Kadr.
13) Wyrejestrowanie może mieć charakter czasowy lub trwały.
14) Wyrejestrowanie następuje przez:
    1) zablokowanie konta użytkownika do czasu ustania przyczyny uzasadniającej blokadę (wyrejestrowanie czasowe),
    2) usunięcie danych użytkownika z bazy użytkowników systemu (wyrejestrowanie trwałe).
15) Przyczyną czasowego wyrejestrowania użytkownika z systemu informatycznego może być:
    1) wypowiedzenie umowy o pracę,
    2) wszczęcie postępowania dyscyplinarnego względem osoby upoważnionej do przetwarzania danych osobowych.
16) Przyczyną trwałego wyrejestrowania użytkownika z systemu informatycznego jest rozwiązanie lub wygaśnięcie stosunku pracy lub innego stosunku prawnego, w ramach którego zatrudniony był użytkownik.
17) Hasło administratora systemu przechowywane jest w zalakowanej kopercie w kasie pancernej.

3. Procedury rozpoczęcia, zawieszenia i zakończenia pracy przeznaczone dla użytkowników systemu

Tryb pracy na poszczególnych stacjach roboczych

12) Rozpoczęcie pracy na stacji roboczej następuje po włączeniu napięcia w listwie podtrzymującej napięcie, włączeniu zasilacza awaryjnego (UPS) i komputera, a następnie wprowadzeniu indywidualnego, znanego tylko użytkownikowi, hasła i identyfikatora.
13) W pomieszczeniu, w którym przetwarzane są dane osobowe, mogą znajdować się osoby postronne tylko za zgodą i w towarzystwie użytkownika albo administratora bezpieczeństwa informacji.
14) Przed osobami postronnymi należy chornić ekrany komputerów (ustawienie monitora powinno uniemożliwić podgląd), wydruki leżące na biurkach oraz w otwartych szafach.
15) Monitory komputerów wyposażone są we włączające się po 10 minutach od przerwania pracy wygaszacze ekranu. Wznowienie wyświetlenia następuje po wpisaniu nazwy użytkownika i podaniu hasła.
16) W przypadku opuszczania stanowiska pracy użytkownik obowiązany jest aktywizować wygaszacz ekranu lub w inny sposób zablokować stację roboczą.
17) Obowiązuje zakaz robienia kopii całych zbiorów danych. Całe zbiory danych mogą być kopiowane tylko przez administratora systemu lub automatycznie przez system, z zachowaniem procedur ochrony danych osobowych.
18) Jednostkowe dane mogą być kopiowane na nośniki magnetyczne, optyczne i inne po ich zaszyfrowaniu i przechowywane w zamkniętych na klucz szafach. Po ustaniu przydatności tych kopii dane należy trwale skasować lub fizycznie zniszczyć nośniki, na których są przechowywane.
19) Jednostkowe dane mogą być przekazywane pocztą elektorniczną między komputerami administratora danych a komputerami przenośnymi użytkowników tylko po ich zaszyfrowaniu.
20) Wypisy ze zbiorów danych udostępniane na podstawie art. 29 ustawy podmiotom niebędącym odbiorcami danych można przesyłać pocztą elektroniczną tylko w postaci zaszyfrowanej.
21) Obowiązuje zakaz wynoszenia na jakichkolwiek nośnikach całych zbiorów danych oraz obszernych z nich wypisów, nawet w postaci zaszyfrowanej.
22) Przetwarzając dane osobowe, należy odpowiednio często robić kopie robocze danych, na których się właśnie pracuje, tak aby zapobiec ich utracie.
23) Zakończnie pracy na stacji roboczej następuje po wprowadzeniu danych tego dnia przetwarzanych w odpowiednie obszary serwera, a nastepnie prawidłowym wylogowaniu się użytkownika i wyłączeniu komputera oraz odcięciu napięcia w zasilaczu awaryjnym (UPS) i listwie.
24) Przed opuszczeniem pokoju należy:
    1) zniszczyć w niszczarce lub schować do zamykanych na klucz szaf wszelkie wykonane wydruki zawierające dane osobowe,
    2) schować do zamykanych na klucz szaf wszelkie akta zawierające dane osobowe,
    3) umieścić klucze do szaf w ustalonym, przeznaczonym do tego miejscu,

4) zamknąć okna.

14. Opuszczając pokój, należy zamknąć za sobą drzwi na klucz. Klucz jest przechowywany w skrzynce na klucze w pokoju Nr 14.

4. Procedury tworzenia kopii zapasowych

12) Kopie zapasowe tworzy się:
1) codziennie – w wypadku zbioru „Kadry i wynagrodzenia”,
2) kwartalnie, na płycie DVD przechowywanej w kasie pancernej – w wypadku całego systemu.

13) Każdą kopię tworzy się na oddzielnym nośniku informatycznym.

14) Zabrania się przechowywania kopii zapasowych w pomieszczeniach przeznaczonych do przechowywania zbiorów danych pozostających w bieżącym użytkowaniu.

15) Administrator systemu przegląda okresowo kopie zapasowe i ocenia ich przydatność do odtwarzania zasobów systemu w wypadku jego awarii.

16) Stwierdzenie utraty przez kopie awaryjne waloru przydatności do celu, o którym mowa w ust. 4, upoważnia administratora systemu do ich zniszczenia.

5. Przechowywanie elektronicznych nośników informacji zawierających dane osobowe oraz ich kopii zapasowych

6. Zbiory danych przechowywane są generalnie na serwerze obsługującym system informatyczny administratora danych. Wszelkie dane przetwarzane w pamięci poszczególnych stacji roboczych są niezwłocznie umieszczane w odpowiednich miejscach na serwerze, przydzielonych każdemu użytkownikowi przez administratora systemu.
7. Zakazuje się przetwarzania danych osobowych na zewnętrznych nośnikach magnetycznych, optycznych i innych oraz ich przesyłania pocztą elektorniczną bez ich uprzedniego zaszyfrowania.
8. Na nośnikach, o których mowa w ust. 2, dopuszczalne jest przetwarzanie jedynie jednostkowych danych osobowych.
9. W przypadku posługiwania się nośnikami danych pochodzącymi od podmiotu zewnetrznego użytkownik jest zobowiązany do sprawdzenia go programem antywirusowym na wyznaczonym w tym celu stanowisku komputerowym oraz do oznakowania tego nośnika.
10. Nośniki magnetyczne raz użyte do przetwarzania danych osobowych nie mogą być wykorzystywane do innych celów, mimo że usunięto z nich dane i podlegają ochronie w trybie niniejszej instrukcji.
11. Nośniki magnetyczne z zaszyfrowanymi, jednostkowymi danymi osobowymi są – na czas ich użyteczności – przechowywane w zamkniętych na klucz szafach, a po ich wykorzystaniu dane na nich zawarte są trwale usuwane lub nośniki te są niszczone.
12. Nośniki informatyczne przechowywane są w miejscach, do których dostęp mają wyłącznie osoby upoważnione do przetwarzania danych osobowych.

13. Zabrania się przechowywania kopii zapasowych w pomieszczeniach przeznaczonych do przechowywania zbiorów danych pozostających w bieżącym użytkowaniu. Jednocześnie kopie zapasowe muszą być odpowiednio zabezpieczone fizycznie (szfa metalowa, w zabezpieczonym pomieszczeniu).
14. Kopie zapasowe mogą być przechowywane tylko w tych pomieszczeniach, w których jest zainstalowany system wykrywania pożaru.
15. Administrator systemu przeprowadza okresowe (co 3 miesiące) weryfikacje przydatności sporządzonych kopii do ewentualnego odtwarzania danych.
16. Kopie zapasowe programów i kwartalnie aktualizowane kopie systemu informatycznego administratora danych przechowywane są w szafie metalowej stojącej w innym pomieszczeniu niż serwery. Po wygasnięciu przydatności tych kopii są one trwale kasowane lub nośniki je przechowujące są niszczone mechanicznie w niszczarce.
17. Codziennie kopie danych przetwarzanych na serwerze przechowywane są w zamkniętych na klucz szafach.

4) Sposób zabezpieczenia systemu informatycznego przed działalnością oprogramowania, którego celem jest uzyskanie nieuprawnionego dostępu do systemu informatycznego

IV. Sprawdzanie obecności wirusów komputerowych w systemie informatycznym oraz ich usuwanie odbywa się za pomocą licencjowanego oprogramowania zainstalowanego na serwerach, stacjach roboczych oraz komputerach przenośnych przez administratora systemu.
V. Oprogramowanie, o którym mowa w ust. 1, sprawuje ciągły nadzór (ciągła praca w tle) nad pracą systemu i jego zasobami oraz serwerami i stacjami roboczymi.
VI. Niezależnie od ciągłego nadzoru, o którym mowa w ust. 2, administrator systemu nie rzadziej niż raz na tydzień przeprowadza pełną kontrolę obecności wirusów komputerowych w systemie oraz jego zasobach, jak również w serwerach i stacjach roboczych.
VII. Do obowiązków administratora systemu należy aktualizacja oprogramowania antywirusowego oraz określenie częstotliwości automatycznych aktualizacji definicji dokonywanych przez to oprogramowanie.
VIII. Użytkownik jest obowiązany zawiadomić administratora systemu o pojawiających się komunikatach wskazujących na wystąpienie zagrożenia wywołanego szkodliwym oprogramowaniem.
IX. Użytkownicy mogą korzystać z zewnętrznych nośników danych tylko na stanowisku wydzielonym z sieci komputerowej administratora danych, po uprzednim sprawdzeniu zawartości nośnika oprogramowaniem antywirusowym.
X. Dostęp do internetu możliwy jest na kilku stacjach roboczych chronionych urządzeniem sprzętowym z wbudowanym programem Firewall i translacją adresów NAT.

4. **Kontrola nad wprowadzaniem, dalszym przetwarzaniem i udostępnianiem danych osobowych**

V. System informatyczny administartora danych umożliwia automatycznie:
1) przypisanie wprowadzonych danych użytkownikowi (identyfikatorowi użytkownika), który te dane wprowadza do systemu,
2) sygnalizację wygaśnięcia czasu obowiązywania hasła dostępu do stacji roboczej,
3) sporządzenie i wydrukowanie dla każdej osoby, której dane są przetwarzane w systemie, raportu zawierajacego:
a) datę pierwszego wprowadzenia danych do systemu administratora danych,
b) identyfikator użytkownika wprowadzającego te dane,
c) źródła danych w przypadku zbierania danych nie od osoby, ktorej one dotyczą,
d) informacje o odbiorcach danych, którym dane osobowe zostały udostępnione,
e) sprzeciwu, o którym mowa w art. 32 ust. 1 pkt. 8 ustawy.

VI. Odnotowanie informacji, o których mowa w ust. 1 pkt. 3, następuje automatycznie po zatwierdzeniu przez użytkownika operacji wprowadzenia danych.

XI. Procedury wykonywania przeglądów i konserwacji systemów oraz nośników informacji służących do przetwarzania danych

1. Przeglądu i konserwacji systemu dokonuje administrator systemu doraźnie.
2. Przeglądu pliku zawierającego raport dotyczący działalności aplikacji bądź systemu (log systemowy) administrator systemu dokonuje nie rzadziej niż raz na tydzień.
3. Przeglądu i sprawdzenia poprawności zbiorów danych zawierających dane osobowe dokonuje użytkownik przy współudziale administratora systemu nie rzadziej niż raz na miesiąc.
4. Zapisy logów systemowych powinny być przeglądane przez administratora systemu codziennie oraz każdorazowo po wykryciu naruszenia zasad bezpieczeństwa.
5. Kontrole i testy przeprowadzane przez administratora bezpieczeństwa informacji powinny obejmować zarówno dostęp do zasobów systemu, jak i profile oraz uprawnienia poszczególnych użytkowników.

XII. Naprawy urządzeń komputerowych z chronionymi danymi osobowymi

1. Wszelkie naprawy urządzeń komputerowych oraz zmiany w systemie

informatycznym administratora danych przeprowadzane są – jeżeli jest to możliwe przez pracownika ds. Obsługi informatycznej Urzędu.

2. Naprawy i zmiany w systemie informatycznym administratora danych przeprowadzane prze serwisanta prowadzone są pod nadzorem administratora systemu, jeżeli jest to możliwe – w siedzibie administratora danych lub poza siedzibą administratora danych, po uprzednim nieodwrcalnym usunięciu danych w nich przetwarzanych, a jeżli wiązałoby się to z nadmiernymi utudnieniami, to po podpisaniu umów powierzenia przetwarzania danych osobowych.
3. Jeśli nośnik danych (dysk, dyskietka, płyta lub inne) zostanie uszkodzony i nie można go odczytać ani usunąć z niego danych, to należy go zniszczyć mechanicznie w niszczarce.

2. Postępowanie w przypadku stwierdzenia naruszenia bezpieczeństwa systemu informatycznego

3. Użytkownik zobowiązny jest zawiadomić administratora bezpieczeństwa informacji o każdym naruszeniu lub podejrzeniu naruszenia bezpieczeństwa systemu, a w szczególności o:
   1) naruszeniu hasła dostępu i identyfikatora (system nie reaguje na hasło lub je ignoruje bądź można przetwarzać dane bez wprowadzenia hasła),
   2) częściowym lub całkowitym braku danych albo dostępie do danych w zakresie szerszym niż wynikający z przyznanych uprawnień,
   3) braku dostępu do właściwej aplikacji lub zmianie zakresu wyznaczonego dostępu do zasobów serwera,
   4) wykryciu wirusa komputerowego,
   5) zauważeniu elektronicznych śladów próby włamania do systemu informatycznego administratora danych,
   6) znacznym spowolnieniu działania systemu informatycznego,
   7) podejrzeniu kradzieży sprzętu komputerowego lub dokumentów zawierających dane osobowe,
   8) zmianie położenia sprzętu komputerowego,
   9) zauważeniu śladów usiłowania lub dokonania włamania do pomieszczeń lub zamykanych szaf.
4. Do czasu przybycia na miejsce administratora bezpieczeństwa informacji należy:
   1) jeżeli istnieje taka możliwość, niezwłocznie podjąć czynności niezbędne do powstrzymania niepożądanych skutków zaistniałego zdarzenia, a następnie uwzględnić w działaniu również ustalenie jego przyczyn lub sprawców,
   2) rozważyć wstrzymanie bieżącej pracy na komputerze lub pracy biurowej w celu zabezpieczenia miejsca zdarzenia,
   3) zaniechać – jeżeli to możliwe – dalszych planowanych przedsięwzięć, które wiążą się z zaistniałym naruszeniem i mogą utrudnić udokumentowanie i analizę,

4) zastosować się do instrukcji i regulaminów lub dokumentacji aplikacji, jeśli odnoszą się one do zaistniałego przypadku,
5) przygotować opis incydentu,
6) nie opuszczać bez uzasadnionej przyczyny miejsca zdarzenia do czasu przybycia administratora bezpieczeństwa informacji.

5. Administrator bezpieczeństwa informacji po otrzymaniu informacji o naruszeniu bezpieczeństwa systemu informatycznego powinien niezwłocznie:
   1) przeprowadzić postępowanie wyjaśniające, w celu ustalenia okoliczności naruszenia ochrony danych osobowych,
   2) podjąć działania chroniące system przed ponownym naruszeniem,
   3) w przypadku stwierdzenia faktycznego naruszenia bezpieczeństwa systemu sporządzić raport naruszenia bezpieczeństwa systemu informatycznego administratora danych (wzór w załączniku), a następnie niezwłocznie przekazać jego kopię administratorowi danych.
6. Administrator bezpieczeństwa informacji w uzgodnieniu z administratorem danych może zarządzić, w razie potrzeby, odłączenie części systemu informatycznego dotkniętej incydentem od pozostałej jego części.
7. W razie odtwarzania danych z kopii zapasowych administrator systemu obowiązany obowiązany jest upewnić się, że odtwarzane dane zapisane zostały przed wystąpieniem incydentu; dotyczy to zwłaszcza przypadków infekcji wirusowej.
8. Administrator danych po zapoznaniu się z raportem. O którym mowa w ust. 3 pkt 3, podejmuje decyzję o dalszym trybie postępowania, powiadomieniu właściwych organów oraz podjęciu innych, szczególnych czynności zapewniających bezpieczeństwo systemu informatycznego administratora danych bądź zastosowaniu środków ochrony fizycznej.
9. Administrator bezpieczeństwa informacji jest zobowiązany do informowania administratora danych o awariach systemu informatycznego, zauważonych przypadkach naruszenia niniejszej instrukcji przez użytkowników, a zwłaszcza o przypadkach posługiwania się przez użytkowników nieautoryzowanymi programami, nieprzestrzegania zasad używania oprogramowania antywirusowego, niewłaściwego wykorzystania sprzętu komputerowego lub przetwarzania danych w sposób niezgodny z procedurami ochrony danych osobowych.
10. Administrator bezpieczeństwa informacji składa raz w roku administratorowi danych kompleksową analizę zarządzania systemem informatycznym.

5. Postanowienia końcowe

VI. W sprawach nieokreślonych niniejszą instrukjcą należy stosować instrukcje obsługi i zalecenia producentów aktualnie wykorzystywanych urządzeń i programów.

VII. Każda osoba upoważniona do przetwarzania danych osobowych zobowiązana jest zapoznać się przed dopuszczeniem do przetwarzania danych z niniejszą instrukcją oraz złożyć stosowne oświadczenie potwierdzające znajomość jej

treści.

VIII. Naruszenie obowiązków wynikających z niniejszej instrukcji oraz przepisów o ochronie danych osobowych może być uznane za ciężkie naruszenie obowiązków pracowniczych, podlegające sankcjom dyscyplinarnym oraz sankcjom karnym, w szczególności wynikającym z art. 51 – 52 ustawy.

RAPORT
stwierdzenia naruszenia bezpieczeństwa systemu informatycznego administratora danych

1. Data .....godzina .....

2. Osoba powiadamiająca o zaistniałym zdarzeniu:

.....
(imię, nazwisko, stanowisko służbowe)

3. Lokalizacja zdarzenia:

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

4. Rodzaj naruszenia bezpieczeństwa oraz okoliczności towarzyszące:

.....

.....

.....

5. Przyczyny wystąpienia zdarzenia:

.....

.....

.....

6. Podjęte działania:

.....

.....

.....

7. Postępowanie wyjaśniające:

.....

.....

.....

8. Uwagi:

.....

.....

.....

.....
data sporządzenia:

.....
(podpis administratora bezpieczeństwa informacji)