ZARZĄDZENIE NR 102/12
WÓJTA GMINY TRZCIANNE

z dnia 8 listopada 2012 r.

w sprawie ustanowienia Polityki Bezpieczeństwa Informacji, Instrukcji Zarządzania Systemem Informatycznym i Instrukcji Zasad Udostępniania Danych Osobowych w Urzędzie Gminy Trzcianne

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

§ 1. 1. Ustanawia się Politykę Bezpieczeństwa Informacji stanowiącą Załącznik Nr 1 do niniejszego zarządzenia.

2. Ustanawia się Instrukcję Zarządzania Systemem Informatycznym służącym do przetwarzania danych osobowych stanowiącą Załącznik Nr 2 do niniejszego zarządzenia.

3. Ustanawia się Instrukcję Zasad Udostępniania Danych Osobowych stanowiącą Załącznik Nr 3 do niniejszego zarządzenia.

§ 2. Dokumenty, o których mowa w ust. 1-3 mają zastosowanie na wszystkich stanowiskach pracy, na których, przetwarzane są dane osobowe w Urzędzie Gminy Trzcianne.

§ 3. Z treścią instrukcji, o których mowa w § 1, Sekretarz Gminy zapoznaje wszystkich pracowników zatrudnionych przy przetwarzaniu danych osobowych.

§ 4. Wykonanie Zarządzenia powierza się Sekretarzowi Gminy Trzcianne.

§ 5. Zarządzenie wchodzi w życie z dniem podpisania.

Wójt Gminy Trzcianne

Zdzisław Dąbrowski

Załącznik Nr 1 do Zarządzenia Nr 102/12

Wójta Gminy Trzcianne

z dnia 8 listopada 2012 r.

Polityka Bezpieczeństwa Informacji w Urzędzie Gminy Trzcianne

Rozdział 1. Definicje

§ 1. Określenia i skróty użyte w Polityce Bezpieczeństwa Informacji oznaczają:

1. **Urząd** – Urząd Gminy Trzcianne,

2. **Administrator Danych Osobowych** – Wójt Gminy Trzcianne, zwany dalej **Administratorem.**

3. **Administrator Bezpieczeństwa Informacji** - osoba wyznaczona przez Wójta Gminy Trzcianne, odpowiedzialna za bezpieczeństwo danych osobowych przetwarzanych w systemach informatycznych oraz za sprawność i konserwację oraz wdrażanie technicznych zabezpieczeń systemów informatycznych w przetwarzanych zbiorach danych osobowych.

4. **Administrator Systemów Informatycznych** – osoba wyznaczona przez Wójta Gminy Trzcianne.

5. **Zarządzający oprogramowaniem** – osoba wyznaczona przez Wójta Gminy Trzcianne, odpowiedzialna za zarządzanie oprogramowaniem komputerowym w Urzędzie Gminy Trzcianne.

6. **u.o.d.o.** – ustawę z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (Dz. U. z 2002 r. Nr 101, poz. 926 ze zm.),

7. **Rozporządzenie** – Rozporządzenie Ministra Spraw Wewnętrznych i Administracji z dnia 29 kwietnia 2004 r. w sprawie dokumentacji przetwarzania danych osobowych oraz warunków technicznych i organizacyjnych, jakim powinny odpowiadać urządzenia i systemy informatyczne służące do przetwarzania danych osobowych (Dz. U. Nr 100, poz. 1024),

8. **Bezpieczeństwo systemu informatycznego** – wdrożenie przez Administratora lub osobę przez niego uprawnioną środków organizacyjnych i technicznych w celu zabezpieczenia oraz ochrony danych przed ich udostępnieniem osobom nieupoważnionym, zabraniem przez osobę nieuprawnioną, przetwarzaniem z naruszeniem ustawy oraz nieuprawnioną zmianą, utratą, uszkodzeniem lub zniszczeniem.

9. **Przetwarzanie danych osobowych** – wykonywanie jakichkolwiek operacji na danych osobowych, takich jak zbieranie, utrwalanie, przechowywanie, opracowywanie, zmienianie, udostępnianie i ich usuwanie.

10. **Osoba upoważniona lub użytkownik systemu** – osoba posiadająca upoważnienie wydane przez Administratora lub uprawnioną przez niego osobę i dopuszczona jako użytkownik do przetwarzania danych osobowych w systemie informatycznym danej komórki organizacyjnej w zakresie wskazanym w upoważnieniu, zwana dalej **użytkownikiem.**

11. **Przełożony użytkownika** – Kierownik Referatu lub Sekretarz Gminy, zwany dalej **przełożonym.**

12. **Osoba uprawniona** – osoba posiadająca upoważnienie wydane przez Administratora do wykonywania w jego imieniu określonych czynności.

13. **Użytkownik uprzywilejowany** – osoba posiadająca najwyższy stopień uprawnień do zarządzania systemem informatycznym.

Rozdział 2. Postanowienia ogólne

§ 2. 1. Niniejsza „Polityka Bezpieczeństwa Informacji" zwana dalej Polityką Bezpieczeństwa ma zastosowanie do ochrony zbiorów danych osobowych przetwarzanych w Urzędzie Gminy Trzcianne, w celu ich bezpiecznego wykorzystania oraz określa zasady korzystania z systemów informatycznych.

2. Polityka Bezpieczeństwa została opracowana na podstawie art. 36 ustawy z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (Dz. U. z 2002 r. Nr 101, poz. 926 z późn. zm.) w celu realizacji § 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).

3. Na Politykę Bezpieczeństwa składają się poszczególne instrukcje i procedury zawierające informacje dotyczące rozpoznania procesów ich przetwarzania oraz wprowadzonych zabezpieczeń technicznych i organizacyjnych zapewniających ochronę przetwarzanych danych osobowych. W skład Polityki Bezpieczeństwa wchodzą:

1) Realizacja podstawowych założeń rozporządzenia,

2) Zarządzanie przetwarzaniem danych osobowych oraz ich bezpieczeństwem,

3) Zasady Udostępniania Danych Osobowych,

4) Ochrona obszaru przetwarzania i monitorowanie ochrony zasobów danych osobowych,

5) Instrukcja zarządzania systemem informatycznym służącym do przetwarzania danych osobowych w Urzędzie Gminy w Trzciannem.

Rozdział 3.
Realizacja podstawowych założeń Rozporządzenia

§ 3. 1. Obszar przetwarzania danych osobowych w Urzędzie Gminy Trzcianne obejmuje budynek, pomieszczenia i części pomieszczeń, w których przetwarzane są dane osobowe, tzn. Miejsca, w których wykonuje się operacje na danych osobowych (wpisuje, modyfikuje, kopiuje), jak również miejsca gdzie przechowuje się wszelkie nośniki informacji zawierające dane osobowe (szafy z dokumentacją papierową, szafy zawierające komputerowe nośniki informacji). Obszar przetwarzania danych osobowych określony został w „Wykazie pomieszczeń, w których przetwarzane są dane osobowe", stanowiącym Załącznik Nr 1a do Polityki Bezpieczeństwa Informacji.

2. Zawiera następujące informacje:

1) lokalizację,

2) numer pomieszczenia/przeznaczenie,

3) piętro,

4) wydział użytkujący pomieszczenie,

5) osoby pracujące w pomieszczeniu (stanowiska + liczba osób),

6) zabezpieczenia.

3. Wymogi dotyczące ochrony obszaru przetwarzania danych określone zostały w Załączniku Nr 1c do Polityki Bezpieczeństwa Informacji (Zasady ochrony pomieszczeń, w których przetwarzane są dane osobowe).

§ 4. Wykaz zbiorów danych przetwarzanych w Urzędzie Gminy Trzcianne i programów zastosowanych do przetwarzania danych.

1. Wykaz zbiorów znajduje się w odrębnym dokumencie „Wykaz zasobów danych osobowych i systemów ich przetwarzania", stanowiącym Załącznik Nr 1b do Polityki Bezpieczeństwa Informacji i zawiera następujące informacje:

1) nazwa zbioru danych,

2) system przetwarzania (nazwa),

3) lokalizacja miejsca przetwarzania,

4) zastosowane oprogramowanie,

5) pełny zakres danych osobowych w systemie (pola i relacje pomiędzy nimi),

6) pola informacyjne w systemie,

7) sposób przepływu danych pomiędzy systemami,

8) możliwość wydruku zakresu przetwarzania danych osobowych.

2. Szczegółowe informacje dotyczące platformy sprzętowej oraz oprogramowania danego systemu informatycznego znajdują się w poszczególnych instrukcjach zarządzania danym systemem.

§ 5. Opis struktury zbiorów danych wskazujący zawartość poszczególnych pól i nformacyjnych i powiązania między nimi.

1. Przetwarzanie odbywa się częściowo na serwerze, częściowo na stacjach roboczych użytkowników (dostęp możliwy wyłącznie ze specjalizowanego oprogramowania klienckiego).

2. Program Płatnik pracuje na zbiorze znajdującym się fizycznie na komputerze w dziale finansowym. Dostęp do tego zbioru danych możliwy jest tylko z tego stanowiska.

3. SWDO (System Wydawania Dowodów Osobistych) znajduje się na komputerach dostarczonych przez Ministerstwo i dostęp do tego zbioru danych jest możliwy tylko z tych stanowisk dla osób upoważnionych przez Ministerstwo do pracy na tych komputerach.

§ 6. Sposób przepływu danych pomiędzy poszczególnymi systemami.

1. W ramach procesów przetwarzania danych dochodzi do przepływu danych pomiędzy różnymi systemami informatycznymi. Informacje na temat przepływu danych pomiędzy różnymi systemami informatycznymi znajdują się w „Wykazie zasobów danych osobowych i systemów ich przetwarzania" stanowiącym Załącznik nr 1b do Polityki Bezpieczeństwa Informacji.

2. Szczegółowe informacje dotyczące przepływu danych osobowych pomiędzy danymi systemami informatycznymi znajdują się w poszczególnych instrukcjach zarządzania danym systemem.

Rozdział 4.
Zarządzanie przetwarzaniem danych osobowych oraz ich bezpieczeństwem

§ 7. Zakres praw i obowiązków administratora danych osobowych oraz ich bezpieczeństwem

1. Administratorem danych osobowych w Urzędzie Gminy Trzcianne w rozumieniu art. 7 pkt 4 u.o.d.o. jest Wójt Gminy Trzcianne.

2. Administrator, powołuje Administratora Bezpieczeństwa Informacji (ABI), który w jego imieniu wykonuje zadania w zakresie:

1) nadzoru nad przestrzeganiem zasad ochrony danych osobowych w Urzędzie Gminy Trzcianne,

2) przeprowadzania czynności kontrolnych w Urzędzie w celu oceny zgodności przetwarzania danych osobowych z u.o.d.o.,

3) przekazywania do Administratora sprawozdań z kontroli zgodności przetwarzania danych osobowych w Urzędzie z u.o.d.o.,

4) prowadzenia dokumentacji opisującej sposób przetwarzania danych osobowych oraz środki techniczne i organizacyjne zabezpieczenia danych osobowych – niniejsza polityka oraz wynikające z niej instrukcje,

5) nadzoru nad prowadzeniem ewidencji osób upoważnionych do przetwarzania danych osobowych,

6) współuczestniczenia w czynnościach związanych ze zgłoszeniem zbiorów danych osobowych do rejestracji GIODO - przygotowywania nowych wniosków rejestracyjnych lub aktualizacji wniosków zgłoszonych wcześniej,

7) wdrażania znajomości przepisów dot. ochrony danych osobowych,

8) kontrolowania procesów udostępniania danych osobowych,

9) przygotowywania projektów umów powierzania przetwarzania danych osobowych innemu podmiotowi,

10) wydawania zaleceń dla kierowników komórek organizacyjnych w zakresie podwyższenia standardów zabezpieczeń danych osobowych,

11) monitorowania ochrony zasobów danych osobowych w Urzędzie,

12) współpracy z Administratorem Systemu Informatycznego w zakresie nadzoru i kontroli nad bezpieczeństwem systemu informatycznego , w którym przetwarzane są dane osobowe,

13) prowadzenia wykazu obszarów przetwarzania danych osobowych – spis budynków, pomieszczeń lub części pomieszczeń, tworzących obszar, w którym przetwarzane są dane osobowe,

14) przeprowadzania kontroli stanu zabezpieczeń fizycznych i technicznych obszaru przetwarzania danych,

15) podejmowania działań zgodnych z obowiązującymi w Urzędzie procedurami w sytuacji naruszenia ochrony danych osobowych.

3. Administrator powołuje zastępcę ABI, który wykonuje zadania ABI podczas jego nieobecności.

4. Wójt wyznacza Właścicieli (Opiekunów) poszczególnych zasobów danych osobowych (zwanych dalej Właścicielami ZDO).

5. Rolę Właścicieli zasobów danych osobowych pełnią Kierownicy Referatów odpowiedzialni za dany zasób danych osobowych (wynikający z zakresu pełnionych obowiązków).

6. Do obowiązków Właścicieli ZDO należy:

1) zarządzanie zasobem danych osobowych w ramach zadań realizowanych przez nadzorowane referaty,

2) występuje z wnioskiem do Administratora o nadawanie upoważnień dotyczących dostępu do zasobu danych osobowych podległym pracownikom,

3) zgłaszanie do ABI zamiaru utworzenia zbioru danych osobowych oraz informacji dotyczących zmian w zakresie i sposobach przetwarzania tego zbioru,

4) realizacja procesu udostępniania danych osobowych innemu podmiotowi lub osobie, której dane dotyczą,

5) prowadzenie w podległym referacie nadzoru nad obiegiem oraz przechowywaniem dokumentów zawierających dane osobowe generowane przez system informatyczny,

6) dopilnowanie aby monitory stanowisk dostępu do danych osobowych w podległym referacie były tak ustawione, aby uniemożliwić postronnym osobom wgląd w dane oraz dopilnowanie stosowania wygaszaczy ekranów na tych stanowiskach,

7) zapoznawanie pracowników mających dostęp do danych osobowych z przepisami dotyczącymi ochrony danych osobowych.

7. Za bezpieczeństwo danych osobowych przetwarzanych w systemach informatycznych Urzędu, odpowiada Administrator Systemu Informatycznego (ASI).

8. Do obowiązków ASI w zakresie ochrony danych osobowych należy:

1) zapewnienie bezawaryjnego zasilania komputerów oraz innych urządzeń mających wpływ na bezpieczeństwo przetwarzania danych osobowych w Urzędzie,

2) prowadzenia nadzoru nad naprawami, konserwacją i likwidacją urządzeń komputerowych, na których zapisane są dane osobowe,

3) prowadzenie w Urzędzie nadzoru nad przeglądami, konserwacją, uaktualnianiem systemów służących do przetwarzania danych osobowych oraz podejmowanie natychmiastowych działań zabezpieczających stan systemu informatycznego w Urzędzie w przypadku otrzymania informacji o naruszeniu zabezpieczeń informatycznych. Powiadomienie o zaistnieniu tego faktu Administratora,

4) prowadzenie nadzoru nad przesyłaniem danych osobowych drogą teletransmisji,

5) nadzór nad przestrzeganiem zasad bezpieczeństwa w przypadku udostępniania danych osobowych innym podmiotom drogą teletransmisji danych.

6) przeciwdziałanie dostępowi osób niepowołanych do systemu informatycznego, w którym przetwarzane są dane osobowe,

7) podejmowanie odpowiednich działań w przypadku naruszeń w systemie zabezpieczeń,

8) właściwy nadzór nad funkcjonowaniem mechanizmów uwierzytelniania użytkowników oraz kontroli dostępu do danych osobowych,

9) nadzór nad wykonywaniem kopii awaryjnych, ich przechowywaniem oraz okresowym sprawdzaniem pod kątem ich dalszej przydatności do odtworzenia danych w przypadku awarii systemu,

9. Zapisy dotyczące zadań poszczególnych osób muszą zostać wpisane w ich zakresy obowiązków i być przechowywane w ich aktach osobowych.

Rozdział 5.
Odpowiedzialność karna

§ 8. Sankcje

1. Naruszenie przepisów o ochronie danych osobowych jest zagrożone sankcjami karnymi określonymi w art. 49 – 54a u.o.d.o. oraz w art. 130, 266 – 269, 287 Kodeksu Karnego.

2. Niezależnie od odpowiedzialności przewidzianej w przepisach, o których mowa w ust. 1, naruszenie zasad ochrony danych osobowych obowiązujących w Urzędzie Gminy Trzcianne może zostać uznane za ciężkie naruszenie podstawowych obowiązków pracowniczych i skutkować odpowiedzialnością dyscyplinarną.

Rozdział 6.
Postanowienia końcowe

§ 9. 1. Niniejsza Instrukcja przeznaczona jest dla użytkowników i ich przełożonych, którzy nadzorują przetwarzanie danych osobowych.

2. Wykonanie postanowień Instrukcji ma na celu wprowadzenie jednolitego systemu zarządzania systemem informatycznym w Urzędzie Gminy Trzcianne.

§ 10. W sprawach nieuregulowanych Instrukcją znajdują zastosowanie przepisy ustawy z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (Dz.U. z 2002 r. Nr 101, poz. 926 z późn. zm.) i rozporządzenia Ministra Spraw Wewnętrznych i Administracji z dnia 29 kwietnia 2004 r. w sprawie dokumentacji przetwarzania danych osobowych oraz warunków technicznych i organizacyjnych, jakimi powinny odpowiadać urządzenia i systemy informatyczne służące do przetwarzania danych osobowych (Dz.U. Nr 100, poz. 1024).

§ 11. Wszelkie zmiany w Polityce Bezpieczeństwa mogą być wprowadzone tylko na podstawie zarządzeń Administratora.

Załącznik Nr 1a do Zarządzenia Nr 102/12

Wójta Gminy Trzcianne

z dnia 8 listopada 2012 r.

Wykaz pomieszczeń, w których przetwarzane są dane osobowe

Lp.	Lokalizacja adres i numer budynku	Numer pomieszczenia (przeznaczenie)	Piętro	Dział/pion użytkujący pomieszczenie	Osoby pracujące w pomieszczeniu /stanowiska + liczba osób/	Zabezpieczenie pomieszczenia
1	2	3	4	5	6	7

Załącznik Nr 1b do Zarządzenia Nr 102/12

Wójta Gminy Trzcianne

z dnia 8 listopada 2012 r.

Wykaz zasobów danych osobowych i systemów ich przetwarzania.

Lp.	Nazwa zbioru/ zasobu danych osobowych	System przetwarzania /nazwa systemu/	Lokalizacja miejsca przetwarzania	Zastosowane oprogramowanie	Pełny zakres danych osobowych w systemie	Pola informacyjne w systemie	Sposób przepływu danych pomiędzy systemami	Możliwość wydruku zakresu przetwarzanych danych osobowych
1	2	3	4	5	6	7	8	9

Załącznik Nr 1c do Zarządzenia Nr 102/12

Wójta Gminy Trzcianne

z dnia 8 listopada 2012 r.

Ochrona obszaru przetwarzania i monitorowania ochrony zasobów danych osobowych

§ 1. Zasady ochrony pomieszczeń, w których przetwarzane są dane osobowe

1. Wójt Gminy wspólnie z kierownikami referatów odpowiadają za należyte zabezpieczenie fizyczne zasobów danych osobowych w podległych komórkach.

2. ABI przeprowadza bezpośrednią kontrolę stanu zabezpieczeń fizycznych zbiorów danych osobowych oraz zgłasza do Wójta Gminy swoje uwagi lub rekomenduje zlecenie kontroli specjalistycznej firmie.

3. Obszarem w którym przetwarzane są dane osobowe jest siedziba Urzędu Gminy Trzcianne, ul. Wojska Polskiego 10, 19-104 Trzcianne.

4. ABI jest odpowiedzialny za prowadzenie aktualnego wykazu pomieszczeń, w których przetwarzane są dane osobowe.

5. Przebywanie wewnątrz pomieszczeń, o których mowa w ust 4, osób nieuprawnionych do dostępu do danych osobowych jest dopuszczalne tylko w obecności osoby upoważnionej do przetwarzania tych danych lub za zgodą Właściciela ZDO.

6. Osoby upoważnione do przetwarzania danych osobowych zobowiązane są do przestrzegania zasad dotyczących wprowadzania osób trzecich do obszaru, o którym mowa w ust 3. Ruch osób z zewnątrz w wymienionym obszarze powinien odbywać się pod kontrolą osób upoważnionych.

7. Sekretarz Gminy zezwala na przebywanie w pomieszczeniach (o których mowa w ust 4.) osobom sprzątającym te pomieszczenia poza godzinami pracy Urzędu bez konieczności obecności osoby dopuszczonej do przetwarzania danych. Osoby te podpisują oświadczenie o zachowaniu poufności.

8. Budynki lub pomieszczenia, w których przetwarzane są dane osobowe, powinny być zamykane na czas nieobecności w nich osób dopuszczonych do danych osobowych, w sposób uniemożliwiający dostęp do nich osobom nieupoważnionym.

9. Pomieszczenia w których przetwarzane są dane wrażliwe oraz pomieszczenia serwerowni i archiwów powinny podlegać specjalnej ochronie.

10. Właściciel ZDO zabezpiecza zgodnie z wytycznymi ust 8,9,10 obszar przetwarzania danych.

11. Budynek i pomieszczenia Urzędu Gminy Trzcianne posiadają następujące zabezpieczenia :

1) 2 drzwi zewnętrzne zaopatrzone w podwójne zamki patentowe, dostęp (klucze) do drzwi głównych wejściowych posiadają: 3 pracowników.

2) Wszystkie okna Urzędu Gminy znajdują się na I i II piętrze.

3) Okna do pomieszczeń podlegających specjalnej ochronie (serwerownia) znajdują się na I piętrze i zabezpieczone są kratami.

4) Wszystkie drzwi do pomieszczeń biurowych posiadają zamki.

5) dokumenty z danymi osobowymi powinny być przechowywane w szafach na akta wyposażonych w zamki,

6) system sygnalizacji alarmu i włamania, do którego szyfr posiadają: wójt i 3 pracowników.

§ 2. Przetwarzanie danych osobowych poza obszarem przetwarzania

1. W sytuacji przetwarzania danych osobowych na komputerach przenośnych lub dokumentach papierowych poza obszarem wymienionym w § 1 ust. 3, należy bezwzględnie chronić te dane przed dostępem do nich osób nieupoważnionych.

2. Zasady ochrony komputerów przenośnych, na których przetwarzane są dane osobowe, określa ASI w „Instrukcji zarządzania systemami informatycznymi służącymi do przetwarzania danych osobowych w Urzędzie Gminy Trzianne".

§ 3. Monitorowanie ochrony zasobów danych osobowych

1. Właściciele ZDO przekazują (w formie elektronicznej) ABI:

1) aktualny wykaz zasobów danych osobowych przetwarzanych w danej komórce organizacyjnej,

2) wykaz osób upoważnionych do przetwarzania określonego zasobu danych osobowych,

3) wykaz pomieszczeń, w których przetwarzany jest poszczególny zasób danych osobowych w podległej komórce organizacyjnej i ich zabezpieczeń.

2. Pracownik ds. kadr na bieżąco informuje ABI o:

1) ustaniu zatrudnienia w Urzędzie określonej osoby, celem kontroli aktywności jego kont w systemie informatycznym,

2) przeniesieniu pracownika do innego referat Urzędu, celem kontroli jego praw do dostępu do danych osobowych.

3. ASI przekazuje ABI:

1) aktualny wykaz systemów teleinformatycznych – aplikacji, w których przetwarzane są dane osobowe z informacją o programach zastosowanych do przetwarzania tych danych,

2) opis struktury zbiorów danych wskazujący zawartość poszczególnych pól informacyjnych i powiązania między nimi,

3) sposób przepływu danych pomiędzy poszczególnymi systemami.

4. ABI ustala szczegółowe zakresy potrzebnych informacji oraz formę i tryb ich przekazywania.

5. Każda zmiana informacji w zakresie ujętym w ust 1-3 wymaga bieżącej aktualizacji przez osoby wskazane w wymienionych punktach.

6. Na podstawie przekazywanych informacji ABI prowadzi aktualny wykaz zasobów danych osobowych przetwarzanych w Urzędzie, który zamieszcza w dokumencie „Wykaz zasobów danych osobowych i systemów ich przetwarzania".

Załącznik Nr 2 do Zarządzenia Nr 102/12

Wójta Gminy Trzcianne

z dnia 8 listopada 2012 r.

Instrukcja Zarządzania Systemem Informatycznym służącym do przetwarzania danych osobowych w Urzędzie Gminy Trzcianne.

§ 1. Przetwarzanie danych w systemie teleinformatycznym

1. Dane osobowe mogą być przetwarzane w systemach spełniających wymogi u.o.d.o. oraz Rozporządzenia.

2. „Instrukcja Zarządzania Systemami Informatycznymi służącymi do przetwarzania danych osobowych w Urzędzie Gminy Trzcianne" określa zasady zarządzania systemem informatycznym służącym do przetwarzania danych osobowych w zakresie:

1) określenia sposobu przydziału i zarządzania hasłami użytkowników,

2) określenia uprawnień użytkowników oraz sposobu ich rejestrowania i wyrejestrowania w systemie informatycznym,

3) zasad rozpoczęcia i zakończenia pracy w systemie,

4) ochrony antywirusowej,

5) przeglądów i konserwacji systemu,

6) postępowania w zakresie komunikacji w sieci komputerowej,

7) zarządzania systemem informatycznym,

8) przechowywania i niszczenia nośników informacji.

§ 2. Wymagania dla systemu teleinformatycznego

1. System informatyczny służący do przetwarzania danych osobowych wyposażony jest w mechanizmy uwierzytelniania użytkownika oraz kontroli dostępu do tych danych.

2. Identyfikator użytkownika wraz z jego imieniem i nazwiskiem wpisuje się do ewidencji osób upoważnionych do przetwarzania danych osobowych prowadzonej przez Właścicieli ZDO.

3. Identyfikator użytkownika nie powinien być zmieniany, a po wyrejestrowaniu użytkownika z systemu informatycznego nie powinien być przydzielany innej osobie.

4. Identyfikator osoby, która utraciła uprawnienia dostępu do danych osobowych, należy bezzwłocznie wyrejestrować z systemu informatycznego, w którym są one przetwarzane, unieważnić jej hasło oraz podjąć stosowne działania w celu zapobieżenia dalszemu dostępowi tej osoby do danych osobowych.

5. W pomieszczeniach, w których przebywają osoby postronne, monitory stanowisk dostępu do danych osobowych powinny być ustawione w taki sposób, żeby uniemożliwić tym osobom wgląd w te dane.

§ 3. Przetwarzanie danych osobowych w systemie informatycznym poza zbiorem danych

1. Jeżeli zachodzi taka konieczność dopuszcza się przetwarzanie danych osobowych w plikach poza bazą danych, znajdującą się w określonym systemie informatycznym.

2. Zgodę na przetwarzanie danych w formie w takiej sytuacji wydaje właściciel ZDO wg wzoru upoważnienia określonego w Załączniku Nr 2a do Instrukcji zarządzania systemem informatycznym służącym do przetwarzania danych osobowych w Urzędzie Gminy Trzcianne.

3. Dane przetwarzane w plikach mogą stanowić kopie części bazy znajdującej się w systemie lub być nową celową ewidencją tworzoną na potrzeby realizacji zadań związanych z przetwarzaniem danych osobowych przez uprawnionych pracowników.

4. Dostęp do plików z danymi powinien być ograniczony jedynie do osoby tworzącej taki plik na swojej stacji roboczej. W tej sytuacji pliki:

1) nie mogą być udostępnione przez sieć komputerową innym użytkownikom,

2) możliwe są do otwarcia jedynie po zalogowaniu się na profil danego użytkownika,

3) muszą być chronione hasłem, jeżeli mają być dostępne dla innych Użytkowników.

5. W sytuacji umieszczenia plików z danymi osobowymi na serwerze plików, dostęp do niego powinien być ograniczony do określonej grup uprawnionych użytkowników.

6. Grupę użytkowników określa dany Właściciel ZDO.

§ 4. Przetwarzanie danych osobowych znajdujących się na nośnikach papierowych.

1. Dane osobowe zawarte w dokumentacji papierowej przetwarzane są przez osoby upoważnione zgodnie z zasadami niniejszej polityki.

2. Rejestracje, obieg i udostępnianie – w tym na zewnątrz Urzędu – dokumentów papierowych zawierających dane osobowe reguluje „Instrukcja Kancelaryjna".

3. Przechowywanie i likwidację dokumentów papierowych wykorzystywanych w Urzędzie reguluje Rozporządzenie Prezesa Rady Ministrów z dnia 18 stycznia 2011 r. w sprawie instrukcji kancelaryjnej, jednolitych rzeczowych wykazów akt oraz instrukcji w sprawie organizacji i zakresu działania archiwów zakładowych.

§ 5. Nadawanie/cofanie uprawnień do przetwarzania danych osobowych.

1. W celu nadania uprawnień do przetwarzania danych osobowych i rejestracji tych uprawnień w systemie informatycznym ma zastosowanie „Procedura nadawania/cofania uprawnień do przetwarzania danych osobowych". Osobą odpowiedzialną za rejestrację osoby upoważnionej do przetwarzania danych osobowych w ewidencji osób upoważnionych (art. 39 ust. 1 ustawy o ochronie danych osobowych) jest Sekretarz Gminy, natomiast za rejestrację uprawnień użytkownika w systemach informatycznych osobą odpowiedzialną jest Administrator Bezpieczeństwa.Procedura nadawania/cofania uprawnień do przetwarzania danych osobowych.

1) przełożony użytkownika będącego pracownikiem Urzędu Gminy Trzcianne składa wniosek o nadanie/cofnięcie uprawnień dla użytkownika systemu. Wniosek zawiera dokładny opis uprawnień, które powinny zostać nadane/cofnięte oraz okres (od...do...). Wniosek składa się do Sekretarza Gminy. Wzór wniosku stanowi Załącznik Nr 2b do Instrukcji zarządzania systemem informatycznym służącym do przetwarzania danych osobowych w Urzędzie Gminy Trzcianne.

2) w przypadku użytkowników niebędących pracownikami Urzędu Gminy Trzcianne, wniosek przygotowuje Sekretarz Gminy.

3) Sekretarz Gminy przygotowuje upoważnienie do przetwarzania danych osobowych dla użytkownika systemu. Upoważnienie przygotowane jest na piśmie w dwóch egzemplarzach (wzór upoważnienia stanowi Załącznik Nr 2c do Instrukcji zarządzania systemem informatycznym służącym do przetwarzania danych osobowych w Urzędzie Gminy Trzcianne).

4) Administrator podpisuje upoważnienie do przetwarzania danych osobowych i przekazuje Sekretarzowi Gminy.

2. Ustanie stosunku pracy jest równoważne z cofnięciem uprawnień do przetwarzania danych osobowych.

3. Osoby dopuszczone do przetwarzania danych osobowych zobowiązane są do zachowania tajemnicy w zakresie tych danych oraz sposobów ich zabezpieczenia. Obowiązek ten istnieje również po ustaniu zatrudnienia.

4. Sekretarz Gminy i Administrator Bezpieczeństwa Informacji są jednocześnie użytkownikami uprzywilejowanymi.

5. Sekretarz Gminy wydaje pozwolenie na dostęp do systemu informatycznego, w którym przetwarzane są dane osobowe, podmiotom zewnętrznym.

§ 6. Zarządzanie metodami oraz środkami uwierzytelniania

1. W celu zarządzania metodami oraz środkami uwierzytelniania mają zastosowanie „Procedura uwierzytelniania użytkownika w systemie informatycznym" oraz „Procedura rejestrowania/wyrejestrowania użytkownika z systemu informatycznego".

1) Procedura uwierzytelniania użytkownika w systemie informatycznym.

a) niepowtarzalny identyfikator oraz pierwsze hasło jest przydzielone użytkownikowi przez Administratora Bezpieczeństwa po nadaniu uprawnień do przetwarzania danych osobowych.

b) pierwsze hasło jest przekazane użytkownikowi systemu przez Administratora Bezpieczeństwa w formie pisemnej.

c) bezpośredni dostęp do danych użytkownik uzyskuje po podaniu identyfikatora i właściwego hasła.

2) Procedura rejestrowania/wyrejestrowania użytkownika z systemu informatycznego.

a) użytkownicy systemu informatycznego są niezwłocznie rejestrowani lub wyrejestrowywani przez Administratora Bezpieczeństwa, gdy uzyskują lub tracą prawo dostępu do systemu, zgodnie z procedurą nadawania/cofania uprawnień do przetwarzania danych osobowych.

b) identyfikator po wyrejestrowaniu użytkownika zostaje zablokowany przez Administratora Bezpieczeństwa.

c) identyfikator po wyrejestrowaniu użytkownika nie jest przydzielany innej osobie.

§ 7. Rozpoczęcie, zawieszenie i zakończenie pracy w systemie informatycznym

1. W celu rozpoczęcia, zawieszenia i zakończenia pracy w systemie informatycznym mają zastosowanie następujące procedury:

1) Procedura rozpoczęcia pracy w systemie informatycznym.

a) w celu rozpoczęcia pracy w systemie informatycznym użytkownik obowiązany jest do podania hasła dostępu do systemu.

b) podczas pierwszego uwierzytelniania w systemie użytkownik ma obowiązek zmiany hasła.

c) hasło składa się, z co najmniej z 6 znaków. Jego długość jest uzależniona od poziomu bezpieczeństwa. Hasło zawiera wielkie i małe litery oraz cyfry lub znaki specjalne.

d) zabrania się wpisywania hasła lub jego zmiany w obecności innych osób.

e) hasło nie może być zapisywane lub przechowywane w miejscu dostępnym dla osób nieuprawnionych.

f) w przypadku zagubienia hasła użytkownik musi skontaktować się z Administratorem Bezpieczeństwa w celu uzyskania nowego hasła.

g) użytkownikowi wolno używać tylko zainstalowanego oprogramowania, wyłącznie zgodnie z instrukcją obsługi, warunkami licencji i bezpieczeństwa przetwarzania danych.

2) Procedura zawieszenia/odwieszenia pracy w systemie informatycznym.

a) w celu zawieszenia/wstrzymania pracy w systemie informatycznym służącym do przetwarzania danych osobowych użytkownik zobowiązany jest do wylogowania się z systemu operacyjnego.

b) w przypadku komputerów PC po wylogowaniu się z systemu operacyjnego użytkownik blokuje pulpit uniemożliwiając dostęp do danych osobom niepowołanym.

c) w celu ponownego przystąpienia do pracy w systemie użytkownik loguje się na swoje konto w komputerze i rozpoczyna pracę w systemie informatycznym zgodnie z procedurą rozpoczęcia pracy w systemie informatycznym.

d) zabrania się pozostawiania stanowiska komputerowego z uruchomionym systemem bez kontroli pracującego na nim użytkownika,

e) na komputerach, na których przetwarzane są dane osobowe wygaszacz ekranu zabezpieczony hasłem jest ustawiony na 10 min., na pozostałych 15 min.

3) Procedura zakończenia pracy w systemie informatycznym.

a) w celu zakończenia pracy w systemie informatycznym użytkownik wyrejestrowuje się z programu służącego do obsługi danych osobowych.

b) użytkownik „zamyka system operacyjny" i wyłącza komputer.

§ 8. Podejrzenie lub stwierdzenie naruszenia ochrony danych osobowych

1. W przypadku podejrzenia lub stwierdzenia naruszenia ochrony danych osobowych ma zastosowanie procedura postępowania w sytuacjach naruszenia ochrony danych osobowych.

1) Procedura postępowania w sytuacji naruszenia ochrony danych osobowych.

a) Na fakt naruszenia zabezpieczeń systemu informatycznego mogą wskazywać:

- stan stacji roboczej (np. brak zasilania, problemy z uruchomieniem, naruszenie lub uszkodzenie obudowy stacji roboczej)
- wszelkiego rodzaju różnice w funkcjonowaniu systemu (np. komunikaty informujące o błędach, brak dostępu do funkcji systemu, nieprawidłowości w wykonywanych operacjach),
- różnice w zawartości zbioru danych osobowych (np. brak lub nadmiar danych),
- jakości komunikacji w sieci telekomunikacyjnej (gwałtowne opóźnienia lub przyśpieszenia wykonywanych czynności),
- inne sytuacje nadzwyczajne.

b) W przypadku podejrzenia naruszenia zabezpieczenia systemu informatycznego użytkownik niezwłocznie powiadamia bezpośredniego przełożonego oraz Administratora Bezpieczeństwa.

c) Administrator Bezpieczeństwa niezwłocznie wszczyna postępowanie wyjaśniające i o jego wynikach informuje Administratora.

§ 9. Zabezpieczenie danych i programów

1. W celu zabezpieczenia danych i programów służących do przetwarzania danych osobowych ma zastosowanie poniższa procedura:

1) procedura tworzenia kopii zapasowych zbiorów danych oraz programów i narzędzi programowych służących do ich przetwarzania.

a) kopie zapasowe baz danych wykonywane są codziennie w dni robocze, po zakończeniu czasu pracy na macierzy dyskowej.

b) na koniec każdego miesiąca informatyk tworzy kopię miesięczną na płytach kompaktowych (DVD-R), które są przechowywane przez okres 5 lat.

c) kopie bezpieczeństwa bazy danych przechowywane są poza pomieszczeniami, w których zostały utworzone. Kopie miesięczne przechowywane są w szafie zamykanej na klucz Urzędu Gminy Trzcianne

d) po okresie przechowywania kopie miesięczne są komisyjnie niszczone poprzez ich fizyczne zniszczenie. W komisji likwidacyjnej biorą udział ABI oraz pracownik Referatu Organizacyjnego-Prawnego.

2) procedura zabezpieczenia systemu przetwarzania danych osobowych przed złośliwym oprogramowaniem:

a) skanowanie komputerów osobowych programami antywirusowymi działa w czasie rzeczywistym, czyli podczas pracy komputera oprogramowanie antywirusowe skanuje używane programy i pliki w poszukiwaniu potencjalnie niebezpiecznego złośliwego oprogramowania.

b) procedura zaleca, w miarę możliwości, aktualizowanie systemów operacyjnych.

§ 10. Zabezpieczenie systemu informatycznego

1. Sieć zewnętrzna posiada dostęp do Internetu. Głównym urządzeniem zabezpieczającym sieć zewnętrzną Urzędu Gminy Trzcianne jest router. Urządzenie to umożliwia blokowanie wielu obszarów dostępu do Internetu, w tym portów i protokołów sieciowych.

2. Serwery znajdujące się w sieci posiadają własne programowe zapory systemowe. To samo tyczy się komputerów działających w tych sieciach.

§ 11. Zasady archiwizowania danych osobowych przetwarzanych papierowo

1. Archiwizowanie papierowych zbiorów danych osobowych odbywa się w oparciu o Rozporządzenie Prezesa Rady Ministrów z dnia 18 stycznia 2011 r. w sprawie instrukcji kancelaryjnej, jednolitych rzeczowych wykazów akt oraz instrukcji w sprawie organizacji i zakresu działania archiwów zakładowych.

2. Kopie papierowe z danymi osobowymi muszą być oznaczone i przechowywane w zamykanych na klucz szafach.

§ 12. Zasady napraw i likwidacji sprzętu komputerowego służącego do przetwarzania danych osobowych

1. Urządzenia przekazywane do naprawy należy pozbawić możliwości zapisu danych oraz możliwości ich odczytania przez nieupoważnione osoby, które dokonują naprawy.

2. Jeśli naprawa sprzętu lub oprogramowania musi zostać wykonana w miejscu przetwarzania danych osobowych albo na komputerze gdzie są przetwarzane dane osobowe, to naprawy mogą być dokonywane w obecności osoby upoważnionej przez Administratora danych.

3. Dyski i inne nośniki danych zawierające dane do likwidacji, należy pozbawić możliwości zapisu i odczytu tych danych, a w przypadku, gdy nie jest to możliwe należy uszkodzić nośnik w sposób uniemożliwiający odzyskanie danych z nośnika.

Załącznik Nr 2a do Zarządzenia Nr 102/12

Wójta Gminy Trzcianne

z dnia 8 listopada 2012 r.

UPOWAŻNIENIE DO PRZETWARZANIA DANYCH OSOBOWYCH POZA BAZĄ DANYCH SYSTEMU INFORMATYCZNEGO URZĘDU GMINY TRZCIANNE

Data nadania upoważnienia: .....

1. Upoważniam Panią/Pana .....

zatrudnioną/-ego na stanowisku .....

w Urzędzie Gminy Trzcianne do przetwarzania poza bazą danych systemu informatycznego następujących danych osobowych:

– .....

– .....

– .....

(zakres upoważnienia: wskazanie kategorii danych, które może przetwarzać określona w upoważnieniu osoba, lub rodzaj czynności lub operacji, jakich może dokonywać na danych osobowych)

2. Identyfikator: .....

3. Okres trwania upoważnienia: .....

(okres obowiązywania upoważnienia)

.....

(podpis Właściciela Zbioru Danych Osobowych)

4. Osoba upoważniona do przetwarzania danych, objętych zakresem, o którym mowa wyżej, jest zobowiązana do zachowania ich w tajemnicy, nie kopiowania ich i nie udostępniania, również po ustaniu zatrudnienia oraz zachowania w tajemnicy informacji o ich zabezpieczeniu.

Data i podpis osoby upoważnionej: .....

Załącznik Nr 2b do Zarządzenia Nr 102/12

Wójta Gminy Trzcianne

z dnia 8 listopada 2012 r.

Trzcianne, dnia .....

...../.....

W N I O S E K

o nadanie/cofnięcie uprawnień do przetwarzania danych osobowych

Na podstawie art. 37 ustawy z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (Dz.U. z 2002 Nr 101, poz. 926 z późn. zm.) proszę o nadanie/cofnięcie uprawnień dla

Pani/Pana.....

Pracownika.....

.....

.....

.....

do wykonywania czynności związanych z przetwarzaniem danych osobowych w zakresie:.

.....

.....

na okres od ..... do .....

.....

Podpis

Administratora Danych Osobowych

Załącznik Nr 2c do Zarządzenia Nr 102/12

Wójta Gminy Trzcianne

z dnia 8 listopada 2012 r.

U P O W A Ż N I E N I E

Na podstawie art. 31 ustawy z dnia 8 marca 1990 r. o samorządzie gminnym (Dz.U. z 2001 r. Nr 142, poz. 1591 z późn. zm.) w związku z art. 268a ustawy z dnia 14 czerwca 1960 r. Kodeks postępowania administracyjnego (Dz.U. z 2000 r. Nr 98, poz. 1071 z późn. zm.) oraz art. 37 ustawy z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (Dz.U. z 2002 Nr 101, poz. 926 z późn. zm.)

Upoważniam Panią/Pana .....

pracownika Referatu .....Urzędu Gminy Trzcianne do wykonywania czynności związanych z przetwarzaniem danych osobowych w zakresie:.

.....

.....

.....

ze szczególnym uwzględnieniem zadań zawartych w rozporządzeniu Ministra Spraw Wewnętrznych i Administracji z dnia 29 kwietnia 2004r. w sprawie dokumentacji przetwarzania danych osobowych oraz warunków technicznych i organizacyjnych, jakim powinny odpowiadać urządzenia i systemy informatyczne służące do przetwarzania danych osobowych (Dz.U. z 2004 r. Nr 100, poz. 1024).

Upoważnienie niniejsze nie upoważnia do udzielania dalszych upoważnień i wygasa z dniem ustania stosunku pracy, a ponadto może być w każdym czasie zmienione lub odwołane.

Z dniem podpisania niniejszego upoważnienia traci moc upoważnienie udzielone Pani/Panu ..... z dnia .....

.....

Podpis

Administratora Danych Osobowych

Załącznik Nr 3 do Zarządzenia Nr 102/12

Wójta Gminy Trzcianne

z dnia 8 listopada 2012 r.

Instrukcja Zasad Udostępniania Danych Osobowych

§ 1. Dane osobowe mogą być udostępniane w następujących przypadkach:

1. Na podstawie wniosku od podmiotu uprawnionego do otrzymywania danych osobowych na podstawie przepisów.

2. Na podstawie umowy z innym podmiotem, w ramach której istnieje konieczność udostępnienia danych.

3. Wniosku osoby, której dane dotyczą.

§ 2. Dane osobowe, udostępnia się na pisemny, umotywowany wniosek, chyba, że inny przepis stanowi inaczej.

§ 3. Udostępniając dane osobowe należy zaznaczyć, że można je wykorzystać wyłącznie zgodnie z przeznaczeniem, dla którego zostały udostępnione.

§ 4. W przypadku żądania udzielenia informacji na temat przetwarzanych danych osobowych na pisemny wniosek pochodzący od osoby, której dane dotyczą, odpowiedź na nie następuje w terminie 30 dni od daty jego otrzymania.

§ 5. Właściciel ZDO jest odpowiedzialny za przygotowanie danych osobowych do udostępnienia w zakresie wskazanym we wniosku.

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

1. Listem poleconym za potwierdzeniem odbioru.

2. Poprzez teletransmisję danych, zgodnie z procedurami ochrony danych podczas transmisji – określonymi w instrukcji zarządzania danym systemem teleinformatycznym służącym do przetwarzania danych osobowych.

3. Inny, określony konkretnym wymogiem prawnym lub umową.