

ZARZĄDZENIE WEWNĘTRZNE NR 21/16
WÓJTA GMINY KUŹNICA
z dnia 20 grudnia 2016 roku

w sprawie wprowadzenia Polityki Bezpieczeństwa i Instrukcji Zarządzania Systemem Informatycznym

Na podstawie ustawy z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (t.j. Dz. U. z 2016 r. poz. 922) oraz Rozporządzenia Ministra Spraw Wewnętrznych i Administracji z dnia 29 kwietnia 2004 r. w sprawie dokumentacji przetwarzania danych osobowych oraz warunków technicznych i organizacyjnych, jakim powinny odpowiadać urządzenia i systemy informatyczne służące do przetwarzania danych osobowych (Dz. U. z 2004 r. Nr 100, poz. 1024) zarządza się, co następuje:

§ 1

Wprowadza się w Urzędzie Gminy Kuźnica, Plac Tysiąclecia Państwa Polskiego 1, 16-123 Kuźnica Politykę Bezpieczeństwa oraz Instrukcję Zarządzania Systemem Informatycznym stanowiącą załączniki do niniejszego zarządzenia.

§ 2

Zarządzenie jest adresowane do pracowników Urzędu Gminy Kuźnica, wykonujących czynności określone w załącznikach. Każdy pracownik, zgodnie z wykazem, jest obowiązany zapoznać się z treścią do niniejszego zarządzenia. Oświadczenie o zapoznaniu się z treścią powyższych załączników zaopatrzone w podpis pracownika i datę, dołącza się do akt osobowych. Administratora Bezpieczeństwa Informacji zobowiązuje się do nadzoru nad przestrzeganiem postanowień niniejszego Zarządzenia.

§ 3

Traci moc Zarządzenie Wewnętrzne nr 24/15 Wójta Gminy Kuźnica z dnia 15 czerwca 2015 roku w sprawie wprowadzenia Polityki Bezpieczeństwa i Instrukcji Zarządzania Systemem Informatycznym

§ 4

Zarządzenie wchodzi w życie z dniem podpisania.


WÓJTA
mgr inż. Paweł Mikłasz

POLITYKA BEZPIECZEŃSTWA

Administrator Danych – Wójt Gminy Kuźnica

Zgodnie z **ROZPORZĄDZENIEM 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)

wdraża dokument o nazwie „Polityka Bezpieczeństwa”. Zapisy tego dokumentu wchodzi w życie

z dniem **20 grudnia 2016 roku**

§ 1.

Polityka Bezpieczeństwa w zakresie ochrony danych osobowych w Urzędzie Gminie Kuźnica, określa zasady przetwarzania danych osobowych oraz środki techniczne i organizacyjne zastosowane dla zapewnienia poufności, integralności i rozliczalności przetwarzanych danych osobowych. Polityka bezpieczeństwa służy zapewnieniu wysokiego poziomu bezpieczeństwa przetwarzanych danych. Polityka bezpieczeństwa dotyczy danych osobowych przetwarzanych w zbiorach manualnych oraz w systemach informatycznych.

§ 2

Ilekroć w „Polityce Bezpieczeństwa” jest mowa o:

1. zbiorze danych - rozumie się przez to każdy posiadający strukturę zestaw danych o charakterze osobowym, dostępnych według określonych kryteriów, niezależnie od tego, czy zestaw ten jest rozproszony lub podzielony funkcjonalnie,
2. przetwarzaniu danych - rozumie się przez to jakiegokolwiek operacje wykonywane na danych osobowych, takie jak zbieranie, utrwalanie, przechowywanie, opracowywanie, zmienianie, udostępnianie i usuwanie, a zwłaszcza te, które wykonuje się w systemach informatycznych,
3. systemie informatycznym - rozumie się przez to zespół współpracujących ze sobą urządzeń, programów, procedur przetwarzania informacji i narzędzi programowych zastosowanych w celu przetwarzania danych,
4. zabezpieczeniu danych w systemie informatycznym - rozumie się przez to wdrożenie i eksploatację stosownych środków technicznych i organizacyjnych zapewniających ochronę danych przed ich nieuprawnionym przetwarzaniem,
5. usuwaniu danych - rozumie się przez to zniszczenie danych osobowych lub taką ich modyfikację, która nie pozwoli na ustalenie tożsamości osoby, której dane dotyczą,
6. administratorze danych - rozumie się przez to organ, jednostkę organizacyjną, podmiot lub osobę, o których mowa w art. 3, decydujące o celach i środkach przetwarzania danych osobowych,
7. administratorze bezpieczeństwa informacji – rozumie się przez to osobę wyznaczoną przez Administratora Danych w celu nadzorowania i przestrzegania zasad ochrony, o których mowa w ust. 1, chyba, że Administrator Danych sam wykonuje te czynności.
8. podmiocie – rozumie się przez to spółkę prawa handlowego, podmiot gospodarczy nie posiadający osobowości prawnej, jednostkę budżetową;

§ 3.

Administrator Danych Urzędu Gminy Kuźnica wyznacza **Administradora Bezpieczeństwa Informacji** w celu nadzorowania i przestrzegania zasad ochrony, o których mowa w USTAWIE z dnia 29 sierpnia 1997 r. o ochronie danych osobowych chyba, że Administrator Danych sam wykonuje te czynności. Upoważnienie dla **Administradora Bezpieczeństwa Informacji** oraz zakres obowiązków określa **załącznik do „Polityki Bezpieczeństwa” nr 1**

§ 4.

Wykaz budynków, pomieszczeń lub części pomieszczeń, tworzących obszar, w którym przetwarzane są dane osobowe określa **załącznik do „Polityki Bezpieczeństwa” nr 2**

§ 5.

Wykaz zbiorów danych osobowych wraz ze wskazaniem programów zastosowanych do przetwarzania tych danych określa **załącznik do „Polityki Bezpieczeństwa” nr 3**

§ 6.

Opis struktury zbiorów danych wskazujący zawartość poszczególnych pól informacyjnych i powiązania między nimi oraz sposób przepływu danych pomiędzy poszczególnymi systemami określa **załącznik do „Polityki Bezpieczeństwa” nr 4**

§ 7.

Administradora Bezpieczeństwa Informacji dba o to aby dane osobowe w formie papierowej były niedostępne dla osób nieupoważnionych. Dokumenty powinny znajdować się w pomieszczeniu zamykanym na klucz do którego dostęp mają tylko osoby posiadające aktualne upoważnienie do przetwarzania danych osobowych.

§ 8.

Do przetwarzania danych mogą być dopuszczone wyłącznie osoby posiadające upoważnienie nadane przez **Administradora Danych** lub **Administradora Bezpieczeństwa Informacji**. **Administradora Bezpieczeństwa Informacji** jest obowiązany zastosować środki techniczne i organizacyjne zapewniające ochronę przetwarzanych danych osobowych odpowiednią do zagrożeń oraz kategorii danych objętych ochroną, a w szczególności powinien zabezpieczyć dane przed ich udostępnieniem osobom nieupoważnionym, zabranieniem przez osobę nieuprawnioną, przetwarzaniem z naruszeniem ustawy oraz zmianą, utratą, uszkodzeniem lub zniszczeniem. Administrator Bezpieczeństwa Informacji nadaje uprawnienia pracownikom którzy przetwarzają dane poprzez podpisanie oświadczenia które stanowi **załącznik nr 5 do „Polityki Bezpieczeństwa”**. Administrator Bezpieczeństwa Informacji prowadzi wszelką dokumentację opisującą sposób przetwarzania danych w podmiocie a w szczególności:

1. Ewidencja osób przetwarzających dane w podmiocie posiadających upoważnienie – **załącznik nr 6 do „Polityki Bezpieczeństwa”**
2. Zestawienie danych osobowych. Kiedy i przez kogo zostały do zbioru wprowadzone oraz komu są przekazywane. – **załącznik nr 7 do „Polityki Bezpieczeństwa”**
3. Określenie środków technicznych i organizacyjnych niezbędnych dla zapewnienia poufności, integralności i rozliczalności przetwarzanych danych - **załącznik nr 8 do „Polityki Bezpieczeństwa”**

§ 9.

Na wniosek osoby, której dane dotyczą, Administrator Bezpieczeństwa Informacji jest obowiązany, w terminie 30 dni, poinformować o przysługujących jej prawach oraz udzielić, odnośnie do jej danych osobowych, informacji.

§ 10.

Administrator Bezpieczeństwa Informacji może powierzyć innemu podmiotowi, w drodze umowy zawartej na piśmie, przetwarzanie danych osobowych w podmiocie. Podmiot ten może przetwarzać dane wyłącznie w zakresie i celu przewidzianym w umowie.

§ 11.

Sposób zabezpieczenia oraz przetwarzania danych w systemie informatycznym reguluje Instrukcja Zarządzania Systemem Informatycznym.

§ 12.

W sprawach nieuregulowanych w niniejszej „Polityce Bezpieczeństwa” mają zastosowanie odpowiednie przepisy ustawy o ochronie danych osobowych z dnia 29 sierpnia 1997 r. oraz **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**

§ 13.

Deklaracja intencji, cele i zakres polityki bezpieczeństwa

1. Administrator Danych wyraża pełne zaangażowanie dla zapewnienia bezpieczeństwa przetwarzanych danych osobowych oraz wsparcie dla przedsięwzięć technicznych i organizacyjnych związanych z ochroną danych osobowych.
2. Polityka określa podstawowe zasady bezpieczeństwa i zarządzania bezpieczeństwem systemów, w których dochodzi do przetwarzania danych osobowych.
3. Polityka dotyczy wszystkich danych osobowych przetwarzanych w podmiocie, niezależnie od formy ich przetwarzania (zbiory ewidencyjne, systemy informatyczne) oraz od tego czy dane są lub mogą być przetwarzane w zbiorach danych.
4. Polityka ma zastosowanie wobec wszystkich komórek organizacyjnych w tym oddziałów, samodzielnych stanowisk pracy i wszystkich procesów przebiegających w ramach przetwarzania danych osobowych.
5. Celem Polityki jest przetwarzanie zgodnie z przepisami danych osobowych przetwarzanych w podmiocie oraz ich ochrona przed udostępnieniem osobom nieupoważnionym, zabranieniem przez osobę nieuprawnioną, przetwarzaniem z naruszeniem przepisów określających zasady postępowania przy przetwarzaniu danych osobowych oraz przed uszkodzeniem, zniszczeniem lub nieupoważnioną zmianą.
6. Ze względu na nieustannie zmieniające się zagrożenia przetwarzania danych o osobowych i zmiany prawa niniejsza polityka może być dokumentem dynamicznie zmieniającym się w czasie. Uaktualnienia procedur ochrony, oprogramowania i innych parametrów stosowanych przy przetwarzaniu danych osobowych znajdują na bieżąco odzwierciedlenie funkcjonalne w niniejszej Polityce.
7. Cele Polityki realizowane są poprzez zapewnienie danym osobowym następujących cech:
 - a) poufności - właściwości zapewniającej, że dane nie są udostępniane nieupoważnionym podmiotom;
 - b) integralności - właściwości zapewniającej, że dane osobowe nie zostały zmienione lub

zniszczone w sposób nieautoryzowany;

c) rozliczalności - właściwości zapewniającej, że działania podmiotu operującego na danych osobowych mogą być przypisane w sposób jednoznaczny tylko temu podmiotowi;

d) ciągłości - zdolności do niezakłóconego ich przetwarzania, bez przerw uniemożliwiających ich udostępnianie osobom upoważnionym.

8. Dla skutecznej realizacji Polityki Administrator Danych zapewnia:

a) odpowiednie do zagrożeń i kategorii danych objętych ochroną, środki techniczne i rozwiązania organizacyjne;

b) szkolenia w zakresie przetwarzania danych osobowych i sposobów ich ochrony;

c) kontrolę i nadzór nad przetwarzaniem danych osobowych;

d) monitorowanie zastosowanych środków ochrony;

e) ciągłe śledzenie zmieniających się zagrożeń wewnętrznych i zewnętrznych, także uwzględnianie zmieniającego się prawa;

f) kontrolę i nadzór nad przetwarzaniem danych osobowych przez podmioty trzecie, którym dane zostały udostępnione lub powierzone.

9. Monitorowanie przez Administratora Danych zastosowanych środków ochrony obejmuje m.in. działania użytkowników, naruszanie zasad dostępu do danych, zapewnienie integralności plików oraz ochronę przed atakami zewnętrznymi oraz wewnętrznymi.

10. Administrator Danych lub osoba przez niego upoważniona wdraża wszystkie dokumenty składające się na Polityki Bezpieczeństwa i zapewnia zgodność niniejszej Polityki z przepisami określającymi zasady przetwarzania danych osobowych:

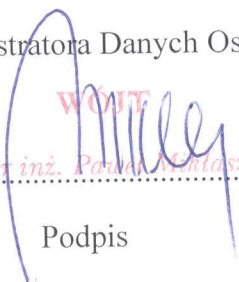
a) ustawą z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (Dz. U. z 2016 r. poz. 922);

b) rozporządzeniem 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);

c) Innymi przepisami mającymi zastosowania przy przetwarzaniu danych osobowych.

Podpis Administratora Danych Osobowych

WÓJT
mgr inż. Paweł Matusz



Podpis

.....
miejsowość i data

Upoważnienie dla Administratora Bezpieczeństwa Informacji oraz zakres obowiązków

załącznik nr 1 do „Polityki Bezpieczeństwa”

**Na podstawie § 2. Polityki Bezpieczeństwa z dnia 20 grudnia 2016 roku zgodnie z założeniami
ROZPORZĄDZENIEM 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**

Na podstawie art. 36.3 Ustawy o ochronie danych osobowych z dnia 29 sierpnia 1997r. (Dz. U. z 2016 r. poz. 922)

Administrator Danych Wójt Gminy Kuźnica powołuje w *Urzędzie Gminy Kuźnica*

Administratora Bezpieczeństwa Informacji (*imię i nazwisko*).....

pesel.....

Upoważnienie jest ważne od chwili podpisania przez strony do dnia wycofania upoważnienia przez **Administrator Danych**.

Administrator Bezpieczeństwa Informacji jest zobowiązany zastosować środki techniczne i organizacyjne zapewniające ochronę przetwarzanych danych osobowych odpowiednią do zagrożeń oraz kategorii danych objętych ochroną, a w szczególności powinien zabezpieczyć dane przed ich udostępnieniem osobom nieupoważnionym, zabranieniem przez osobę nieuprawnioną, przetwarzaniem z naruszeniem ustawy oraz zmianą, utratą, uszkodzeniem lub zniszczeniem. **Administrator Bezpieczeństwa Informacji** jest zobowiązany zgłosić zbiór danych do rejestracji Generalnemu Inspektorowi, z wyjątkiem przypadków, o których mowa w art. 43 ust. 1. **Administrator Bezpieczeństwa Informacji** nadaje uprawnienia pracownikom którzy przetwarzają dane poprzez podpisanie oświadczenia, które stanowi **załącznik nr 5 do „Polityki Bezpieczeństwa”**.

Administrator Bezpieczeństwa Informacji jest odpowiedzialny za przestrzeganie w podmiocie zapisów Instrukcji Zarządzania Systemem Informatycznym. **Administrator Bezpieczeństwa Informacji** prowadzi wszelką dokumentację opisującą sposób przetwarzania danych w podmiocie a w szczególności:

zgodnie z § 4. „Polityki Bezpieczeństwa”

Wykaz budynków, pomieszczeń lub części pomieszczeń, tworzących obszar, w którym przetwarzane są dane osobowe, który określa załącznik do „Polityki Bezpieczeństwa” nr 2

zgodnie z § 5. „Polityki Bezpieczeństwa”

Wykaz zbiorów danych osobowych wraz ze wskazaniem programów zastosowanych do przetwarzania tych danych, który określa załącznik do „Polityki Bezpieczeństwa” nr 3

zgodnie z § 6. „Polityki Bezpieczeństwa”

Opis struktury zbiorów danych wskazujący zawartość poszczególnych pól informacyjnych i powiązania między nimi oraz sposób przepływu danych pomiędzy poszczególnymi systemami, który określa załącznik do „Polityki Bezpieczeństwa” nr 4

zgodnie z § 8. „Polityki Bezpieczeństwa”

Ewidencję osób przetwarzających dane w podmiocie posiadających upoważnienie - załącznik nr 6 do „Polityki Bezpieczeństwa”

Zestawienie danych osobowych. Kiedy i przez kogo zostały do zbioru wprowadzone oraz komu są przekazywane. – załącznik nr 7 do „Polityki Bezpieczeństwa”

Oświadczam, że zapoznałem się z treścią i obowiązkami wynikającymi z tego upoważnienia oraz, że jako administrator bezpieczeństwa informacji, będę nadzorował przestrzeganie zasad ochrony danych w Urzędzie Gminy Kuźnica zgodnie z obowiązkami wynikającymi z tego upoważnienia oraz ustawy o ochronie danych osobowych.

Administrator Bezpieczeństwa Informacji

.....

Podpis

Administrator Danych

.....

Podpis

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

załącznik do „Polityki Bezpieczeństwa” nr 2 zgodnie z § 4 pkt 1 Rozporządzenia Ministra Spraw Wewnętrznych i Administracji z dnia 29 kwietnia 2004 r.

Lp.	Dokładny adres <i>(np. adres siedziby firmy gdzie przetwarzane są dane)</i>	Nr pokoju lub pomieszczenia	Uwagi
1	Urząd Gminy Kuźnica Plac Tysiąclecia Państwa Polskiego 1 16-123 Kuźnica	5	
2		8	
3		11	
		12	
4		16	
		18	
5		19	
6		21	
7		22	
8	23		
9	24		

Data i podpis Administratora Danych

2016 -12- 2 0

Wojciech
mgr inż. Jarosław Wójcik

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

załącznik do „Polityki Bezpieczeństwa” nr 3 zgodnie, z § 4 pkt 2 Rozporządzenia Ministra Spraw Wewnętrznych i Administracji z dnia 29 kwietnia 2004 r.

Lp.	Nazwa zbioru danych <i>(np. dane klientów, pracowników itd.)</i>	Programy zastosowane do przetwarzania danych <i>(np. program księgowy, papierowa ewidencja pracowników, adres internetowy aplikacji itd.)</i>	Uwagi
1	Akta osobowe pracowników oraz osób zatrudnionych na podstawie umów cywilnoprawnych.	wersja papierowa i elektroniczna – program	
2	Pracowniczy fundusz socjalny	wersja papierowa	
3	Kasa zapomogowa – pożyczkowa pracowników	wersja papierowa	
4	Rejestr zaświadczeń o zatrudnieniu i dochodach	wersja papierowa	
5	Dane mieszczące się w dokumentacji księgowej	wersja papierowa i elektroniczna – program	
6	Źródło	wersja papierowa i elektroniczna – program	
7	Ewidencja ludności	wersja papierowa i elektroniczna – program	
8	Rejestr wyborców	wersja papierowa i elektroniczna – program	
9	Dowody osobiste	wersja papierowa i elektroniczna – program	
10	Dane klientów, dotyczące umów cywilnoprawnych	wersja papierowa	
11	Rejestr Radnych Rady Gminy Kuźnica	wersja papierowa	
12	Oświadczenia majątkowe Radnych Rady Gminy, Wójta Gminy oraz kierowników	wersja papierowa i elektroniczna	

Lp.	Nazwa zbioru danych <i>(np. dane klientów, pracowników itd.)</i>	Programy zastosowane do przetwarzania danych <i>(np. program księgowy, papierowa ewidencja pracowników, adres internetowy aplikacji itd.)</i>	Uwagi
13	Rejestr softysów	wersja papierowa	
14	Ewidencja osób, którym udzielono zezwolenia na wycinkę drzew	wersja papierowa	
15	CEIDG	wersja papierowa i elektroniczna	
16	Rejestr wydanych zezwoleń na handel alkoholem	wersja papierowa	
17	Ewidencja wnioskodawców ubiegających się o dofinansowanie usunięcia wyrobów zawierających azbest	wersja papierowa	
18	Dziennik Korespondencji	wersja papierowa	
19	Rejestr skarg i wniosków	wersja papierowa	
20	Rejestr delegacji służbowych	wersja papierowa	
21	Kartoteka osób posiadających nieruchomości i grunty na terenie gminy (wymiar)	wersja papierowa i elektroniczna – program	
22	Akcyza	wersja papierowa i elektroniczna – program	
23	Rejestr decyzji o warunkach zabudowy	wersja papierowa	
24	Rejestr dzierżawców i najemców	wersja papierowa	
25	Rejestr decyzji o środowiskowych uwarunkowaniach	wersja papierowa	
26	Awanse zawodowe nauczycieli	wersja papierowa	
27	Dowóz dzieci do szkół	wersja papierowa	
28	System Informacji Oświatowej	wersja papierowa i elektroniczna – program	
29	Karta Nauczyciela	wersja papierowa	

Lp.	Nazwa zbioru danych <i>(np. dane klientów, pracowników itd.)</i>	Programy zastosowane do przetwarzania danych <i>(np. program księgowy, papierowa ewidencja pracowników, adres internetowy aplikacji itd.)</i>	Uwagi
30	Wnioski o odznaczenia i nagrody MENIS, Kuratora Oświaty dla dyrektorów szkół	wersja papierowa	
31	Pomoc materialna dla uczniów (wnioski decyzje)	wersja papierowa	
32	Pozyskiwanie europejskich i innych środków spoza budżetu gminy	wersja papierowa	
33	Współpraca z organizacjami pozarządowymi	wersja papierowa	
34	Rejestr kurierów i wykonawców akcji kurierskiej	wersja papierowa	
35	Wykaz stanowisk oraz osób z dostępem do informacji niejawnej	wersja papierowa	
36	Ankiety bezpieczeństwa osobowego (dokumentacja Pełnomocnika informacji niejawnej)	wersja papierowa	
37	Wykaz osób odpowiedzialnych za bezpieczeństwo systemu teleinformatycznego	wersja papierowa	
38	System Elektronicznego Zarządzania Dokumentacją EZD	wersja elektroniczna	
39	System monitoringu wizyjnego	wersja elektroniczna	

Data i podpis Administratora Danych

2016 - 12 - 2 0

W.O.T.
mgr inż. Paweł Wójcik

.....

Opis struktury zbiorów danych wskazujący zawartość poszczególnych pól informacyjnych i powiązania między nimi oraz sposób przepływu danych pomiędzy poszczególnymi systemami - załącznik do „Polityki Bezpieczeństwa” nr 4 zgodnie, z § 4 pkt 3 i 4 Rozporządzenia Ministra Spraw Wewnętrznych i Administracji z dnia 29 kwietnia 2004 r.

Lp.	Nazwa zbioru danych <i>(np. dane Klientów, pracowników itd.)</i>	Struktura zbiorów <i>(np. imię i nazwisko, e-mail, telefon itd.)</i>	Przeptyw danych <i>(np. wydruk danych z internetu)</i>	Uwagi
1	Akta osobowe pracowników oraz osób zatrudnionych na podstawie umów cywilnoprawnych.	Imiona, nazwisko, data i miejsce urodzenia, adres zamieszkania, nr telefonu, PESEL, NIP, nr i seria dowodu osobistego oraz książeczki wojskowej, wykształcenie, stan zdrowia, adres poczty elektronicznej	wersja papierowa i elektroniczna	
2	Pracowniczy fundusz socjalny	imiona i nazwisko, adres zamieszkania	wersja papierowa	
3	Kasa zapomogowa – pożyczkowa pracowników	imiona i nazwisko, adres zamieszkania	wersja papierowa	
4	Rejestr zaświadczeń o zatrudnieniu i dochodach	imiona i nazwisko, adres zamieszkania	wersja papierowa	
5	Dane mieszczące się w dokumentacji księgowej	imiona i nazwisko, adres zamieszkania	wersja papierowa i elektroniczna	
6	Źródło	imiona, nazwisko (rodowe), data i miejsce urodzenia, adres zamieszkania, PESEL, nr i seria dowodu osobistego, imiona rodziców	wersja papierowa i elektroniczna	
7	Ewidencja ludności	imiona, nazwisko (rodowe), data i miejsce urodzenia, adres zamieszkania, PESEL, nr i seria dowodu osobistego, imiona rodziców	wersja papierowa i elektroniczna	
8	Rejestr wyborców	Imiona, nazwisko, data urodzenia, adres zamieszkania	wersja papierowa i elektroniczna	
9	Dowody osobiste	imiona, nazwisko (rodowe), data i miejsce urodzenia, adres zamieszkania, PESEL, nr i seria dowodu osobistego, imiona rodziców	wersja papierowa i elektroniczna	

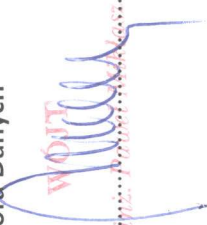
Lp.	Nazwa zbioru danych <i>(np. dane klientów, pracowników itd.)</i>	Struktura zbiorów <i>(np. imię i nazwisko, e-mail, telefon itd.)</i>	Przeptyw danych <i>(np. wydruk danych z internetu)</i>	Uwagi
10	Dane klientów, dotyczące umów cywilnoprawnych	Imiona, nazwisko, data i miejsce urodzenia, adres zamieszkania, PESEL, nr i seria dowodu osobistego	wersja papierowa	
11	Rejestr Radnych Rady Gminy Kuźnica	imiona, nazwisko, adres zamieszkania, telefon	wersja papierowa	
12	Oświadczenia majątkowe Radnych Rady Gminy, Wójta Gminy oraz kierowników	imiona, nazwisko, adres zamieszkania	wersja papierowa i elektroniczna	
13	Rejestr sołtysów	imiona, nazwisko, adres zamieszkania, telefon	wersja papierowa	
14	Ewidencja osób, którym udzielono zezwolenia na wycinkę drzew	imiona, nazwisko, adres zamieszkania, telefon	wersja papierowa	
15	Rejestr wydanych zezwoleń na handel alkoholem	imiona, nazwisko, adres zamieszkania, telefon	wersja papierowa	
16	Ewidencja wnioskodawców ubiegających się o dofinansowanie usunięcia wyrobów zawierających azbest	imiona, nazwisko, adres zamieszkania, telefon	wersja papierowa	
17	Dziennik Korespondencji	imiona, nazwisko, adres	wersja papierowa	
18	Rejestr skarg i wniosków	imiona, nazwisko, adres	wersja papierowa	
19	Rejestr delegacji służbowych	imiona, nazwisko	wersja papierowa	
20	Kartoteka osób posiadających nieruchomości i grunty na terenie gminy (wymiar)	imiona, nazwisko, adres, PESEL	Wersja papierowa i elektroniczna	
21	Akcyza	imiona, nazwisko, adres, PESEL	Wersja papierowa i elektroniczna	

Lp.	Nazwa zbioru danych <i>(np. dane klientów, pracowników itd.)</i>	Struktura zbiorów <i>(np. imię i nazwisko, e-mail, telefon itd.)</i>	Przeptyw danych <i>(np. wydruk danych z internetu)</i>	Uwagi
22	Rejestr decyzji o warunkach zabudowy	imiona, nazwisko, adres	wersja papierowa	
23	Rejestr dzierżawców i najemców	imiona, nazwisko, adres	wersja papierowa	
24	Rejestr decyzji o środowiskowych warunkach	imiona, nazwisko, adres	wersja papierowa	
25	Awanse zawodowe nauczycieli	imiona, nazwisko, adres	wersja papierowa	
26	Dowóz dzieci do szkół	imiona, nazwisko, adres	wersja papierowa	
27	System Informacji Oświatowej	imiona, nazwisko, adres	wersja papierowa i elektroniczna	
28	Karta Nauczyciela	imiona, nazwisko, adres	wersja papierowa	
29	Wnioski o odznaczenia i nagrody MENIS, Kuratora Oświaty dla dyrektorów szkół	imiona, nazwisko, adres	wersja papierowa	
30	Pomoc materialna dla uczniów (wnioski decyzje)	imiona, nazwisko, adres	wersja papierowa	
31	Pozyskiwanie europejskich i innych środków spoza budżetu gminy	imiona, nazwisko, adres	wersja papierowa	
32	Współpraca z organizacjami pozarządowymi	imiona, nazwisko, adres	wersja papierowa	
33	Rejestr kurierów i wykonawców akcji kurierskiej	imiona, nazwisko, adres	wersja papierowa	
34	Wykaz stanowisk oraz osób z dostępem do informacji niejawnej	imiona, nazwisko, adres	wersja papierowa	

Lp.	Nazwa zbioru danych <i>(np. dane klientów, pracowników itd.)</i>	Struktura zbiorów <i>(np. imię i nazwisko, e-mail, telefon itd.)</i>	Przeptyw danych <i>(np. wydruk danych z internetu)</i>	Uwagi
35	Ankiety bezpieczeństwa osobowego (dokumentacja Pełnomocnika informacji niejawniej)	imiona, nazwisko, adres	wersja papierowa	
36	Wykaz osób odpowiedzialnych za bezpieczeństwo systemu teleinformatycznego	imiona, nazwisko, adres	wersja papierowa	
37	System Elektronicznego Zarządzania Dokumentacją EZD	imiona, nazwisko, adres	wersja elektroniczna	
38	System monitoringu wizyjnego	wizerunek osób	wersja elektroniczna	

Data i podpis Administratora Danych

2016 -12- 2 0

.....




**Upoważnienie do przetwarzania danych osobowych załącznik nr 5 do „Polityki Bezpieczeństwa”
zgodnie z Art 37 Ustawy o ochronie danych osobowych z dnia 29 sierpnia 1997 r.**

Wójt Gminy Kuźnica jako Administrator Danych

dnia nadaje upoważnienie do przetwarzania danych osobowych
w podmiocie dla:

Imię i nazwisko:

Adres zamieszkania:

Nr PESEL:

Stanowisko służbowe:

Upoważniony otrzymuje dostęp do poniższych zasobów danych osobowych w celu ich przetwarzania:

.....
.....
.....

Upoważnienie nadaje się do dnia

Ja niżej podpisany zobowiązuje się do przestrzegania zasad panujących w podmiocie w zakresie ochrony danych osobowych a w szczególności „Polityki Bezpieczeństwa” oraz respektowania zapisów **Ustawy o ochronie danych osobowych z dnia 29 sierpnia 1997 r.** Upoważnionego zobowiązuje się do zapewnienia ochrony danych, zachowania tajemnicy dotyczącej danych osobowych przetwarzanych w podmiocie oraz sposobów zabezpieczeń a także zgłaszania faktu naruszenia/zagrożenia zabezpieczeń danych osobowych.

Oświadczam, że zostałem(am) zapoznany(a) z przepisami Ustawy o ochronie danych osobowych (Dz. U. z 2016 r. poz. 922) oraz 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 ze zm.).

Oświadczam, że zostałem(am) poinformowany o grożącej, stosownie do przepisów Rozdziału 8 Ustawy o ochronie danych osobowych, odpowiedzialności karnej. Niezależnie od odpowiedzialności przewidzianej w wymienionych przepisach, mam świadomość, że naruszenie zasad ochrony danych osobowych, obowiązujących w podmiocie może zostać uznane za ciężkie naruszenie podstawowych obowiązków pracowniczych i skutkować odpowiedzialnością dyscyplinarną.

Administrator Danych

.....

Podpis

Użytkownik

.....

Podpis

Ewidencja osób przetwarzających dane w podmiocie posiadających upoważnienie

załącznik nr 6 do „Polityki Bezpieczeństwa” zgodnie z Art 39. 1. Ustawy o ochronie danych osobowych z dnia 29 sierpnia 1997 r.

Lp.	Imię i nazwisko	Stanowisko służbowe	Data nadania upoważnienia	Data ustania upoważnienia	Wykaz zbiorów danych wynikających z upoważnienia	Identyfikator <i>(Jeżeli dane są przetwarzane w systemie informatycznym)</i>

Data i podpis Administratora Danych

.....

Zestawienie danych osobowych z informacją kiedy i przez kogo zostały do zbioru wprowadzone oraz komu są przekazywane.

załącznik nr 7 do „Polityki Bezpieczeństwa” zgodnie z art. 38 Ustawy o ochronie danych osobowych z dnia 29 sierpnia 1997 r.

Lp.	Rodzaj udostępnionych danych osobowych	Data wprowadzenia danych do zbioru	Data przekazania danych osobowych	Imię i nazwisko osoby która otrzymała dane	Cel przekazania danych osobowych

Data i podpis Administratora Danych

.....

Określenie środków technicznych i organizacyjnych niezbędnych dla zapewnienia poufności, integralności i rozliczalności przetwarzanych danych

załącznik nr 8 do „Polityki Bezpieczeństwa” zgodnie z art. 38 Ustawy o ochronie danych osobowych z dnia 29 sierpnia 1997 r.

1. Administrator Danych zapewnia zastosowanie środków technicznych i organizacyjnych niezbędnych dla zapewnienia poufności, integralności, rozliczalności i ciągłości przetwarzanych danych.

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

W odniesieniu do innych osób upoważnionych do przetwarzania danych osobowych, w sytuacji naruszeń obowiązków wynikających z niniejszego dokumentu ponieść mogą odpowiedzialność odszkodowawczą. Wszystkie osoby upoważnione do przetwarzania danych osobowych mogą ponieść odpowiedzialność karną w sytuacji naruszenia zasad określonych w niniejszym dokumencie.

Data i podpis Administratora Danych

2016 -12- 2 0

WÓJT
mgr inż. Paweł Woźniak

INSTRUKCJA ZARZĄDZANIA SYSTEMEM INFORMATYCZNYM

Administrator Danych – Wójt Gminy Kuźnica

Zgodnie z **ROZPORZĄDZENIEM 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
wdraża dokument o nazwie „Instrukcja zarządzania systemem informatycznym” zwany dalej „instrukcją”. Zapisy tego dokumentu wchodzi w życie z dniem 20 grudnia 2016 roku

Ilekroć w „instrukcji” jest mowa o:

- 1) Urzędzie — rozumie się przez to Urząd Gminy Kuźnica Plac Tysiąclecia PP 1, 16-123 Kuźnica;
- 2) ustawie — rozumie się przez to ustawę z dnia 29 sierpnia 1997 r. o ochronie danych osobowych, zwaną dalej „ustawą”;
- 3) identyfikatorze użytkownika — rozumie się przez to ciąg znaków literowych, cyfrowych lub innych jednoznacznie identyfikujący osobę upoważnioną do przetwarzania danych osobowych w systemie informatycznym;
- 4) hasle — rozumie się przez to ciąg znaków literowych, cyfrowych lub innych, znany jedynie osobie uprawnionej do pracy w systemie informatycznym;
- 5) sieci telekomunikacyjnej — rozumie się przez to sieć telekomunikacyjną w rozumieniu art. 2 pkt 23 ustawy z dnia 21 lipca 2000 r. — Prawo telekomunikacyjne (Dz. U. Nr 73, poz. 852, z późn. zm.);
- 6) sieci publicznej — rozumie się przez to sieć publiczną w rozumieniu art. 2 pkt 22 ustawy z dnia 21 lipca 2000 r. — Prawo telekomunikacyjne;
- 7) teletransmisji — rozumie się przez to przesyłanie informacji za pośrednictwem sieci telekomunikacyjnej;
- 8) rozliczalności — rozumie się przez to właściwość zapewniającą, że działania podmiotu mogą być przypisane w sposób jednoznaczny tylko temu podmiotowi;
- 9) integralności danych — rozumie się przez to właściwość zapewniającą, że dane osobowe nie zostały zmienione lub zniszczone w sposób nieautoryzowany;
- 10) raporcie — rozumie się przez to przygotowane przez system informatyczny zestawienia zakresu i treści przetwarzanych danych;
- 11) poufności danych — rozumie się przez to właściwość zapewniającą, że dane nie są udostępniane nieupoważnionym podmiotom;
- 12) uwierzytelnianiu — rozumie się przez to działanie, którego celem jest weryfikacja deklarowanej tożsamości podmiotu.

§ 1

Za przestrzeganie w Urzędzie Gmina Kuźnica zapisów „instrukcji” odpowiedzialny jest Administrator danych lub zgodnie z zapisem §2 „Polityki Bezpieczeństwa” wyznaczony **Administrator Bezpieczeństwa Informacji**

§2

W związku z tym, że w Urzędzie Gmina Kuźnica przynajmniej jedno urządzenie systemu informatycznego, służącego do przetwarzania danych osobowych, połączone jest z siecią publiczną, oraz uwzględniając kategorie przetwarzanych danych i zagrożenia wprowadza się poziom bezpieczeństwa przetwarzania danych osobowych w systemie informatycznym na poziomie **wysokim**, a w związku z tym wprowadza się poniższe postanowienia:

I

Obszar, w który są przetwarzane dane, zabezpiecza się przed dostępem osób nieuprawnionych na czas nieobecności w nim osób upoważnionych do przetwarzania danych osobowych. Przebywanie osób nieuprawnionych w obszarze, w którym są przetwarzane dane, jest dopuszczalne za zgodą Administratora Danych, Administratora Bezpieczeństwa Informacji lub w obecności osoby upoważnionej do przetwarzania danych osobowych.

II

1. W systemie informatycznym służącym do przetwarzania danych osobowych, przetwarzać dane mogą wyłącznie osoby posiadające aktualne upoważnienie nadane przez Administratora Bezpieczeństwa Informacji. Użytkownik przetwarzający dane po otrzymaniu upoważnienia oraz loginu i hasła jest zobowiązany niezwłocznie dokonać zmiany hasła oraz zachować je w tajemnicy. Użytkownik jest zobowiązany do zmiany hasła nie rzadziej niż co 30 dni. Hasło nadane przez użytkownika musi składać się z co najmniej z 8 znaków, zawierać małe i wielkie litery oraz cyfry lub znaki specjalne.

2. Jeżeli dostęp do danych przetwarzanych w systemie informatycznym posiadają co najmniej dwie osoby, wówczas zapewnia się, aby:

w systemie tym rejestrowany był dla każdego użytkownika odrębny identyfikator oraz aby dostęp do danych był możliwy wyłącznie po wprowadzeniu identyfikatora i dokonaniu uwierzytelnienia.

III

System informatyczny służący do przetwarzania danych osobowych zabezpiecza się, w szczególności przed:

1) działaniem oprogramowania, którego celem jest uzyskanie nieuprawnionego dostępu do systemu informatycznego

•poprzez zainstalowanie programu antywirusowego.

2) utratą danych spowodowaną awarią zasilania lub zakłóceniami w sieci zasilającej poprzez zastosowanie zasilacza awaryjnego ups.

IV

1. Identyfikator użytkownika, który utracił uprawnienia do przetwarzania danych, nie może być przydzielony innej osobie.

2. W przypadku gdy do uwierzytelniania użytkowników używa się hasła, jego zmiana następuje nie rzadziej niż co 30 dni. Hasło składa się ono co najmniej z 8 znaków, zawiera małe i wielkie litery oraz cyfry lub znaki specjalne.

3. Dane osobowe przetwarzane w systemie informatycznym zabezpiecza się przez wykonywanie

kopii zapasowych zbiorów danych oraz programów służących do przetwarzania danych.

4. Kopie zapasowe:

- a) przechowuje się w miejscach zabezpieczających je przed nieuprawnionym przejęciem, modyfikacją, uszkodzeniem lub zniszczeniem w pomieszczeniu zamkniętym,
- b) usuwa się niezwłocznie po ustaniu ich użyteczności.

V

Osoba użytkująca komputer przenośny zawierający dane osobowe zachowuje szczególną ostrożność podczas jego transportu, przechowywania i użytkowania poza obszarem przetwarzania danych osobowych w tym stosuje hasła dostępu do komputera przenośnego oraz do plików, w których przetwarzane są dane osobowe.

VI

Urządzenia, dyski lub inne elektroniczne nośniki informacji, zawierające dane osobowe, przeznaczone do:

- 1) likwidacji — pozbawia się wcześniej zapisu tych danych, a w przypadku gdy nie jest to możliwe, uszkadza się w sposób uniemożliwiający ich odczytanie;
- 2) przekazania podmiotowi nieuprawnionemu do przetwarzania danych — pozbawia się wcześniej zapisu tych danych, w sposób uniemożliwiający ich odzyskanie (uszkodzenie mechaniczne / fizyczne);
- 3) naprawy — pozbawia się wcześniej zapisu tych danych w sposób uniemożliwiający ich odzyskanie albo naprawia się je pod nadzorem osoby upoważnionej przez administratora danych.

§3

1. Dla każdej osoby, której dane osobowe są przetwarzane w systemie informatycznym — z wyjątkiem systemów służących do przetwarzania danych osobowych ograniczonych wyłącznie do edycji tekstu w celu udostępnienia go na piśmie — system ten zapewnia odnotowanie:

- 1) daty pierwszego wprowadzenia danych do systemu;
- 2) identyfikatora użytkownika wprowadzającego dane osobowe do systemu, chyba że dostęp do systemu informatycznego i przetwarzanych w nim danych posiada wyłącznie jedna osoba;
- 3) źródła danych, w przypadku zbierania danych, nie od osoby, której one dotyczą;
- 4) informacji o odbiorcach, w rozumieniu art. 7 pkt 6 ustawy, którym dane osobowe zostały udostępnione, dacie i zakresie tego udostępnienia, chyba że system informatyczny używany jest do przetwarzania danych zawartych w zbiorach jawnych;
- 5) sprzeciwu, o którym mowa w art. 32 ust. 1 pkt 8 ustawy.

2. Odnotowanie informacji, o których mowa w ust. 1 pkt 1 i 2, następuje automatycznie po zatwierdzeniu przez użytkownika operacji wprowadzenia danych.

3. Dla każdej osoby, której dane osobowe są przetwarzane w systemie informatycznym, system zapewnia sporządzenie i wydrukowanie raportu zawierającego w powszechnie zrozumiałej formie informacje, o których mowa w ust. 1.

4. W przypadku przetwarzania danych osobowych, w co najmniej dwóch systemach informatycznych, wymagania, o których mowa w ust. 1 pkt 4, mogą być realizowane w jednym z nich lub w odrębnym systemie informatycznym przeznaczonym do tego celu.

§ 4.

W sprawach nieuregulowanych w niniejszej „instrukcji” mają zastosowanie przepisy ustawy o ochronie danych osobowych z dnia 29 sierpnia 1997 r. oraz **ROZPORZĄDZENIEM 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

Podpis Administratora Danych Osobowych

WOJT

mgr inż. Radosław Adamski

Podpis