WÓJT GMINY
GORZYCE
pow.tarnobrzeski
woj.podkarpackie

ZARZĄDZENIE Nr 137/18
Wójta Gminy Gorzyce
z dnia 6 grudnia 2018 roku

w sprawie **wprowadzenia Polityki Bezpieczeństwa w Urzędzie Gminy w Gorzycach.**

Na podstawie art. 33 ust. 3 ustawy z dnia 8 marca 1990 r. o samorządzie gminnym (t.j. Dz. U. z 2018 r., poz. 994 ze zm.) i art. 24 ust. 1 i2 Rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/4/WE Wójt Gminy Gorzyce

Zarządza się, co następuje:

§ 1

Celem określenia reguł i zasad obowiązujących przy przetwarzaniu danych osobowych w Urzędzie Gminy Gorzyce, wprowadza się Politykę Bezpieczeństwa, która stanowi załącznik do niniejszego zarządzenia,

§ 2

Zobowiązuje się wszystkich pracowników Urzędu Gminy Gorzyce do przestrzegania postanowień zawartych w Polityce Bezpieczeństwa

§ 3

Uchyla się zarządzenie nr 83/16 Wójta Gminy Gorzyce z dnia 26 lipca 2016r. w sprawie wprowadzenia Polityki Bezpieczeństwa w Urzędzie Gminy w Gorzycach.

§ 4

Zarządzenie wchodzi w życie z dniem podpisania.

WÓJT
mgr Leszek Surdy

dr Bogusław Sowa
ADWOKAT
Sprawdzono pod względem
formalno-prawnym

URZĄD GMINY GORZYCE
ul. Sandomierska 75
39-432 Gorzyce
tel. 15 836 20 75, tel./fax 15 836 22 09
NIP 867-11-90-262

Załącznik
do zarządzenia nr 137/18
Wójta Gminy Gorzyce
z dnia 6 grudnia 2018r.

Polityka Bezpieczeństwa

Administrator Danych Osobowych:
Wójt Gminy Gorzyce mgr Leszek Surdy

§1

1. Polityka Bezpieczeństwa Informacji jest dokumentem opracowanym i wdrożonym w **Urzędzie Gminy w Gorzycach** w celu zapewnienia przestrzegania zasad ochrony danych osób fizycznych, które są przez nią przetwarzane oraz opisu stosowanych środków technicznych i organizacyjnych, mających na celu zapewnienie ochrony przetwarzanych danych osobowych odpowiedniej do zagrożeń oraz kategorii danych objętych ochroną.

2.**Wójt Gminy Gorzyce** jest administratorem danych osobowych osób fizycznych, które są przetwarzane w ramach prowadzonej przez urząd działalności.

3. Mając na uwadze zgodne z prawem przetwarzanie danych osobowych klientów, pracowników, współpracowników oraz innych osób fizycznych, **Wójt Gminy Gorzyce, zwany dalej także Administratorem Danych Osobowych**, wprowadza do stosowania niniejszą Politykę Bezpieczeństwa.

4. **Wójt Gminy Gorzyce** zapewnia, że:
a) nie prowadzi przetwarzania danych, które wiązałoby się z wysokim ryzykiem naruszenia praw lub wolności osoby fizycznej;
b) uwzględnia ochronę danych w fazie projektowania oraz stosuje domyślną politykę ochrony tam, gdzie ma to zastosowanie
c) respektuje prawa osoby, której dane dotyczą, w szczególności prawa dostępu do danych, sprostowania danych, bycia zapomnianym, prawo do ograniczenia przetwarzania, prawo do przenoszenia danych, prawo do sprzeciwu, zgodnie z aktualnie obowiązującymi przepisami prawa;
d) jeśli dany rodzaj przetwarzania - w szczególności z użyciem nowych technologii - ze względu na swój charakter, zakres, kontekst i cele może powodować wysokie ryzyko naruszenia praw lub wolności osób fizycznych, to przed rozpoczęciem przetwarzania dokona oceny skutków dla planowanych operacji przetwarzania danych osobowych.

5. **Administrator Danych** podlega obowiązkowi powołania Administratora Bezpieczeństwa Informacji, który od 25 maja 2018 r. będzie pełnił funkcję Inspektora Ochrony Danych, w zakresie określonym przepisami prawa.

6. Pracownicy i współpracownicy **Urzędu Gminy w Gorzycach** są zobowiązani do zapoznania się z obowiązującymi procedurami i instrukcjami, a także stosowania tych zasad.

§2
Definicje

7. **Administrator Danych Osobowych** - oznacza organ, jednostkę organizacyjną, podmiot lub osobę decydującą o celach i środkach przetwarzania danych osobowych. W niniejszym dokumencie rozumie się przez to **Wójta Gminy Gorzyce**

8. **Dane osobowe** - za dane osobowe uważa się wszelkie informacje dotyczące zidentyfikowanej lub możliwej do zidentyfikowania osoby fizycznej. Daną osobową jest każda informacja, na podstawie której można bezpośrednio lub pośrednio zidentyfikować tożsamość osoby fizycznej, w szczególności poprzez powołanie się na numer identyfikacyjny albo jeden lub kilka specyficznych czynników określających jej cechy fizyczne, fizjologiczne, umysłowe, ekonomiczne, kulturowe lub społeczne.

9. **Dane osobowe zwykłe** - to dane osobowe, które określają podstawowe dane identyfikujące osobę fizyczną. Mogą być to takie dane, jak imię i nazwisko, data urodzenia, numer PESEL, adres zamieszkania, adres e-mail, numer telefonu.

10. **Dane osobowe wrażliwe** – dane osobowe ujawniające pochodzenie rasowe lub etniczne, poglądy polityczne, przekonania religijne lub filozoficzne, przynależność wyznaniowa , partyjna lub związkowa , stan zdrowia i wszelkie informacje dotyczące zdrowia psychicznego lub fizycznego, kod genetyczny, dane genetyczne i biometryczne, nałogi lub życie seksualne, dotyczące skazań, orzeczeń o ukaraniu, mandatów karnych, a także innych orzeczeń, wydanych w postępostępowaniu sądowym lub administracyjnym.

11. **Ustawa** – oznacza ustawę z dnia 29 sierpnia 1997 r. o ochronie danych osobowych.

12. **RODO** - oznacza Rozporządzenie Parlamentu Europejskiego i Rady UE 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych).

13. **Zbiór danych** – dane osobowe zgromadzone w usystematyzowany sposób, pozwalający na łatwe dotarcie do konkretnej informacji. Oznacza to, z e dane dostępne są według określonych kryteriów. Zbiór może być prowadzony w formie papierowej lub w systemie informatycznym.

14. **Przetwarzanie danych** – wykonywanie jakichkolwiek operacji na danych osobowych, takich jak: zbieranie, utrwalanie, przechowywanie, opracowywanie, zmienianie, udostępnianie i ich usuwanie, niezależnie od formy, w jakiej wykonywane są te czynności. Zasady określone w niniejszej polityce należy stosować przy każdej operacji na danych.

15. **Powierzenie danych osobowych** - przekazanie danych osobowych innemu podmiotowi w określonym celu i zakresie w ramach realizacji umowy.

16. **Udostepnienie danych** - przekazanie danych osobowych innemu administratorowi danych na podstawie odpowiednich przepisów prawa.

17. **Osoba upoważniona** - osoba upoważniona przez administratora danych osobowych do przetwarzania danych w celu i zakresie określonym w upoważnieniu. Osobą upoważnioną może być osoba zatrudniona na podstawie umowy o pracę, umowy cywilnoprawnej, stażysta lub wolontariusz.

18. **Państwo trzecie** - państwo nienależące do Europejskiego Obszaru Gospodarczego.

19. **System informatyczny** – zespół powiązanych ze sobą środków technicznych (urządzenia komputerowe, drukujące, oprogramowanie), zabezpieczeń, sieć informatyczna i udostępniane przez nią zasoby;

20. **Użytkownik** – osoba upoważniona przez Administratora Danych Osobowych, przetwarzająca dane osobowe w systemie informatycznym na podstawie przydzielonych jej uprawnień;

21. **Identyfikator użytkownika** - nazwa w systemie informatycznym przypisana określonemu użytkownikowi. Do identyfikatora przypisane jest konto użytkownika oraz ściśle określone uprawnienia, które umożliwiają dostęp p do danego komputera, systemu lub sieci.

22. **Hasło** — mieszany ciąg znaków literowych, cyfrowych lub innych, znany jedynie osobie uprawnionej do pracy w systemie informatycznym;

23. **Uwierzytelnienie** — działanie, którego celem jest weryfikacja tożsamości użytkownika w systemach informatycznych, najczęściej poprzez prawidłowe wprowadzenie identyfikatora (loginu) i hasła użytkownika;

§3

Zadania i obowiązki Administratora Danych Osobowych

1. Administrator Danych Osobowych decyduje o celach i środkach przetwarzania danych. Do jego obowiązków należy w szczególności:
a) dochowanie szczególnej staranności przy przetwarzaniu danych osobowych w celu ochrony interesów osób, których dane dotyczą ;

b) stosowanie środków technicznych i organizacyjnych, zapewniających ochronę przetwarzanych danych osobowych odpowiednią do zagrożeń oraz kategorii danych objętych ochroną ;

c) nadzorowanie i kontrolowanie wdrożonych do stosowania środków technicznych i organizacyjnych zapewniających ochronę przetwarzanych danych osobowych odpowiednią do zagrożeń oraz kategorii tych danych, w szczególności zabezpieczających dane przed udostepnieniem osobom nieupoważnionym, zabraniem przez osobę nieuprawnioną, utratą, zmianą, uszkodzeniem lub zniszczeniem;

d) kontrola nad tym kto i w jakim zakresie ma dostęp do danych, w szczególności prowadzenie ewidencji osób upoważnionych do przetwarzania danych osobowych;

e) respektowanie praw osób, których dane dotyczą, w szczególności prawa dostępu do treści danych oraz och poprawiania, a także prawa do przenoszenia danych, prawa do bycia zapomnianym, prawa do wstrzymania przetwarzania danych ze względu na szczególną sytuacją osoby - na podstawie obowiązujących przepisów prawa.

f) spełnienie obowiązku informacyjnego wobec osoby, której dane dotyczą , zgodnie z aktualnie obowiązującymi przepisami;

g) zapewnienia zapoznania pracowników i współpracowników, zgodnie z obowiązującymi przepisami prawa w zakresie ochrony danych osobowych.

§4

Zadania i obowiązki Inspektora Ochrony Danych

1. Inspektor ochrony danych nadzoruje i kontroluje zgodność przetwarzania danych z obowiązującymi przepisami w tym zakresie, w szczególności:

a) zapewnienia zapoznanie administratora danych oraz pracowników z obowiązującymi przepisami prawa w zakresie ochrony danych osobowych;

b) nadzoruje i kontroluje wdrożone przez administratora danych do stosowania środków technicznych i organizacyjnych zapewniających ochronę przetwarzanych danych osobowych odpowiednią do zagrożeń oraz kategorii tych danych, w szczególności zabezpieczających dane przed udostepnieniem osobom nieupoważnionym, zabraniem przez osobę nieuprawnioną, utratą, zmianą, uszkodzeniem lub zniszczeniem;

c) pełnienie punktu kontaktowego dla organu nadzorczego w kwestiach związanych z przetwarzaniem, współpracą z organem nadzorczym;

d) udzielenie na żądanie zaleceń co do oceny skutków dla ochrony danych oraz monitowanie jej wykonania zgodnie z art. 35 RODO.

§5

Zadania i obowiązki kierownika komórki organizacyjnej

1. Kierownik komórki organizacyjnej jest zobowiązany do:

a) sprawowania w podległej komórce organizacyjnej nadzoru nad obiegiem oraz przechowywaniem dokumentów zawierających dane osobowe;

b) umożliwienia przeprowadzenia Inspektorowi ochrony danych czynności w toku sprawdzenia planowanego lub doraźnego;

c) zapoznania pracowników z wprowadzoną dokumentacją przetwarzania danych w zakresie upoważnienia na danym stanowisku.

§6

Zadania i obowiązki osób upoważnionych

1. Do przetwarzania danych osobowych mogą być dopuszczone wyłącznie osoby, które posiadają imienne upoważnienie nadane przez Administratora Danych Osobowych. Wzór upoważnienia do przetwarzania danych osobowych stanowi *załącznik nr 1* do niniejszej polityki.

2. Upoważnienie wydawane jest przez Administratora Danych Osobowych w celu i zakresie wynikającym z zadań i obowiązków służbowych.

3. Upoważnienie wydawane jest na czas trwania umowy o pracę lub innej umowy cywilnoprawnej, a także na czas wykonania określonego zadania, które związane jest z przetwarzaniem danych.

4. Osoba upoważniona do przetwarzania danych osobowych składa pisemne oświadczenia o zobowiązaniu do zachowania w tajemnicy danych osobowych oraz sposobów ich zabezpieczenia. Wzór oświadczenia osoby upoważnionej do przetwarzania danych osobowych stanowi *załącznik nr 2* do niniejszej polityki.

5. Osoba upoważniona do przetwarzania danych jest zobowiązana do:
a) przetwarzania danych osobowych zgodnie z upoważnieniem wydanym przez Administratora Danych Osobowych;

b) stosowania się do instrukcji i procedur zawartych w dokumentacji przetwarzania danych, wydanych przez Administratora Danych Osobowych;

c) stosowania wprowadzonych środków organizacyjnych i technicznych, zapewniających ochronę przetwarzania danych, w szczególności przed ich udostepnieniem, kradzieżą , uszkodzeniem lub zniszczeniem przez osoby nieupoważnione;

d) umożliwienia przeprowadzenia czynności w toku sprawdzenia planowanego lub doraźnego prowadzonego przez Administratora Danych Osobowych lub na jego zlecenie;

e) sprawowania nadzoru nad obiegiem oraz przechowywaniem i zabezpieczeniem dokumentów zawierających dane osobowe, do których ma dostęp w chwili wykonywania czynności służbowych;

f) każdorazowego niezwłocznego informowania Administratora Danych Osobowych w sytuacji naruszenia ochrony danych osobowych lub uzasadnionego podejrzenia takiego naruszenia;

6. Administrator Danych Osobowych prowadzi ewidencję osób upoważnionych do przetwarzania danych osobowych. Wzór ewidencji osób upoważnionych do przetwarzania danych osobowych stanowi *załącznik nr 3* do niniejszej polityki.

§7

Ogólne zasady przetwarzania danych osobowych

1. **Urząd Gminy w Gorzycach** przetwarza dane osobowe wyłącznie, gdy jest to dopuszczone aktualnie obowiązującymi przepisami prawa.

2. Dane osobowe mogą być przetwarzane wyłącznie w celu i zakresie, w jakim zostały zgromadzone, a także nie dłużej niż jest to niezbędne dla osiągniecia tego celu.

3. Dane osobowe po wykorzystaniu są niezwłocznie usuwane lub przechowywane wyłącznie w postaci uniemożliwiającej identyfikacje osób, których dotyczą , o ile przepisy odrębnych ustaw nie precyzują określonego czasu przechowywania danych.

4. Dane osobowe są przetwarzane przez **Urząd Gminy w Gorzycach ,** gdy:
a) Administrator Danych Osobowych uzyskał zgodę osoby, której dane dotyczą;

b) jest to niezbędne do wykonania umowy, której stroną jest osobą lub do podjęcia działań na żądanie osoby, której dane dotyczą przed zawarciem umowy;

c) jest to niezbędne do wypełnienia obowiązku prawnego ciążącego na administratorze danych osobowych;

d) jest niezbędne do celów wynikających z prawnie uzasadnionych interesów realizowanych przez administratora lub przez stronę trzecią;

5. Administrator Danych nie przetwarza danych na teranie państwa trzeciego, ani nie powierza danych innym podmiotom poza obszarem Europejskiego Obszaru Gospodarczego.

6. Administrator Danych nie przetwarza szczególnych kategorii danych, tzw. danych wrażliwych, za wyjątkiem, gdy jest to niezbędne do wypełnienia obowiązków i wykonywania szczególnych praw przez administratora lub osobę, której dane dotyczą, w dziedzinie prawa pracy, zabezpieczenia społecznego i ochrony socjalnej, o ile jest to dozwolone przepisami prawa.

7. W przypadku gdy dane osobowe są niekompletne, nieaktualne, nieprawdziwe lub zostały zebrane z naruszeniem ustawy lub są zbędne do realizacji celu, dla którego zostały zebrane, Administrator Danych Osobowych jest zobowiązany do ich uzupełnienia, uaktualnienia, sprostowania lub usunięcia.

8. Administrator Danych Osobowych stosuje ogólne zasady przetwarzania danych osobowych, tj.:
a) zasadę legalności - dane mogą być przetwarzane, jeśli Administrator Danych Osobowych będzie dysponował przynajmniej jedną z przesłanek przetwarzania wskazanych w obowiązujących przepisach prawa;
b) zasadę celowości - dane przetwarza tylko dla zgodnych z prawem celów i nie poddaje dalszemu przetwarzaniu niezgodnemu z tymi celami;
c) zasadę adekwatności - przetwarzane dane niezbędne ze względu na cel zbierania danych, nie zbiera danych na tzw. zapas.
d) zasadę merytorycznej poprawności - zapewnia się, aby dane były zgodne z prawdą, kompletne i aktualne;
e) zasada ograniczenia czasowego - dane nie są przetwarzane dłużej niż to jest niezbędne do osiągniecia celu przetwarzania lub uregulowane obowiązującymi przepisami;
f) zasadę integralności i poufności - dane przetwarzane w sposób zapewniający odpowiednie bezpieczeństwo danych, w tych ochronę przed niedozwolonym lub niezgodnym z prawem przetwarzaniem, przypadkową utratą, zniszczeniem lub uszkodzeniem, za pomocą odpowiednich środków technicznych lub organizacyjnych;

§8

Obszar przetwarzania danych osobowych i jego ochrona

1. Obszarem przetwarzania u Administratora Danych Osobowych obejmuje się wszystkie pomieszczenia, w których wykonuje się jakiekolwiek operacje na danych osobowych, w szczególności wprowadza się , modyfikuje, archiwizuje, usuwa dane, a także wszystkie miejsca, gdzie przechowuje się nośniki informacji zawierające dane osobowe.

2. Wykaz obszaru przetwarzania prowadzony jest i aktualizowany przez Administratora Danych Osobowych. Wzór wykazu stanowi *załącznik nr 4* do niniejszej polityki.

3. W celu ochrony obszaru przetwarzania przed dostępem osób nieupoważnionych Administrator Danych Osobowych stosuje politykę klucza, alarm, zabezpieczając w ten sposób budynki lub pomieszczenia, w których przetwarza się dane osobowe.

4. Dostęp do pomieszczenia, w którym dane osobowe są przetwarzane mogą mieć wyłącznie osoby upoważnione. Obecność innych osób może mieć miejsce wyłącznie pod nadzorem osoby upoważnionej.

5. W przypadku, gdy nie jest możliwe nadzorowanie pracy osób nieupoważnionych w obszarze przetwarzania Administrator Danych Osobowych zapewnia zabezpieczenie danych osobowych, znajdujących się w danym pomieszczeniu, w taki sposób, aby nie było możliwe zabranie, zniszczenie lub jakikolwiek dostęp do tych danych.

§9

Obowiązek informacyjny

1. Każdej osobowe przysługuje prawo do kontroli przetwarzania danych, które jej dotyczą, zawartych w zbiorach danych u Administratora Danych Osobowych.

2. Administrator Danych informuje osoby, której dane dotyczą, o swoich danych, adresie siedziby, celu zbierania danych, obowiązku lub dobrowolności ich podania, a także przekazuje inne informacje, które mogą być wymagane aktualnie obowiązującymi przepisami prawa.

3. Obowiązek informacyjny w przypadku pozyskiwania danych bezpośrednio od osoby, której dane dotyczą wykonywane jest przed rozpoczęciem ich zbierania danych. Osobę, której dane dotyczą informuje się o:
a) dokładnej nazwie i adresie swojej siedziby;

b) celu zbierania danych;

c) dobrowolności lub obowiązku podania danych, a jeżeli taki obowiązek istnieje o jego podstawie prawnej;

d) prawie wglądu do treści swoich danych oraz możliwości ich poprawiania.

e) innych informacjach, wynikających z aktualnych przepisów prawa, szczególnie od 25 maja 2018 r. dodaje informacje o tym:

- w jakim celu przetwarza dane na podstawie interesu prawnego administratora danych;

- czy ma zamiar przekazania danych do państwa trzeciego;

- podaje okres przez który dane będą przetwarzane, a gdy nie jest to możliwe to podaje kryteria ustalenia tego okresu;

- informacje o prawie do żądania sprostowania, usunięcia lub ograniczenia przetwarzania lub o prawie do wniesienia sprzeciwu wobec przetwarzania, a także o prawie do przenoszenia danych (jeśli przetwarzanie odbywa się na podstawie umowy lub zgody);

- jeśli przetwarzanie odbywa się na podstawie zgody osoby to informuje ją o prawie do cofnięcia zgody w dowolnym momencie, bez wpływu na zgodność z prawem przetwarzania , którego dokonano na podstawie zgody przed jej cofnięciem;

- o prawie wniesienia skargi do organu nadzorczego;

- o profilowaniu i jego konsekwencjach, jeśli jest to zasadne;

4. Powyższych informacji nie udziela się jeśli osoba dysponuje już tymi informacjami, a Administrator Danych Osobowych będzie w stanie to wykazać.

5. W przypadku zbierania danych osobowych nie bezpośrednio od osoby, której one dotyczą , osobę te należy w rozsądnym terminie po pozyskaniu danych osobowych - najpóźniej w ciągu miesiąca - mając na uwadze konkretne okoliczności przetwarzania danych osobowych - poinformować ją dodatkowo o:
a) źródle danych

b) innych uprawnieniach wynikających z aktualnie obowiązujących przepisów;

6. Administrator Danych Osobowych ma również na uwadze, że każda osoba, której dane dotyczą , może wystąpić z wnioskiem o otrzymanie informacji o jej danych, które są przetwarzane w zbiorze u Administratora Danych Osobowych, zgodnie z obowiązującymi przepisami. Odpowiedź na zapytanie osoby, której dane dotyczą , jest udzielana na piśmie w terminie nieprzekraczającym miesiąca od daty wpłynięcia wniosku.

7. Wyłączenie obowiązku udzielenia odpowiedzi następuje wyłącznie w przypadkach, określonych aktualnie obowiązującymi przepisami prawa.

§10

Postępowanie w przypadku naruszenia bezpieczeństwa ochrony danych osobowych.

1. W **Urzędzie Gminy w Gorzycach** został ustalony sposób postępowania w przypadku stwierdzenia lub uzasadnionego o podejrzenia naruszenia bezpieczeństwa danych osobowych, bez względu na formę przetwarzania danych.

2. Szczegółowy opis zasad postępowania w przypadku naruszenia ochrony danych został ustalony w Instrukcji postępowania w przypadku naruszenia ochrony danych, która została opracowana i wdrożona w **Urzędzie Gminy w Gorzycach.**

§11

Powierzenie przetwarzania danych osobowych

1. Powierzenie przetwarzania danych osobowych odbywa się wyłącznie na podstawie umowy zawartej na piśmie pomiędzy Administratorem Danych a podmiotem trzecim, któremu dane się powierza w celu i zakresie wykonania konkretnej czynności w imieniu Administratora Danych.

2. Umowa powierzenia określa w szczególności cel i zakres powierzenia przetwarzania danych osobowych.

3. Administrator Danych Osobowych powierza dane osobowe wyłącznie tym podmiotom, które gwarantują zastosowanie środków organizacyjnych i technicznych, zabezpieczających dane przed dostępem osób nieupoważnionych na zasadach określonych w przepisach prawa.

4. Administrator Danych Osobowych sprawuje kontrolę nad tym w jakim zakresie i w jakim celu powierza dane osobowe. Prowadzi w tym celu ewidencję podmiotów, którym dane zostały powierzone do przetwarzania.

§12

Udostępnianie danych osobowych

1. Administrator Danych udostępnia dane osobowe przetwarzane w zbiorach danych wyłącznie osobom lub podmiotom uprawnionym do ich otrzymania na podstawie aktualnych przepisów prawa.

2. Dane osobowe mogą być udostępniane na podstawie:
a) wniosku od podmiotu uprawnionego do otrzymywania danych osobowych na podstawie przepisów prawa, w szczególności sąd, prokuratura, policja

b) wniosku innej osoby lub podmiotu, na zasadach określonych w przepisach prawa;

3. Wszystkie osoby upoważnione, które otrzymają wniosek o udostepnienie danych, zobowiązane są do przekazywania go bezpośrednio do Administratora Danych Osobowych, który podejmuje decyzję o udostępnieniu lub odmowie udostępnienia.

§13

Rejestr czynności przetwarzania i kategorii przetwarzania

1. Administrator Danych Osobowych każdorazowo weryfikuje podstawę prawną , cel oraz zakres tworzenia nowego zbioru danych, a następnie ustala, czy przetwarzanie danych jest legalne.

2. Od dnia 25 maja 2018 r. Administrator Danych Osobowych prowadzi rejestr czynności przetwarzania, w którym odnotuje następujące informacje:

a) nazwę oraz dane kontaktowe administratora danych, a także jeśli będzie miało to zastosowanie - inspektora ochrony danych;
b) cele przetwarzania;
c) opis kategorii osób, których dane dotyczą , oraz kategorii danych osobowych;
d) kategorie odbiorców, którym dane zostały lub zostaną ujawnione, w tym w państwach trzecich i organizacji międzynarodowych (jeśli tak, to poda także nazwę państwa lub organizacji);
e) jeśli to możliwe, planowane terminy usunięcia poszczególnych kategorii danych;
f) jeśli to możliwe, ogólny opis środków technicznych i organizacyjnych.

3. Od dnia 25 maja 2018 r. Administrator Danych Osobowych będą jednocześnie podmiotem przetwarzającym prowadzi rejestr kategorii przetwarzania, w którym odnotuje następujące informacje:

a) nazwę oraz dane kontaktowe podmiotu przetwarzającego, a także jeśli będzie miało to zastosowanie - inspektora ochrony danych;

b) kategorie przetwarzania;

c)nazwa i dane kontaktowe administratora,

d) nazwa i dane kontaktowe współadministratora i/lub przedstawiciela (jeśli dotyczy)

e) dane kontaktowe inspektora ochrony danych osobowych

f) nazwy państw trzecich lub organizacji międzynarodowych, do których dane są przekazywane

g) dokumentacja odpowiednich zabezpieczeń danych osobowych przekazywanych,

h) jeśli to możliwe, ogólny opis środków technicznych i organizacyjnych.

§ 14

Środki organizacyjne i techniczne niezbędne do zapewnienia poufności, integralności i rozliczności w systemach informatycznych

1. **Urząd Gminy w Gorzycach** zapewnia, że przeprowadził identyfikację ryzyka, szacowania skutków i prawdopodobieństwa wystąpienia ryzyka w obszarze ochrony danych osobowych pod kątem poufności, integralności i rozliczności przetwarzanych danych.

2. Wdrożone środki organizacyjne i techniczne w są adekwatne względem kategorii danych, których dotyczą. Stanowią zabezpieczenie danych przed ich udostepnieniem osobom nieupoważnionym, zabraniem przez osobę nieuprawnioną , przetwarzaniem z naruszeniem przepisów, zmianą , utratą , uszkodzeniem lub zniszczeniem.

§ 15
Odpowiedzialność osób przetwarzających dane osobowe

1. Wszyscy pracownicy i współpracownicy **Urzędu Gminy w Gorzycach** są zobowiązani do przestrzegania zasad, instrukcji i procedur wprowadzonej dokumentacji przetwarzania danych osobowych.

2. Nieprzestrzeganie zasad ochrony danych osobowych może skutkować odpowiedzialnością każdej osoby, która dopuściła się naruszenia, na zasadach określonych w przepisach, a w szczególności, gdy:
a) przetwarza w zbiorze danych dane osobowe do których przetwarzania nie została upoważniona, których przetwarzanie jest zabronione lub niezgodne z celem zebrania danych;

b) udostępnia lub umożliwia dostęp do danych osobowych osobom nieupoważnionym;

c) uniemożliwia osobie, której dane dotyczą , korzystanie z przysługujących jej praw.

WÓJT
mgr Leszek Surdy

06.12.2018 .....

(data i podpis Administratora Danych Osobowych)

Załącznik nr 1 – wzór opoważnienia

Upoważnienie do przetwarzania danych osobowych

Numer ewidencyjny:

Osoba upoważniona	
Zbiór, do którego osoba jest upoważniona	
Zakres upoważnienia	
Identyfikatory w systemach	
Data nadania upoważnienia	
Data ustania upoważnienia	do odwołania

Data .....

podpis Administratora Danych .....

Oświadczenie o poufności

Oświadczam, iż zapoznano mnie z przepisami dotyczącymi ochrony danych osobowych, w szczególności ogólnego Rozporządzenia o ochronie danych UE z dnia 27 kwietnia 2016 r. oraz odnośnymi wymaganiami "Regulaminu Ochrony Danych Osobowych".

W szczególności zobowiązuję się do:
- przetwarzania danych osobowych wyłącznie w zakresie i celu przewidzianym w powierzonych przez Administratora zadaniach
- zachowania w tajemnicy danych osobowych do których mam lub będę mieć dostęp w związku z wykonywaniem zadań powierzonych przez Administratora
- niewykorzystywania danych osobowych w celach niezgodnych z zakresem i celem powierzonych zadań przez Administratora
- zachowania w tajemnicy sposobów zabezpieczenia danych osobowych

ochrony danych osobowych przed przypadkowym lub niezgodnym z prawem zniszczeniem, utratą, modyfikacją danych osobowych, nieuprawnionym ujawnieniem danych osobowych, nieuprawnionym dostępem do danych osobowych oraz przetwarzaniem.

Przyjmuję do wiadomości, iż postępowanie sprzeczne z powyższymi zobowiązaniami może być uznane przez Administratora za naruszenie przepisów Rozporządzenia o ochronie danych UE z dnia 27 kwietnia 2016 r.

Data.....

Podpis pracownika/zleceniobiorcy .....

Wzór

Ewidencja osób przetwarzających dane w podmiocie posiadających upoważnienie

załącznik nr 3 do „Polityki Bezpieczeństwa"

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

.....

Podpis Administratora Danych

Wzór

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

załącznik do „Polityki Bezpieczeństwa" nr 4

Lp.	Dokładny adres *(np. adres siedziby firmy gdzie przetwarzane są dane)*	Dział użytkujący pomieszczenie	Nr pokoju lub pomieszczenia	Rodzaj zastosowanego zabezpieczenia pomieszczenia	Uwagi
1.					

.....

podpis Administratora Danych