

## ZARZĄDZENIE NR 6.2016

**Wójta Gminy Rogowo**

**z dnia 1 lutego 2016 r.**

### **w sprawie: wprowadzenia Polityki Bezpieczeństwa Przetwarzania Danych Osobowych w Urzędzie Gminy w Rogowie oraz przyjęcia instrukcji zarządzania systemem informatycznym.**

Na podstawie: art. 36 ustawy z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (T.j. Dz. U. z 2015 poz. 2135 ze zm.) oraz § 3 ust. 3, § 4, § 5 rozporządzenia Ministra Spraw Wewnętrznych i Administracji z dnia 29 kwietnia 2004 roku 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) oraz art. 33 ust.3 ustawy z dnia 8 marca 1990 o samorządzie gminnym (T. j. Dz. U. z 2015 r. poz. 1515 ze zm.) zarządza się, co następuje:

#### **§ 1**

1. Wprowadza się „Politykę Bezpieczeństwa Przetwarzania Danych Osobowych w Urzędzie Gminy w Rogowie” zwaną dalej „Polityką Bezpieczeństwa”, która stanowi załącznik 1 do niniejszego zarządzenia.

2. Wprowadza się „Instrukcję Zarządzania Systemem Informatycznym”, zwaną dalej „Instrukcją”, która stanowi załącznik 2 do niniejszego zarządzenia.

#### **§ 2**

Zobowiązuje się pracowników Urzędu Gminy w Rogowie do stosowania zasad określonych w „Polityce” i „Instrukcji”

#### **§ 3**

Traci moc zarządzenie nr 12/2011 Wójta Gminy Rogowo z dnia 05 kwietnia 2011 roku w sprawie ochrony danych osobowych oraz wprowadzenia dokumentacji Polityki Bezpieczeństwa Informacji w Urzędzie Gminy w Rogowie.

#### **§ 4**

Zarządzenie wchodzi w życie z dniem podpisania.

Rogowo, dnia 01.02.2016 roku

**WÓJTA**  
*mgr Barbara Nowakowska*

.....



Załącznik Nr 1 do Zarządzenia Wójta Gminy Rogowo Nr 6.2016 z dnia 01.02.2016 r.

**POLITYKA BEZPIECZEŃSTWA  
PRZETWARZANIA DANYCH OSOBOWYCH  
W URZĘDZIE GMINY W ROGOWIE**



## POSTANOWIENIA OGÓLNE

§ 1. **Polityka Bezpieczeństwa** została opracowana w związku z wymaganiami zawartymi w ustawie z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (T.J. Dz. U. z 2015 r. poz. 2135 ze zm.) oraz rozporządzeniu 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 ). Dokument został opracowany zgodnie z dyrektywą 2002/58/WE Parlamentu Europejskiego i Rady z dnia 12 lipca 2002 r. w sprawie przetwarzania danych osób oraz ochrony prywatności w sektorze komunikacji elektronicznej.

§ 2. Polityka określa tryb i zasady ochrony danych osobowych przetwarzanych w Urzędzie Gminy w Rogowie.

§ 3. Ilekroć w Polityce jest mowa o :

- 1) **jednostka** – rozumie się przez to Urząd Gminy w Rogowie;
- 2) **zbiore danych osobowych** - rozumie się przez to każdy posiadający strukturę zestaw danych o charakterze osobowym, dostępnych według określonych kryteriów, niezależnie od tego, czy zestaw ten jest rozproszony lub podzielony funkcjonalnie;
- 3) **danych osobowych** - rozumie się przez to wszelkie informacje dotyczące zidentyfikowanej lub możliwej do zidentyfikowania osoby fizycznej;
- 4) **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;
- 5) **systemie informatycznym** - rozumie się przez to zespół współpracujących ze sobą urządzeń, programów, procedur przetwarzania informacji i narzędzi programowych zastosowanych w celu przetwarzania danych osobowych;

- 6) **systemie tradycyjnym** - rozumie się przez to zespół procedur organizacyjnych, związanych z mechanicznym przetwarzaniem informacji, wyposażenia i środków trwałych w celu przetwarzania danych osobowych na papierze;
- 7) **zabezpieczeniu danych w systemie informatycznym** - rozumie się przez to wdrożenie i eksploatację stosownych środków technicznych i organizacyjnych zapewniających ochronę danych przed ich nieuprawnionym przetwarzaniem;
- 8) **usuwaniu danych** - rozumie się przez to zniszczenie danych osobowych lub taką ich modyfikację, która nie pozwoli na ustalenie tożsamości osoby, której dane dotyczą;
- 9) **Administratorze Danych Osobowych** zwanym też **Administratorem Danych (ADO)** - w świetle art. 3 i 7 pkt 4 ustawy o ochronie danych osobowych rozumie się przez to Wójta Gminy Rogowo, który decyduje o celach i środkach przetwarzania danych osobowych;
- 10) **Administratorze Bezpieczeństwa Informacji** zwanym też **Administratorem Bezpieczeństwa (ABI)**- rozumie się przez to osobę wyznaczoną przez Wójta Gminy Rogowo, nadzorującą przestrzeganie zasad ochrony danych osobowych, w szczególności zabezpieczenia danych przed ich udostępnieniem osobom nieupoważnionym, zabraniam przez osobę nieuprawnioną, przetwarzaniem z naruszeniem ustawy oraz zmianą, utratą, uszkodzeniem lub zniszczeniem;
- 11) **Administratorze Systemu Informatycznego** zwanym też **Administratorem Systemu (ASI)** - rozumie się przez to osobę zatrudnioną przez Wójta Gminy Rogowo, upoważnioną do realizacji zadań związanych z zarządzaniem systemem informatycznym;
- 12) **kierownik referatu** – rozumie się również samodzielne stanowisko pracy,
- 13) **użytkownika systemu** zwanym też **użytkownikiem systemu informatycznego** - rozumie się przez to upoważnionego przez Wójta Gminy Rogowo wyznaczonego do przetwarzania danych osobowych w systemie informatycznym pracownika, który odbył szkolenie prowadzone przez ABI w zakresie ochrony tych danych;
- 14) **zgódzie osoby, której te dane dotyczą** - rozumie się przez to oświadczenie woli, którego treścią jest zgoda na przetwarzanie danych osobowych tego, kto składa

oświadczenie - zgoda nie może być domniemana lub dorozumiana z oświadczenia woli o innej treści.

## Rozdział I

### CELE

§ 4.1. Dane osobowe w Urzędzie Gminy w Rogowie są gromadzone, przechowywane, edytowane, archiwizowane w kartotekach, skorowidzach, księgach, wykazach, zestawieniach oraz w innych zestawach i zbiorach ewidencyjnych poszczególnych referatów i samodzielnych stanowisk pracy Urzędu Gminy w Rogowie na dokumentach papierowych, jak również w systemach informatycznych na elektronicznych nośnikach informacji.

2. Wykaz budynków, pomieszczeń lub części pomieszczeń, tworzących obszar, w którym przetwarzane są dane osobowe określa **załącznik do Polityki Bezpieczeństwa nr 1**.

§ 5. Polityka Bezpieczeństwa wprowadza regulacje w zakresie zasad organizacji procesu przetwarzania danych osobowych i odnosi się swoją treścią do informacji:

- 1) w formie papierowej - przetwarzanej w ramach systemu tradycyjnego;
- 2) w formie elektronicznej - przetwarzanej w ramach systemu informatycznego.

§ 6. Celem opracowania Polityki Bezpieczeństwa jest ochrona danych osobowych przed niepożądanym dostępem do zgromadzonych i przetwarzanych danych.

§ 7. Procedury i zasady określone w niniejszej Polityce Bezpieczeństwa stosuje się do wszystkich pracowników Urzędu Gminy w Rogowie, jak i innych osób mających dostęp do danych osobowych przetwarzanych w Urzędzie Gminy w Rogowie łącznie z osobami realizującymi zadania na podstawie umów zlecenia lub o dzieło, wolontariuszy, stażystów, praktykantów, serwisantów i innych mających dostęp do danych osobowych.

§ 8.1. Przetwarzanie danych osobowych do celów związanych z działalnością Administratora Danych jest zgodne z prawem w sytuacji, gdy dane te zostały uzyskane od osoby, której dotyczą i wyraziła ona na ich przetwarzanie zgodę.

2. W sytuacji, gdy dane osobowe nie zostały uzyskane od osoby, której dotyczą, to ich przetwarzanie jest zgodne z prawem, gdy przepis szczególny tak stanowi.

3. Usunięcie danych nie wymaga zgody osoby, której dotyczą.

4. Ocena niezbędności przetwarzania danych do wypełnienia usprawiedliwionych celów Administratora Danych powinna być dokonywana indywidualnie w każdej sytuacji.

§ 9.1. W przypadku zbierania danych osobowych od osoby, której one dotyczą, w wypadkach przewidzianych ustawą należy poinformować tę osobę o:

- 1) adresie swojej siedziby i pełnej nazwie,
- 2) celu zbierania danych, a w szczególności o znanych w czasie udzielania informacji lub przewidywanych odbiorcach lub kategoriach odbiorców danych,
- 3) prawie dostępu do treści swoich danych oraz ich poprawiania,
- 4) dobrowolności albo obowiązku podania danych, a jeżeli taki obowiązek istnieje, o jego podstawie prawnej.

2. Powyższy obowiązek Administrator Danych nakłada na osoby zatrudnione przy przetwarzaniu danych osobowych.

§ 10.1. W przypadku zbierania danych osobowych nie od osoby, której one dotyczą, Administrator Danych jest obowiązany poinformować tę osobę, bezpośrednio po utrwaleniu zebranych danych, o:

- 1) adresie swojej siedziby i pełnej nazwie,
- 2) celu i zakresie zbierania danych, a w szczególności o odbiorcach lub kategoriach odbiorców danych,
- 3) źródle danych,
- 4) prawie dostępu do treści swoich danych oraz ich poprawiania,
- 5) prawie wniesienia pisemnego, umotywowanego żądania zaprzestania przetwarzania jej danych ze względu na jej szczególną sytuację, jeżeli nawet przetwarzanie jest niezbędne

do wypełnienia usprawiedliwionych celów administratora danych, a przetwarzanie danych nie narusza praw i wolności osoby, której dane dotyczą,

- 6) prawie wniesienia sprzeciwu wobec przetwarzania jej danych w przypadkach, gdy przetwarzanie jest niezbędne do wypełnienia usprawiedliwionych celów administratora danych, a przetwarzanie danych nie narusza praw i wolności osoby, której dane dotyczą, gdy administrator danych zamierza je przetwarzać w celach marketingowych lub wobec przekazywania jej danych osobowych innemu administratorowi danych.

2. Powyższy obowiązek Administrator Danych nakłada na osoby zatrudnione przy przetwarzaniu danych osobowych.

§ 11. Bezpośredni nadzór nad przetwarzaniem danych osobowych sprawują Kierownicy Referatów.

§ 12.1. Z zasadami w Polityce Bezpieczeństwa obowiązkowo są zapoznawani wszyscy użytkownicy systemów tradycyjnych i informatycznych, składając odpowiednie oświadczenie, którego wzór stanowi załącznik Nr 2 do Polityki.

2. Oświadczenie przechowywane jest w aktach osobowych pracownika a drugi egzemplarz w dokumentacji ABI.

§ 13.1. Do informacji przechowywanych w systemach tradycyjnych jak i informatycznych mają dostęp jedynie upoważnieni pracownicy Urzędu Gminy w Rogowie oraz osoby mające imienne zarejestrowane upoważnienie, którego wzór stanowi załącznik Nr 3 do niniejszej Polityki. Wszyscy pracownicy zobowiązani są do zachowania tych danych w tajemnicy. Dopuszczalny sposób i zakres przetwarzania danych osobowych regulują zapisy ustaw kompetencyjnych, właściwych dla poszczególnych referatów i samodzielnych stanowisk pracy Urzędu Gminy w Rogowie;

2. Upoważnienie określone w ust. 1 przechowywane jest w aktach osobowych pracownika a drugi egzemplarz w dokumentacji ABI;

2. Ewidencję osób uprawnionych do przetwarzania danych osobowych prowadzi Administrator Bezpieczeństwa Informacji;

3. Wzór ewidencji określonej w ust. 2 stanowi **załącznik Nr 4** do Polityki Bezpieczeństwa.

§ 14.1. Dane osobowe są chronione zgodnie z polskim prawem oraz procedurami obowiązującymi w jednostce dotyczącymi bezpieczeństwa i poufności przetwarzanych danych.

2. Systemy informatyczne oraz tradycyjne, które przechowują dane osobowe, są chronione odpowiednimi środkami technicznymi.

## Rozdział II

### ADMINISTRACJA I ORGANIZACJA BEZPIECZEŃSTWA

§ 15.1. Za bezpieczeństwo danych osobowych przetwarzanych w systemach przetwarzania danych osobowych odpowiada Administrator Danych Osobowych (ADO).

2. Kierownicy referatów obowiązani są zastosować środki techniczne i organizacyjne zapewniające ochronę przetwarzanych danych osobowych odpowiednie do zagrożeń oraz kategorii danych objętych ochroną, a w szczególności powinni zabezpieczyć dane przed ich udostępnieniem osobom nieupoważnionym, zabraniem przez osobę nieuprawnioną, przetwarzaniem z naruszeniem ustawy oraz zmianą, utratą, uszkodzeniem lub zniszczeniem.

§ 16. Administrator Danych wyznacza Administratora Bezpieczeństwa Informacji w celu nadzorowania i przestrzegania zasad ochrony, o której mowa w USTAWIE z dnia 29 sierpnia 1997 roku o ochronie danych osobowych. Prowadzi on dokumentację opisującą sposób przetwarzania danych oraz środków technicznych i organizacyjnych zapewniających ochronę przetwarzanych danych osobowych.

§ 17.1. Administrator Bezpieczeństwa Informacji wykonuje wszystkie prace niezbędne do efektywnego oraz bezpiecznego zarządzania systemami informatycznymi i tradycyjnymi.

2. Administrator Bezpieczeństwa Informacji jest zobowiązany do zapewnienia, poprzez zastosowanie odpowiednich środków i metod kontroli dostępu, tak by wyłącznie uprawniony użytkownik miał dostęp do systemów informatycznych i tradycyjnych.

3. Administrator Bezpieczeństwa Informacji posiada bieżącą listę osób upoważnionych do przetwarzania danych osobowych.

4. Szczegółowy zakres odpowiedzialności i obowiązków Administratora Bezpieczeństwa Informacji jest następujący:

- 1) zapewnianie przestrzegania przepisów o ochronie danych osobowych, w szczególności przez:
  - a) sprawdzanie zgodności przetwarzania danych osobowych z przepisami o ochronie danych osobowych oraz opracowanie w tym zakresie sprawozdania dla administratora danych,
  - b) nadzorowanie opracowania i aktualizowania dokumentacji, o której mowa w art. 36 ust. 1 i 2, oraz przestrzegania zasad w niej określonych,
  - c) zapewnianie zapoznania osób upoważnionych do przetwarzania danych osobowych z przepisami o ochronie danych osobowych,
- 2) prowadzenie rejestru zbiorów danych przetwarzanych przez administratora danych, z wyjątkiem zbiorów, o których mowa w art. 43 ust. 1, zawierającego nazwę zbioru oraz informacje, o których mowa w art. 41 ust. 1 pkt 2-4a i 7.
- 3) nadzoruje bezpieczeństwo systemów informatycznych i tradycyjnych;
- 4) nadzoruje przestrzeganie przez wszystkich użytkowników stosowanie obowiązujących procedur;
- 5) weryfikuje listę autoryzowanych użytkowników systemów informatycznych;
- 6) doradza użytkownikom w zakresie bezpieczeństwa;
- 7) dba, aby użytkownicy mający dostęp do systemu posiadali stosowne upoważnienia oraz byli przeszkoleni w zakresie obowiązujących regulacji bezpieczeństwa;
- 8) prowadzi kontrolę w zakresie bezpieczeństwa;
- 9) prowadzi postępowanie wyjaśniające w przypadku naruszenia ochrony danych osobowych (załącznik nr 5),
- 10) przygotowuje wnioski pokontrolne dla Administratora Danych Osobowych,

- 11) prowadzi rejestr zbiorów danych osobowych przetwarzanych przez administratora danych.

§ 18.1. Administrator Danych Osobowych wyznacza Administratora Systemu Informatycznego (ASI), który posiada najwyższe uprawnienia w systemie informatycznym. Tylko ASI jest osobą uprawnioną do instalowania i usuwania oprogramowania systemowego i narzędziowego.

2. Administrator Systemu Informatycznego wykonuje wszystkie prace niezbędne do efektywnego oraz bezpiecznego zarządzania systemem informatycznym. Jest zobowiązany do zapewnienia, poprzez zastosowanie odpowiednich środków i metod kontroli dostępu, w taki sposób, że wyłącznie uprawniony użytkownik ma dostęp do systemów informatycznych.

3. Szczegółowy zakres odpowiedzialności i obowiązków Administratora Systemu Informatycznego jest następujący:

- 1) zapewnia stałą sprawność urządzeń mających wpływ na bezpieczeństwo danych;
- 2) odpowiada za bezpieczeństwo systemu informatycznego;
- 3) zobowiązuje i bieżąco kontroluje stosowanie się użytkowników do obowiązujących procedur;
- 4) utrzymuje i aktualizuje listę autoryzowanych użytkowników systemu informatycznego;
- 5) zapewnia aktualizację dokumentacji technicznej systemu w tym opis struktur zbiorów i ich zależności;
- 6) prowadzi nadzór nad naprawami, konserwacją oraz likwidacją urządzeń komputerowych, na których zapisywane są dane osobowe;
- 7) wykonuje kopie awaryjne/archiwalne /oraz nadzoruje ich przechowywanie;
- 8) wprowadza i nadzoruje mechanizmy autoryzacji.

§ 19. Kierownik referatu odpowiada za przestrzeganie ustawy o ochronie danych oraz przepisów wewnętrznych na poszczególnych stanowiskach, a w szczególności:

- 1) kontroluje sposób zabezpieczenia zbiorów danych osobowych przez pracowników,
- 2) kontroluje sposób realizacji obowiązku udzielania informacji o jakich mowa w ustawie,

- 3) zgłasza ABI planowaną rejestrację nowych zbiorów oraz przygotowuje wniosek w tej sprawie (załącznik nr 6) ,
- 4) wnioskuje o nadanie upoważnień do przetwarzania danych osobowych pracownikom,
- 5) zgłasza potrzeby w zakresie zabezpieczenia danych osobowych w Urzędzie Gminy w Rogowie.

§ 20. Użytkownik systemu wykonuje wszystkie prace niezbędne do efektywnej oraz bezpiecznej pracy na stanowisku pracy również z wykorzystaniem stacji roboczej. Jest odpowiedzialny przed Administratorem Bezpieczeństwa Informacji za realizację i utrzymanie niezbędnych warunków bezpieczeństwa, w szczególności do przestrzegania procedur dostępu do systemu i ochrony danych osobowych.

### Rozdział III

#### WYKAZ ZBIORÓW DANYCH OSOBOWYCH WRAZ ZE WSKAZANIEM PROGRAMÓW ZASTOSOWANYCH DO PRZETWARZANIA TYCH DANYCH

§ 21.1. Dane osobowe są gromadzone, przechowywane i przetwarzane w kartotekach, skorowidzach, księgach, wykazach oraz w innych zbiorach ewidencyjnych poszczególnych referatów i samodzielnych stanowisk pracy Urzędu Gminy w Rogowie, w postaci dokumentów papierowych i w systemie informatycznym, w którym stosowane są pakiety biurowe lub wyspecjalizowane aplikacje (programy).

2. Zestawienie zbiorów danych osobowych oraz programów do przetwarzania tych danych stanowi załącznik Nr 7 do Polityki Bezpieczeństwa.

§ 22. Ze względu na rodzaj i charakter danych osobowych zawartych w zbiorach, w Urzędzie Gminy w Rogowie wyróżnia się dwie kategorie danych:

- 1) **dane osobowe zwykłe** - wszelkie dane (informacje) dotyczące zidentyfikowanej lub możliwej do zidentyfikowania osoby fizycznej, zgromadzone w zbiorach danych osobowych.

- 2) **dane osobowe szczególnie chronione** – zgodnie z art.27 ust.1 ustawy o ochronie danych osobowych (art. 27 ust. 1) wszelkie dane (informacje) ujawniające pochodzenie rasowe lub etniczne, poglądy polityczne, przekonania religijne, przynależność partyjną lub związkową, jak również informacje o stanie zdrowia, kodzie genetycznym, nałogach lub życiu seksualnym oraz dane dotyczące skazania osoby, orzeczeń o ukaraniu i mandatów karnych, a także innych orzeczeń wydanych w postępowaniu sądowym lub administracyjnym.

§ 23. Zgodnie z postanowieniami art. 40 ustawy o ochronie danych osobowych, z uwagi na gromadzone kategorie zbiorów danych osobowych istnieje obowiązek zgłoszenia do rejestracji tych zbiorów Generalnemu Inspektorowi Ochrony Danych Osobowych z wyjątkiem przypadków, o których mowa w art. 43 ust. 1i 1a tejże ustawy.

## Rozdział V

### SPOSÓB PRZEPLYWU DANYCH POMIĘDZY POSZCZEGÓLNYMI SYSTEMAMI

§ 24.1. Obieg dokumentów zawierających dane osobowe, pomiędzy referatami i samodzielnymi stanowiskami pracy Urzędu Gminy w Rogowie, winien się odbywać w sposób zapewniający pełną ochronę przed ujawnieniem zawartych w tych dokumentach danych (informacji).

2. Przekazywanie informacji (danych) w systemie informatycznym poza sieć lokalną jednostki odbywa się w relacji jednostka organizacyjna - mieszkańcy, przedsiębiorcy, kontrahenci, zakład ubezpieczeń społecznych, urząd skarbowy, banki, Narodowy Fundusz Ochrony Zdrowia, urząd wojewódzki, urząd marszałkowski inne jednostki administracji samorządowej i rządowej.

3. Zabronione jest jednoczesne podłączanie komputerów do sieci wewnętrznej Urzędu Gminy w Rogowie i sieci zewnętrznych (publicznych).

§ 25. Opis struktury zbiorów danych wskazujących zawartość poszczególnych pól informacyjnych i powiązania między nimi oraz sposobu przepływu danych pomiędzy poszczególnymi systemami określa załącznik do Polityki Bezpieczeństwa nr 8.

## Rozdział VI

### OKREŚLENIE ŚRODKÓW TECHNICZNYCH I ORGANIZACYJNYCH NIEZBĘDNYCH DLA ZAPEWNIENIA POUFNOŚCI, INTEGRALNOŚCI I ROZLICZALNOŚCI PRZETWARZANYCH DANYCH

§ 26.1. Dostęp do danych wprowadzonych przez użytkowników systemów informatycznych mają jedynie upoważnione osoby oraz Administrator Systemu Informatycznego zapewniający jego prawidłową eksploatację.

2. Pomieszczenia, w których przetwarza się dane osobowe powinny być fizycznie zabezpieczone przed dostępem osób nieuprawnionych, to znaczy posiadać odpowiednie zamki do drzwi, zabezpieczenia w oknach (w szczególności na parterze) oraz być wyposażone w środki ochrony ppoż.

3. W pomieszczeniach gdzie przebywają osoby postronne, monitory stanowisk dostępu do danych osobowych powinny być ustawione w taki sposób by uniemożliwić tym osobom wgląd w dane osobowe.

4. Dokumenty i nośniki informacji, zawierające dane osobowe powinny być zabezpieczone przed dostępem osób nieupoważnionych do przetwarzania danych. Jeśli nie są aktualnie używane powinny być przechowywane w szafach lub w innych przeznaczonych do tego celu urządzeniach biurowych, posiadających odpowiednie zabezpieczenia w celu zachowania zasady tzw. „czystego biurka”.

## Rozdział VII

### UDOSTĘPNIANIE POSIADANYCH W ZBIORZE DANYCH OSOBOWYCH

§ 27.1. Na wniosek osoby, której dane dotyczą, ADO jest obowiązany, w terminie 30 dni, poinformować o przysługujących jej prawach, a zwłaszcza wskazać w formie zrozumiałej odnośnie danych osobowych jej dotyczących:

- 1) jakie dane osobowe zawiera zbiór,
- 2) w jaki sposób zebrano dane,
- 3) w jakim celu i zakresie dane są przetwarzane,
- 4) w jakim zakresie oraz komu dane zostały udostępnione.

2. Na wniosek osoby, której dane dotyczą, informacji, o których mowa w ust. 1, udziela się na piśmie.

§ 28.1. Każdej osobie przysługuje prawo do kontroli przetwarzania danych, które jej dotyczą, zawartych w zbiorach danych, a zwłaszcza prawo do:

- 1) uzyskania wyczerpującej informacji, czy taki zbiór istnieje, oraz do ustalenia administratora danych, adresu jego siedziby i pełnej nazwy,
- 2) uzyskania informacji o celu, zakresie i sposobie przetwarzania danych zawartych w takim zbiorze,
- 3) uzyskania informacji, od kiedy przetwarza się w zbiorze dane jej dotyczące, oraz podania w powszechnie zrozumiałej formie treści tych danych,
- 4) uzyskania informacji o źródle, z którego pochodzą dane jej dotyczące,
- 5) uzyskania informacji o sposobie udostępniania danych, a w szczególności informacji o odbiorcach lub kategoriach odbiorców, którym dane te są udostępniane,
- 6) żądania uzupełnienia, uaktualnienia, sprostowania danych osobowych, czasowego lub stałego wstrzymania ich przetwarzania lub ich usunięcia, jeżeli są one niekompletne, nieaktualne, nieprawdziwe lub zostały zebrane z naruszeniem ustawy albo są już zbędne do realizacji celu, dla którego zostały zebrane
- 7) prawie wniesienia pisemnego, umotywowanego żądania zaprzestania przetwarzania jej danych ze względu na jej szczególną sytuację, jeżeli nawet przetwarzanie jest niezbędne do wypełnienia usprawiedliwionych celów administratora danych, a przetwarzanie danych nie narusza praw i wolności osoby, której dane dotyczą,

- 8) wniesienia sprzeciwu wobec przetwarzania jej danych w przypadkach, gdy przetwarzanie jest niezbędne do wypełnienia usprawiedliwionych celów administratora danych, a przetwarzanie danych nie narusza praw i wolności osoby, której dane dotyczą, gdy administrator danych zamierza je przetwarzać w celach marketingowych lub wobec przekazywania jej danych osobowych innemu administratorowi danych
- 9) wniesienia do administratora danych żądania ponownego, indywidualnego rozpatrzenia sprawy rozstrzygniętej z naruszeniem zakazu ostatecznego rozstrzygnięcia indywidualnej sprawy, gdy treść była wyłącznie wynikiem operacji na danych osobowych prowadzonych w systemie informatycznym.

2. Osoba zainteresowana może skorzystać z prawa do informacji, o których mowa w ust. 1 pkt 1 - 5, nie częściej niż raz na 6 miesięcy.

§ 29.1. W razie wykazania przez osobę, której dane osobowe dotyczą, że są one niekompletne, nieaktualne, nieprawdziwe lub zostały zebrane z naruszeniem ustawy albo są zbędne do realizacji celu, dla którego zostały zebrane, administrator danych jest obowiązany, bez zbędnej zwłoki, do uzupełnienia, uaktualnienia, sprostowania danych, czasowego lub stałego wstrzymania przetwarzania kwestionowanych danych lub ich usunięcia ze zbioru, chyba że dotyczy to danych osobowych, w odniesieniu do których tryb ich uzupełnienia, uaktualnienia lub sprostowania określają odrębne ustawy.

2. Każda z osób zatrudnionych przy przetwarzaniu danych w razie powzięcia takiej wiadomości ma obowiązek o wystąpieniu osoby, której dane dotyczą, poinformować ABl.

§ 30.1. Do udostępniania posiadanych w zbiorze danych osobowych upoważniony jest Wójt Gminy Rogowo lub pracownik posiadający wymagane prawem upoważnienie.

2 W przypadku udostępniania danych osobowych w celach innych niż wyłączenie do zbioru, administrator danych udostępnia posiadane w zbiorze dane osobom lub podmiotom uprawnionym do ich otrzymania na mocy przepisów prawa.

§ 31.1. Powierzenie przetwarzania danych osobowych innemu podmiotowi może nastąpić wyłącznie w drodze umowy zawartej w formie pisemnej przez ADO z uwzględnieniem wymagań określonych w art.31ust.1 tejże ustawy (załącznik nr 9).

## **Rozdział VIII**

### **ZACHOWANIE BEZPIECZEŃSTWA PRZEZ UŻYTKOWNIKÓW SYSTEMU**

§ 32.1. Użytkownicy systemu zobowiązani są stosować odpowiednie środki bezpieczeństwa w pomieszczeniach, w których zainstalowano sprzęt systemu informatycznego by nie spowodować jego uszkodzenia.

§ 33.1. Wszyscy użytkownicy systemu muszą stosować się do obowiązujących procedur bezpieczeństwa.

2. Hasło podlega szczególnej ochronie. Użytkownik ma obowiązek tworzenia haseł. W przypadku, gdy użytkownik zapomni swoje hasło, może on odnowić hasło w porozumieniu z Administratorem Systemu Informatycznego.

## **Rozdział IX**

### **BEZPIECZEŃSTWO FIZYCZNE**

§ 34.1 Dane osobowe, które są przedmiotem przetwarzania zgodnie z przepisami ustawy o ochronie danych osobowych, gromadzone i przechowywane są w serwerach i w postaci tradycyjnej .

2. Środki bezpieczeństwa fizycznego są konieczne dla zapobiegania niepożądanemu dostępowi do informacji, nieautoryzowanym operacjom w systemie, kontroli dostępu do zasobów oraz w celu zabezpieczenia sprzętu teleinformatycznego.

§ 35.1. Obszar systemów informatycznych w Urzędzie Gminy w Rogowie obejmuje wszystkie pomieszczenia Urzędu Gminy w Rogowie, 87-515 Rogowo 51. Pomieszczenia, w których znajdują się systemy informacji winny być:

- 1) wyposażone w szafy ,meble biurowe zamykane na klucz umożliwiające przechowywanie dokumentów,
- 2) zamknięte, jeśli nikt w nich nie przebywa.

§ 36. Instalacja urządzeń systemu i sieci teleinformatycznej odbywa się za wiedzą i pod kontrolą kierownika referatu, który jest również odpowiedzialny za warunki wprowadzania do użycia, przechowywania, eksploatacji oraz wycofywania z użycia każdego urządzenia.

## Dział X

### BEZPIECZEŃSTWO SPRZĘTU I OPROGRAMOWANIA

§ 37. Sprzęt i oprogramowanie, indywidualnie lub łącznie mają ścisły związek z bezpieczeństwem systemu i sieci teleinformatycznej. Dlatego, powinny być ściśle przestrzegane procedury bezpieczeństwa odnoszące się do tych elementów.

§ 38. Sieć teleinformatyczna jest organizacyjnym i technicznym połączeniem systemów teleinformatycznych wraz z łączącymi je urządzeniami i liniami telekomunikacyjnymi. Niedopuszczalne jest samowolne przemieszczanie lub zmiana konfiguracji stacji roboczej bez wiedzy kierownika referatu.

§ 39. Zabrania się na korzystanie z jakiegokolwiek nowego oprogramowania bez zgody Administratora Systemu Informatycznego.

§ 40.1. Dostęp do zbiorów danych osobowych znajdujących się na serwerach następuje po wprowadzeniu hasła, które znane jest tylko osobie przetwarzającej dane.

2. Każdorazowo po dokonaniu przetworzenia aplikacja powinna być zamknięta.

3. W przypadku podejrzenia, iż wiadomości o sposobie dostępu do elektronicznej bazy danych uzyskała osoba do tego niepowołana, osoba przetwarzająca dane w porozumieniu z ASI powinna dokonać zmiany hasła.

§ 41.1. Elektroniczne bazy danych osobowych są archiwizowane.

2. Kopie są wykonywane na nośnikach magnetycznych, płytach CD/DVD/Blue-ray.

§ 42. Używanie oprogramowania prywatnego w sieci jest zabronione. Na stacjach roboczych powinno być zainstalowane jedynie niezbędne oprogramowanie.

## Rozdział XI

### KONSERWACJE I NAPRAWY

§ 43. Każde urządzenie użytkowane w systemie informatycznym, powinno podlegać rutynowym czynnościom konserwacyjnym oraz przeglądom wykonywanym przez uprawnione osoby.

§ 44.1. Za konserwację oprogramowania systemowego oraz aplikacyjnego serwera systemu informatycznego odpowiedzialny jest Administrator Systemu Informatycznego. Konserwacja oprogramowania obejmuje także jego aktualizację.

2. Za konserwację oprogramowania stanowisk roboczych odpowiedzialny jest kierownik komórki organizacyjnej. Wszelkie aktualizacje oprogramowania powinny być uzgadniane z Administratorem Systemu Informatycznego.

§ 45. Administrator Systemu Informatycznego przed rozpoczęciem naprawy urządzenia przez zewnętrzne firmy sprawdza, czy spełnione są następujące wymagania:

- 1) w przypadku awarii serwera i konieczności oddania sprzętu do serwisu, nośniki magnetyczne zawierające dane osobowe powinny być wymontowane i do czasu naprawy serwera przechowywane w pomieszczeniu biurowym znajdującym się w strefie o ograniczonym dostępie;

- 2) w przypadku uszkodzenia nośnika magnetycznego zawierającego dane osobowe należy komisyjnie dokonać jego zniszczenia.

## **Dział XII**

### **PLANY AWARYJNE I ZAPOBIEGAWCZE**

§ 46. Serwer systemu oraz poszczególne stacje robocze (opcjonalnie) powinny być zabezpieczone urządzeniami podtrzymującymi zasilanie (UPS), co umożliwi funkcjonowanie systemu w przypadku awarii zasilania.

§ 47. W celu zabezpieczenia ciągłości pracy, informacja przechowywana i przetwarzana w systemie podlega codziennej, przyrostowej archiwizacji (opcjonalnie) oraz pełnej archiwizacji przeprowadzanej nie rzadziej niż raz na dwa tygodnie. Kopie archiwalne danych są wykonywane na nośnikach magnetoptycznych, i przechowywane są przez Administratora Systemu Informatycznego. Użycie kopii zapasowych następuje na polecenie Administratora Systemu Informatycznego w przypadku odtwarzania systemu po awarii.

## **Rozdział XIII**

### **POLITYKA ANTYWIRUSOWA**

§ 48. 1. Wszystkie serwery i komputery są sprawdzane przy użyciu oprogramowania do wykrywania i usuwania wirusów komputerowych.

2. W zakresie ochrony antywirusowej wprowadza się następujące zalecenia:

- 1) nie należy używać oprogramowania na stacji roboczej innego niż zaleca Administrator Systemu Informatycznego;
- 2) przed użyciem nośnika danych sprawdzić czy nie jest zainfekowany wirusem komputerowym.

2. W przypadku jakichkolwiek wątpliwości odnośnie zagrożenia wirusowego należy sprawdzić zawartość całego dysku twardego programem antywirusowym. W przypadku dalszych niejasności należy kontaktować się z administratorem sieci lokalnej.

## Rozdział XIV PRZEPISY KOŃCOWE

§ 49. Za naruszenie obowiązków wynikających z niniejszej Polityki Bezpieczeństwa oraz przepisów ustawy o ochronie danych osobowych może być uznane za ciężkie naruszenie obowiązków pracowniczych, podlegające sankcjom dyscyplinarnym oraz sankcjom karnym w szczególności wynikającym z przepisów tejże ustawy.

- **Art.49.1.** *Kto przetwarza dane osobowe, choć ich przetwarzanie nie jest dopuszczalne albo do których nie jest uprawniony , podlega grzywnie, karze ograniczenia wolności albo pozbawienia wolności do lat 2;*

*2. Jeżeli czyn określony w ust. 1 dotyczy danych ujawniających pochodzenie rasowe lub etniczne, poglądy polityczne, przekonania religijne lub filozoficzne, przynależność wyznaniową, partyjną lub związkową, danych o stanie zdrowia, kodzie genetycznym, nałogach lub życiu seksualnym, sprawca podlega grzywnie, karze ograniczenia wolności albo pozbawienia wolności do lat 3.*

- **Art. 51. 1.** *Kto administrując zbiorem danych lub będąc obowiązany do ochrony danych osobowych udostępnia je lub umożliwia dostęp do nich osobom nieupoważnionym, podlega grzywnie, karze ograniczenia wolności albo pozbawienia wolności do lat 2.*

*2. Jeżeli sprawca działa nieumyślnie, podlega grzywnie, karze ograniczenia wolności albo pozbawienia wolności do roku.*

- **Art. 52.** *Kto administrując danymi narusza choćby nieumyślnie obowiązek zabezpieczenia ich przed zabraniem przez osobę nieuprawnioną, uszkodzeniem lub zniszczeniem, podlega grzywnie, karze ograniczenia wolności albo pozbawienia wolności do roku.*

- **Art. 53.** *Kto będąc do tego obowiązany nie zgłasza do rejestracji zbioru danych, podlega grzywnie, karze ograniczenia wolności albo pozbawienia wolności do roku.*
- **Art. 54.** *Kto administrując zbiorem danych nie dopełnia obowiązku poinformowania osoby, której dane dotyczą, o jej prawach lub przekazania tej osobie informacji umożliwiających korzystanie z praw przyznanych jej w niniejszej ustawie, podlega grzywnie, karze ograniczenia wolności albo pozbawienia wolności do roku.*
- **Art. 52.** *Kto administrując danymi narusza choćby nieumyślnie obowiązek zabezpieczenia ich przed zabraniem przez osobę nieuprawnioną, uszkodzeniem lub zniszczeniem, podlega grzywnie, karze ograniczenia wolności albo pozbawienia wolności do roku.*
- **Art. 53.** *Kto będąc do tego obowiązany nie zgłasza do rejestracji zbioru danych, podlega grzywnie, karze ograniczenia wolności albo pozbawienia wolności do roku.*
- **Art. 54.** *Kto administrując zbiorem danych nie dopełnia obowiązku poinformowania osoby, której dane dotyczą, o jej prawach lub przekazania tej osobie informacji umożliwiających korzystanie z praw przyznanych jej w niniejszej ustawie, podlega grzywnie, karze ograniczenia wolności albo pozbawienia wolności do roku.*

§ 50. W sprawach nie uregulowanych w niniejszej Polityce bezpieczeństwa informacji mają zastosowanie przepisy ustawy z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (T.J. Dz. U. z 2015 r. poz. 2135 ze zm.) 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).



Wykaz budynków, pomieszczeń lub części pomieszczeń, tworzących obszar, w którym przetwarzane są dane osobowe załącznik nr 1 do Polityki Bezpieczeństwa, zgodnie z § 4 pkt 1 Rozporządzenia Ministra Spraw Wewnętrznych i Administracji z dnia 29 kwietnia 2004 r.

**1. W budynkach:**

- budynek administracyjny Urzędu Gminy w Rogowie, 87-515 Rogowo 51 (parter 2 pomieszczenia, 6 pomieszczeń na I piętrze, 8 pomieszczeń na II piętrze)

**2. W pomieszczeniach:**

Kondygnacja	Nr pokoju	Dział użytkujący pomieszczenie	Rodzaj zastosowanego zabezpieczenia pomieszczenia	Uwagi
	wszystkie	sprzątaczką	drzwi zamykane na klucze, kraty	Dostęp do pomieszczeń
<b>PIWNICA</b>		Archiwum Urzędu Gminy w Rogowie	drzwi zamykane na klucze, kraty	
<b>PARTER</b>	nr 2	Referat Spraw Obywatelskich	drzwi zamykane na klucze	
	nr 6	Referat Spraw Obywatelskich	drzwi zamykane na klucze	
<b>I PIĘTRO</b>	nr 8	Urząd Stanu Cywilnego	drzwi zamykane na klucze	
	nr 10	Sekretariat	drzwi zamykane na klucze	
	nr 10	Wójt	drzwi zamykane na klucze	
	nr 10	Z-ca Wójta, Sekretarz Gminy	drzwi zamykane na klucze	
	nr 11	Referat Finansowy	drzwi zamykane na klucze, roleta anty włamaniowa, alarm	
	Nr 12	Referat Spraw Obywatelskich	drzwi zamykane na klucze	

Kondygnacja	Nr pokoju	Dział użytkujący pomieszczenie	Rodzaj zastosowanego zabezpieczenia pomieszczenia	Uwagi
II PIĘTRO	nr 13	Referat Finansowy	drzwi zamknięte na klucze	
	nr 14	Referat Finansowy	drzwi zamknięte na klucze	
	nr 15	Referat Finansowy	drzwi zamknięte na klucze	
	nr 16	Referat Ogólny	drzwi zamknięte na klucze	
	nr 17	Referat Ogólny	drzwi zamknięte na klucze	
	nr 18	Referat Spraw Obywatelskich Referat Ogólny	drzwi zamknięte na klucze	
	nr 19	Samodzielne Stanowisko ds. Informatyki	drzwi zamknięte na klucze	
	nr 20	Samodzielne Stanowisko Referat Finansowy	drzwi zamknięte na klucze	

Data i podpis Administratora Danych

**WÓJTA**  
mgr Barbara Nowakowska



Załącznik Nr 2 do Polityki Bezpieczeństwa w Urzędzie Gminy w Rogowie

WZÓR

<b>O Ś W I A D C Z E N I E</b>
--------------------------------

<b>Imię i nazwisko</b>	
<b>Stanowisko służbowe</b>	
<b>Nazwa referatu</b>	

Stwierdzam własnoręcznym podpisem, że zapoznałem/am/ się z „Polityką Bezpieczeństwa w Urzędzie Gminy w Rogowie” oraz Instrukcją zarządzania systemem informatycznym służącym do przetwarzania danych osobowych w Urzędzie Gminy w Rogowie.

Jednocześnie, zgodnie z przepisami ustawy z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (T.J. Dz. U. z 2015 r., poz. 2135 ze zm. ) zobowiązuję się do ochrony przed niepowołanym dostępem, nieuzasadnioną modyfikacją lub zniszczeniem, nielegalnym ujawnieniem lub pozyskaniem, danych osobowych przetwarzanych w Urzędzie Gminy w Rogowie oraz do zachowania ich w tajemnicy w czasie trwania jak i po ustaniu zatrudnienia.

Równocześnie oświadczam, że zostałem(am) poinformowany(a) o odpowiedzialności służbowej i karnej w przypadku naruszenia przepisów.

.....  
(*imię, nazwisko i podpis osoby  
przyjmującej oświadczenie*)

.....  
(*data i podpis składającego  
oświadczenie*)



Upoważnienie do przetwarzania danych osobowych **załącznik nr 3** do Polityki Bezpieczeństwa zgodnie z Art 37 Ustawy o ochronie danych osobowych z dnia 29 sierpnia 1997 r.

..... 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 (Tj. Dz. U. z 2015 r. poz. 2135 ze zm.) 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*







Załącznik nr 5 do Polityki Bezpieczeństwa

W z ó r

**R a p o r t**  
**z naruszenia ochrony danych osobowych**

W .....

1. Data: ..... Godzina: .....  
*(dzień, miesiąc, rok) (00:00)*

2. Osoba powiadamiająca o zaistniałym zdarzeniu:

.....  
*(Imię, nazwisko, stanowisko służbowe, nazwa użytkownika (jeśli występuje) )*

3. Lokalizacja zdarzenia:

.....  
*(np. nr pokoju, nazwa pomieszczenia)*

4. Rodzaj naruszenia bezpieczeństwa oraz okoliczności towarzyszące:

.....  
.....

5. Podjęte działania:

.....  
.....

6. Przyczyny wystąpienia zdarzenia:

.....  
.....

7. Postępowanie wyjaśniające:

.....  
.....

.....  
*/data, podpis Administratora Bezpieczeństwa Informacji/*



**Załącznik nr 6 do Polityki Bezpieczeństwa**

**Nowy wpis / aktualizacja / wykreślenie**

1. **Numer kolejny wpisu lub numer wersji księgi rejestrowej**

.....

2. **Data wpisu, data aktualizacji treści wpisu albo data wykreślenia wpisu**

.....

3. **Nazwa zbioru danych**

.....

4. **Oznaczenie administratora danych i adres jego siedziby lub miejsca zamieszkania oraz numer identyfikacyjny rejestru podmiotów gospodarki, jeżeli został mu nadany**

Nazwa Administratora Danych.....

Adres siedziby Administratora Danych.....

Nr Identyfikacyjny rejestru podmiotów gospodarki.....

5. **Oznaczenie przedstawiciela administratora danych, o którym mowa w art. 31a ustawy i adres jego siedziby lub miejsca zamieszkania – w przypadku wyznaczenia takiego podmiotu;**

Nazwa przedstawiciela Administratora Danych.....

Adres Siedziby przedstawiciela Administratora Danych.....

6. **Oznaczenie podmiotu, któremu powierzono przetwarzanie danych ze zbioru na podstawie art. 31 ustawy, i adres jego siedziby lub miejsca zamieszkania – w przypadku powierzenia przetwarzania danych temu podmiotowi;**

Nazwa podmiotu, któremu powierzono przetwarzanie danych.....

Adres podmiotu, któremu powierzono przetwarzanie danych.....

7. **Podstawa prawna upoważniająca do prowadzenia zbioru danych;**

.....  
.....

8. **Cel przetwarzania danych w zbiorze**

.....

9. **Opis kategorii osób, których dane są przetwarzane w zbiorze;**

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

10. **Zakres danych przetwarzanych w zbiorze**

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

11. **Sposób zbierania danych do zbioru, w szczególności informacja, czy dane do zbioru są zbierane od osób, których dotyczą, czy z innych źródeł niż osoba, której dane dotyczą;**

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

12. **Sposób udostępniania danych ze zbioru, w szczególności informacja, czy dane ze zbioru są udostępniane innym podmiotom niż upoważnione na podstawie przepisów prawa**

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

13. **Oznaczenie odbiorcy danych lub kategorii odbiorców, którym dane mogą być przekazywane;**

.....  
.....

.....  
14. **Informacja dotycząca ewentualnego przekazywania danych do państwa trzeciego**

.....  
.....

15. **Wzmianka o wykreśleniu wpisu**

.....

16. **Uwagi**

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

Kierownik referatu

.....

Administrator Bezpieczeństwa Informacji

.....



Zestawienie zbiorów danych osobowych wraz ze wskazaniem programów zastosowanych do przetwarzania tych danych załącznik nr 7 do Polityki Bezpieczeństwa zgodnie, z § 4 pkt 2 Rozporządzenia Ministra Spraw Wewnętrznych i Administracji z dnia 29 kwietnia 2004 r.

Kondygnacja	Nr pokoju	Nazwa referatu	Stanowisko przetwarzające zbiory danych	Nazwa zbioru danych <i>(np. dane klientów, pracowników itd.)</i>	Programy zastosowane do przetwarzania danych	Uwagi
PIWNICA			Podinspektor ds. świadczeń rodzinnych i alimentów	Archiwum Urzędu Gminy	Ewidencja papierowa	
PARTER	2	Referat Spraw Obywatelskich	Podinspektor ds. świadczeń rodzinnych i alimentów	Świadczenia rodzinne Fundusz alimentacyjny Stypendia i zasiłki szkolne	Sygnity – Świadczenia Rodzinne Płatnik Home Banking Word Ewidencja papierowa	
	2	Referat Spraw Obywatelskich	Młodszy referent ds. świadczeń rodzinnych i stypendiów	Stypendia i zasiłki szkolne Świadczenia rodzinne Karta dużej rodziny	Ewidencja papierowa Sygnity – Świadczenia Rodzinne SIKDR Word Excel	
	6	Referat Spraw Obywatelskich	Młodszy referent	Świadczenia rodzinne	Sygnity – Świadczenia Rodzinne	

Kondygnacja	Nr pokoju	Nazwa referatu	Stanowisko przetwarzające zbiory danych	Nazwa zbioru danych <i>(np. dane Klientów, pracowników itd.)</i>	Programy zastosowane do przetwarzania danych	Uwagi
	14	Referat Finansowy	Referent ds. księgowości budżetowej	Płace i kadry	Płace i kadry Płatnik Budżet	
	15	Referat Finansowy	Skarbnik	Zbiór kontrahentów	Budżet Home Banking	
	15	Referat Finansowy	Z-ca skarbnika	Zbiór kontrahentów	Budżet Home Banking	
	16	Referat Ogólny	Inspektor ds. budownictwa i planowania przestrzennego	Budownictwo Planowanie przestrzenne Ewidencja numerów porządkowych nieruchomości Zbiór dokumentów wynajmu lokali komunalnych	Zbiór danych przestrzennych Word Excel Internetowy menedżer punktów adresowych Ewidencja papierowa	
	16	Referat Ogólny	Inspektor ds. drogownictwa i ochrony środowiska	Zbór dokumentów dotyczących środowiskowych postępowań Zbór dokumentów dotyczących wyrobów zawierających azbest Zbiór dokumentów w sprawie zajęcia pasa drogowego Baza danych systemu gospodarki odpadami CEIDG	QNET – śmieci CEIDG Word Excel Zbiór danych przestrzennych Baza wyrobów zawierających azbest	

Kondygnacja	Nr pokoju	Nazwa referatu	Stanowisko przetwarzające zbiory danych	Nazwa zbioru danych <i>(np. dane klientów, pracowników itd.)</i>	Programy zastosowane do przetwarzania danych	Uwagi
	17	Referat Ogólny	Kierownik referatu ogólnego	Zamówienia publiczne Zbór dokumentów sprzedaży mienia gminnego Gospodarka nieruchomościami Gospodarka wodno – ściekowa	QNET – woda QNET - ścieki Word Ewidencja papierowa	
	17	Referat Ogólny	Młodszy referent	Baza danych systemu gospodarki odpadami Zezwolenia na sprzedaż napojów alkoholowych CEIDG	QNET – śmieci Exel Ewidencja papierowa CEIDG	
	18	Referat Spraw Obywatelskich	Kierownik referatu spraw obywatelskich	Kwalifikacja wojskowa Rejestr skarg i wniosków Rejestr przedpoborowych (kobiet i mężczyzn) Zbiór osób z dostępem do informacji niejawnych Ewidencja ludności Dowody osobiste	Word Ewidencja papierowa	

Kondygnacja	Nr pokoju	Nazwa referatu	Stanowisko przetwarzające zbiory danych	Nazwa zbioru danych (np. dane klientów, pracowników itd.)	Programy zastosowane do przetwarzania danych	Uwagi
	18	Referat Ogólny	Młodszy referent ds. funduszy unijnych, promocji gminy i współpracy z organizacjami pozarządowymi	Rejestr – wycinka drzew	Word Excel Ewidencja papierowa	
	20	Samodzielne Stanowisko	Referent ds. oświaty	System informacji oświatowej Zbiór dokumentów dotyczących dofinansowania kosztów kształcenia młodocianego pracownika Zbiór dokumentów dotyczących organizacji szkół Zbiór uczniów korzystających z różnych programów rządowych i innych form wsparcia Zbiór dokumentów spełniania obowiązków nauki	SIO CIE Word Excel Ewidencja papierowa	
	20	Referat Finansowy	Młodszy referent ds. plac oświatowych	Płace i pochodne nauczycieli Zbór dokumentów rozliczenie dotacji punktów przedszkolnych Zbiór dokumentów rozliczenie refundacji z PUP Zakładowy Fundusz Świadczeń Socjalnych nauczycieli	Płace i kadry Płatnik Home Banking Word Excel Ewidencja papierowa	

Data i podpis Administratora Danych **WÓJT**

  
mgr Andrzej Kłosowski

Opis struktury zbiorów danych wskazujący zawartość poszczególnych pól informacyjnych i powiązania między nimi oraz sposób przepływu danych pomiędzy poszczególnymi systemami - załącznik nr 8 do Polityki Bezpieczeństwa, 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	Uwagi
1.	Archiwum Urzędu Gminy	Dokumentacja wytwarzana w urzędzie , przechowywana według kategorii archiwalnej	Bez przepływu danych	
2.	Świadczenia rodzinne	Nazwiska i imiona, imiona rodziców, data urodzenia, miejsce urodzenia, adres zamieszkania lub pobytu, PESEL, miejsce pracy, seria i numer dowodu osobistego, nr telefonu, stan zdrowia, nr rachunku bankowego, sytuacja rodzinna i finansowa	Świadczenia rodzinne⇒Płatnik⇒Home banking	
3.	Fundusz alimentacyjny	Nazwiska i imiona, imiona rodziców, data urodzenia, miejsce urodzenia, adres zamieszkania lub pobytu, PESEL, miejsce pracy, zawód, wykształcenie, seria i numer dowodu osobistego, nr telefonu, stan zdrowia, nr rachunku bankowego, informacje na temat skazań, oświadczenie majątkowe dłużnika, sytuacja zdrowotna, nr prawa jazdy, stan cywilny, stan rodzinny	Bez przepływu danych	
4.	Stypendia i zasiłki szkolne	Imiona i nazwisko, adres, wysokość dochodów, imiona rodziców, data urodzenia, miejsce urodzenia, PESEL, miejsce pracy, zawód, seria i numer dowodu osobistego, nr telefonu, sytuacja rodzinna, stan cywilny, informacje na temat dochodów, informacje o miejscu nauki, informacje o nałogach, stanie zdrowia	Bez przepływu danych	
5.	Karta dużej rodziny	Nazwiska i imiona, data urodzenia, PESEL, nr dowodu osobistego, miejsce zamieszkania, adres do korespondencji, nr telefonu, sytuacja rodzinna i zdrowotna	Bez przepływu danych	

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	Uwagi
6.	Urząd Stanu Cywilnego	PESEL, imiona i nazwiska, imiona i nazwiska rodziców, nazwiska rodowe rodziców, data i miejsce urodzenia, adres korespondencyjny, wykształcenie, nr seria dowodu osobistego, godzina urodzenia, data i numer aktu zgonu, godzina zgonu, data i miejsce znalezienia zwłok, godzina znalezienia zwłok, data i numer aktu małżeństwa, data i numer aktu urodzenia, imię i nazwisko oraz nazwisko rodowe współmałżonka, płeć, stan cywilny data i miejsce zawarcia związku małżeńskiego, obywatelstwo, informacje o rozwodzie, separacji, zmianie nazwiska, przysposobieniu, informacje o ustaleniu ojcostwa, zaprzeczeniu ojcostwa, kod terytorialny	Bez przepływu danych	
7.	Zakładowy Fundusz Świadczeń Socialnych	Imię i nazwisko wnioskodawcy, sytuacja rodzinna, zdrowotna i finansowa, stanowisko, nr telefonu, seria i numer dowodu osobistego	Bez przepływu danych	
8.	Ewidencja Ludności	PESEL, imiona i nazwisko, nazwisko rodowe, imiona rodziców, nazwisko rodowe matki i ojca, adres do korespondencji, adres zameldowania, dane dotyczące urodzenia, stanu cywilnego, zgonu, dane dotyczące wyjazdu za granicę, seria i numer dowodu osobistego, obywatelstwo, kod terytorialny	ŹRÓDŁO⇒KSN⇒Elud+	
9.	Dowody osobiste	PESEL, imiona i nazwisko, nazwisko rodowe, imiona rodziców, nazwisko rodowe matki, adres do korespondencji, wizerunek twarzy, kod terytorialny	Bez przepływu danych	
10.	Dziennik korespondencyjny	Imię i nazwisko, adres	Bez przepływu danych	
11.	Wykaz softysów	Imiona i nazwisko, adres, numer telefonu	Bez przepływu danych	
12.	Wykaz radnych	Imiona i nazwisko, adres, data urodzenia, PESEL, nr telefonu, wykształcenie	Bez przepływu danych	

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	Uwagi
13.	Akta osobowe pracowników	Imiona i nazwisko, nazwisko rodowe, data i miejsce urodzenia, imiona rodziców, nazwisko rodowe matki PESEL, NIP, stopień wojskowy i nr książeczki wojskowej, miejsce zamieszkania lub zameldowania, adres do korespondencji, nr telefonu, wykształcenie i dodatkowe uprawnienia, nr i seria dowodu osobistego, dane dotyczące niepełnosprawności, zajmowane stanowisko, orzeczenie lekarskie o dopuszczeniu (lub nie) do pracy na danym stanowisku, nr konta bankowego	Bez przepływu danych	
14.	Oświadczenia majątkowe pracowników i radnych	Imiona i nazwiska, nazwisko rodowe, data i miejsce urodzenia, stanowisko, sytuacja finansowa	Bez przepływu danych	
15.	Zbiór dokumentów dotyczących osób startujących w naborze na stanowiska	Imiona i nazwisko, data i miejsce urodzenia, imiona rodziców, PESEL, miejsce zamieszkania lub zameldowania, adres do korespondencji, nr telefonu, wykształcenie i dodatkowe uprawnienia, nr i seria dowodu osobistego, dane dotyczące niepełnosprawności	Bez przepływu danych	
16.	Księgowość podatkowa	Imiona i nazwiska, adres zamieszkania, imiona rodziców powierzchnia nieruchomości	Bez przepływu danych	
17.	Wymiar podatków o opłat	Imiona i nazwiska, adres, nr działki, nr księgi wieczystej	Bez przepływu danych	
18.	Zbiór dokumentów KP, KW, K103	Imiona i nazwiska, adres	Bez przepływu danych	
19.	Zbiór list płac, faktur, rachunków	Imiona i nazwiska, adres, nr rachunku bankowego	Bez przepływu danych	
20.	Rejestr wyborców	Imiona i nazwisko, PESEL, imię ojca, data urodzenia, adres stałego zamieszkiwania, adres zameldowania, nazwa i adres miejscowości/lub okręg wyborczy w którym wyborca umieszczony jest w rejestrze wyborców, przypisanie do danego okręgu i obwodu	ŹRÓDŁO ⇒ KSN ⇒ Elud+ ⇒ Wyb+	

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	Uwagi
21.	Podatek akcyzowy	Imiona i nazwisko, NIP, PESEL, adres zamieszkania lub pobytu, nr dowodu osobistego, numer innego niż dowód osobisty dokumentu potwierdzającego tożsamość producenta rolnego oraz nazwa organu, który go wydał, oświadczenie o powierzchni użytków rolnych, pisemna zgoda pozostałych współwłaścicieli, numer rachunku bankowego, faktury VAT albo potwierdzone przez upoważnionego pracownika za zgodność z oryginałem ich kopie, limit, kwota i stawka zwrotu podatku akcyzowego oraz część limitu pozostała do wykorzystania.	Bez przepływu danych	
22.	Baza danych systemu gospodarki odpadami	Nazwiska i imiona, adres zamieszkania lub pobytu, PESEL, ilość osób zamieszkujących nieruchomość, informacje o odpadach z nieruchomości, rodzaj własności nieruchomości, rodzaj właściciela, adres nieruchomości lub w zarządzie, informacje dotyczące innych orzeczeń wydawanych w postępowaniu sądowym lub administracyjnym	Bez przepływu danych	
23.	Podatek transportowy	Imiona i nazwisko, data urodzenia, adres zamieszkiwania	Bez przepływu danych	
24.	Gospodarka wodno-ściekowa	Imiona i nazwiska, adres zamieszkania lub pobytu	Bez przepływu danych	
25.	Płace i kadry	Imiona i nazwiska, adres zamieszkania lub pobytu, PESEL, nr rachunku bankowego, przebieg zatrudnienia	Płace i kadry ⇒ Płatnik⇒Home banking	
26.	Zbiór kontrahentów	Imiona i nazwiska, adres zamieszkania lub pobytu, NIP, nr telefonu, przedmiot umowy, wartość zobowiązania, numer rachunku bankowego, adres poczty elektronicznej	Bez przepływu danych	
27.	Budownictwo	Imiona i nazwisko, adres zamieszkania lub pobytu, nr działki, nr księgi wieczystej, rodzaj własności	Bez przepływu danych	

Lp.	Nazwa zbioru danych (np. dane klientów, pracowników itd.)	Struktura zbiorów (np. imię i nazwisko, e-mail, telefon itd.)	Przeptywu danych	Uwagi
28.	Planowanie przestrzenne	Imiona i nazwiska, adres zamieszkania lub pobytu, nr działki, położenie, powierzchnia, przeznaczenie	Bez przepływu danych	
29.	Ewidencja numerów porządkowych nieruchomości	Imiona i nazwiska, adres zamieszkiwania lub pobytu, numer działki	Bez przepływu danych	
30.	Zbiór dokumentów wynajmu lokali komunalnych	Imiona i nazwiska, adres zamieszkania lub pobytu, PESEL, nr telefonu	Bez przepływu danych	
31.	Zbiór dokumentów dotyczących środowiskowych postępowań	Imiona i nazwisko, adres, nr działki	Bez przepływu danych	
32.	Zbiór dokumentów dotyczących wyrobów zawierających azbest	Imiona i nazwisko, adres, nr działki	Bez przepływu danych	
33.	Zbiór dokumentów w sprawie zajęcia pasa drogowego	Imiona i nazwisko, adres, nr działki, nr telefonu	Bez przepływu danych	
34.	CEIDG	Imiona i nazwisko, nazwisko rodowe, imię ojca, data urodzenia	Bez przepływu danych	
35.	Zamówienia publiczne	Imiona i nazwiska, data urodzenia, adres zamieszkania lub pobytu, zawód, wykształcenie, PESEL, NIP, seria i nr dowodu osobistego, nr telefonu, nazwa przedsiębiorcy, siedziba, imię i nazwisko/nazwa podwykonawcy, wykaz osób uprawnionych do podpisywania zleceń w imieniu wykonawcy, dokumenty rejestrujące, numer rachunku bankowego, adres poczty elektronicznej, numer fax, stan zatrudnienia	Bez przepływu danych	

Lp.	Nazwa zbioru danych <i>(np. dane Klientów, pracowników itd.)</i>	Struktura zbiorów <i>(np. imię i nazwisko, e-mail, telefon itd.)</i>	Przepływ danych	Uwagi
		Informacje o uprawnieniach, o wypłacalności, zdolności kredytowej, referencje, gwarancje bankowe i ubezpieczeniowe, wysokość wpłaconego wadium, klauzula tajemnicy przedsiębiorstwa, numer wpisu w Centralnej Ewidencji i Informacji Gospodarczej		
36.	Zbiór dokumentów sprzedaży mienia gminnego	Imiona i nazwisko, adres	Bez przepływu danych	
37.	Gospodarka nieruchomościami	Imiona i nazwiska, adres zamieszkania lub pobytu, nr działki, nr księgi wieczystej, rodzaj własności nieruchomości	Bez przepływu danych	
38.	Zezwolenia na sprzedaż napojów alkoholowych	Imiona i nazwiska, adres zamieszkania lub pobytu, NIP, nazwa osoby prawnej	Bez przepływu danych	
39.	Kwalifikacja wojskowa	Imiona i nazwisko, nazwisko rodowe, data i miejsce urodzenia, PESEL, adres i data zameldowania na pobyt stały, stopień wojskowy, nazwa, seria i numer wojskowego dokumentu osobistego, seria nr dowodu osobistego,	Bez przepływu danych	
40.	Rejestr skarg i wniosków	Nazwiska i imiona, adres zamieszkania lub pobytu,	Bez przepływu danych	
41.	Rejestr przedpoborowych (kobiet i mężczyzn)	Imiona i nazwiska, nazwiska rodowe, data i miejsce urodzenia, PESEL, adres i data zameldowania na pobyt stały, czasowy, stopień wojskowy	Bez przepływu danych	
42.	Zbiór osób z dostępem do informacji niejawnych	Imiona i nazwiska, adres zamieszkania lub pobytu, data urodzenia, imiona rodziców	Bez przepływu danych	
43.	Rejestr – wycinka drzew	Imiona i nazwisko, adres, nr działki, nr księgi wieczystej	Bez przepływu danych	
44.	System informacji oświatowej	Imiona i nazwiska, PESEL, stopień awansu zawodowego	Bez przepływu danych	

Lp.	Nazwa zbioru danych (np. dane klientów, pracowników itd.)	Struktura zbiorów (np. imię i nazwisko, e-mail, telefon itd.)	Przeptyw danych	Uwagi
45.	Zbiór dokumentów dotyczących dofinansowania kosztów kształcenia młodościanego pracownika	Imiona i nazwiska, data urodzenia, adres, zaświadczenie o zdaniu egzaminu w zawodzie, dane osobowe pracodawcy, NIP, REGON, nr rachunku bankowego pracodawcy, nr telefonu, informacje o wykształceniu	Bez przepływu danych	
46.	Zbiór dokumentów dotyczących organizacji szkół	Imiona i nazwiska, data i miejsce urodzenia, PESEL, nr dowodu osobistego, przebieg zatrudnienia, nr telefonu, imiona rodziców, nazwisko rodowe matki, wykształcenie	Bez przepływu danych	
47.	Zbiór uczniów korzystających z różnych programów rządowych i innych form wsparcia	Imiona i nazwiska, miejsce zamieszkania lub pobytu, PESEL	Bez przepływu danych	
48.	Zbiór dokumentów spełniania obowiązku nauki	Imiona i nazwiska, data urodzenia, PESEL, miejsce urodzenia, imiona rodziców, miejsce zamieszkania, typ szkoły	Bez przepływu danych	
49.	Płace i pochodne nauczycieli	Imiona i nazwiska, adres zamieszkania lub pobytu, PESEL, imiona rodziców, nr rachunku bankowego, sytuacja rodzinna, data i miejsce urodzenia, wykształcenie, przebieg zatrudnienia	Bez przepływu danych	
50.	Zbiór dokumentów rozliczenie dotacji punktów przedszkolnych	Imiona i nazwiska, adres zamieszkania lub pobytu, PESEL, data urodzenia	Bez przepływu danych	
51.	Zbiór dokumentów rozliczenie refundacji z PUP	Imiona i nazwiska, PESEL, nr rachunku bankowego	Bez przepływu danych	

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	Uwagi
52.	Zakładowy Fundusz Świadczeń Socjalnych nauczycieli	Imiona i nazwiska, adres zamieszkania lub pobytu, sytuacja rodzinna, finansowa, zdrowotna, seria i numer dowodu osobistego	Bez przepływu danych	

Data i podpis Administratora Danych

WÓJCI

*mgr Barbara Nowakowska*



Załącznik nr 9 do Polityki Bezpieczeństwa zgodnie z art. 31 ustawy

**Umowa powierzenia przetwarzania danych osobowych nr.....**

Załącznik do umowy Nr.....

Zawarta w dniu ..... r. w ..... pomiędzy:

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

zwanym w dalszej części niniejszej umowy „Zleceniodawcą”

reprezentowanym przez:

.....

a

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

zwanym w dalszej części niniejszej umowy „Wykonawcą”

reprezentowanym przez:

.....

o następującej treści:

**§ 1**

**Powierzenie przetwarzania danych osobowych**

1. W związku z realizacją umowy nr ..... z dnia ..... r. pomiędzy  
(.....)  
a (.....),

o ..... (np. świadczeniu usług kadrowych) Zleceniodawca powierza Wykonawcy trybie art. 31 ustawy z dnia 29 sierpnia 1997 r. o *ochronie danych osobowych* (T.J. Dz. U. z 2015 r., poz. 2135 ze zm) zwanej dalej „ustawą” przetwarzanie danych osobowych.

2. Zleceniodawca oświadcza, że jest administratorem danych, które powierza.
3. Powierzone dane zawierają informacje o ..... (np. pracownikach).
4. Zleceniodawca powierza Wykonawcy przetwarzanie danych osobowych w zakresie określonym w § 2.

## § 2

### Zakres i cel przetwarzania danych

1. Wykonawca będzie przetwarzał, powierzone na podstawie niniejszej Umowy, następujące kategorie danych osobowych/zbiory danych osobowych/:
  - 1) imię i nazwisko,
  - 2) numer ewidencyjny PESEL,
  - 3) seria i numer dowodu osobistego,
  - 4) .....
2. Celem przetwarzania danych jest ..... (np. realizacja obsługi kadrowo-płacowej).
3. Zakres przetwarzania obejmuje ..... (wprowadzanie, wgląd, modyfikację, drukowanie, usuwanie, archiwizację, przesyłanie) danych osobowych.
4. Powierzone przez Zleceniodawcę dane osobowe będą przetwarzane przez Wykonawcę wyłącznie w celu wykonywania przez Wykonawcę na rzecz Zleceniodawcy usług szczegółowo opisanych w umowie, o której mowa w § 1 ust.1 i w sposób zgodny z niniejszą Umową.

## § 3

### Sposób wykonania Umowy w zakresie przetwarzania danych osobowych

1. Wykonawca zobowiązuje się, przy przetwarzaniu danych osobowych, o których mowa w § 2 ust 1, do ich zabezpieczenia poprzez podjęcie środków technicznych i organizacyjnych, o których mowa w art. 36 – 39a ustawy.
2. Wykonawca oświadcza, że 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 informacyjne służące do przetwarzania danych osobowych (Dz. U. Nr 100, poz. 1024):
  - 1) prowadzi dokumentację opisującą sposób przetwarzania danych osobowych,
  - 2) znajdujące się w jego posiadaniu urządzenia i systemy informatyczne służące do przetwarzania danych osobowych zapewniają określony w Rozporządzeniu poziom bezpieczeństwa,
  - 3) stosuje środki techniczne i organizacyjne zapewniające ochronę przetwarzanych danych osobowych, a w szczególności zabezpieczenia danych osobowych przed ich udostępnieniem osobom nieupoważnionym, zabranieniem przez osobę

- nieuprawnioną, przetwarzaniem z naruszeniem ustawy, zmianą, utratą, uszkodzeniem lub zniszczeniem, w zakresie, za który odpowiada Wykonawca,
- 4) do wykonania czynności objętych umową dopuszcza jedynie osoby posiadające imienne upoważnienia wraz z klauzulą poufności i posiadające odpowiednią wiedzę z zakresu ochrony danych osobowych.
3. Wykonawca zobowiązuje się przetwarzać powierzone mu dane osobowe zgodnie z niniejszą Umową, ustawą oraz z innymi przepisami prawa powszechnie obowiązującego, które chronią prawa osób, których dane dotyczą.
  4. Wykonawca zobowiązuje się niezwłocznie zawiadomić Zleceniodawcę o:
    - 1) każdym prawnie umocowanym żądaniu udostępnienia danych osobowych właściwemu organowi państwa, chyba że zakaz zawiadomienia wynika z przepisów prawa, a szczególności przepisów postępowania karnego, gdy zakaz ma na celu zapewnienia poufności wszczętego dochodzenia,
    - 2) każdym nieupoważnionym dostępie do danych osobowych,
    - 3) każdym żądaniem otrzymanym od osoby, której dane przetwarza, powstrzymując się jednocześnie od odpowiedzi na żądanie.
  5. Zleceniodawca ma prawo do kontroli sposobu wykonywania niniejszej Umowy poprzez przeprowadzenie zapowiedzianych na 7 dni kalendarzowych wcześniej doraźnych kontroli dotyczących przetwarzania danych osobowych przez Wykonawcę oraz żądania składania przez niego pisemnych wyjaśnień.
  6. Na zakończenie kontroli, o których mowa w ust. 8, przedstawiciel Zleceniodawcy sporządza protokół w 2 egzemplarzach, który podpisują przedstawiciele obu stron. Wykonawca może wnieść zastrzeżenia do protokołu w ciągu 5 dni roboczych od daty jego podpisania przez strony.
  7. Wykonawca zobowiązuje się dostosować do zaleceń pokontrolnych mających na celu usunięcie uchybień i poprawę bezpieczeństwa przetwarzania danych osobowych.
  8. Wykonawca zobowiązuje się odpowiedzieć niezwłocznie i właściwie na każde pytanie Zleceniodawcy dotyczące przetwarzania powierzonych mu na podstawie Umowy danych osobowych.
  9. Wykonawca może „pod powierzyć” usługi objęte umową, o której mowa w § 1 ust. 1 i niniejszą umową podwykonawcom jedynie za zgodą Zleceniodawcy.

#### **§4**

##### **Odpowiedzialność Wykonawcy**

1. Wykonawca jest odpowiedzialny za udostępnienie lub wykorzystanie danych osobowych niezgodnie z Umową, a w szczególności za udostępnienie, ujawnienie, przekazanie osobom nieupoważnionym.
2. W przypadku naruszenia przepisów ustawy lub niniejszej Umowy z przyczyn leżących po stronie Wykonawcy, w następstwie, czego Zleceniodawca, jako administrator danych osobowych zostanie zobowiązany do wypłaty odszkodowania lub zostanie ukarany karą grzywny, Wykonawca zobowiązuje się pokryć Zleceniodawcy poniesione z tego tytułu straty i koszty.

## §5

### **Czas obowiązywania Umowy powierzenia**

1. Niniejsza Umowa powierzenia zostaje zawarta na czas określony od dnia ..... do dnia .....

## § 6

### **Warunki wypowiedzenia i rozwiązania Umowy**

1. Zleceniodawca ma prawo rozwiązać niniejszą Umowę bez zachowania terminu wypowiedzenia, gdy Wykonawca:
  - 1) wykorzystał dane osobowe w sposób niezgodny z niniejszą Umową,
  - 2) powierzył przetwarzanie danych osobowych podwykonawcom bez zgody Zleceniodawcy,
  - 3) nie zaprzestanie niewłaściwego przetwarzania danych osobowych,
  - 4) zawiadomi o swojej niezdolności do dalszego wykonywania niniejszej Umowy, a w szczególności niespełniania wymagań określonych w §3.
2. Rozwiązanie niniejszej Umowy przez Zleceniodawcę jest równoznaczne z wypowiedzeniem umowy, o której mowa w § 1 ust. 1.
3. Wykonawca, w przypadku wygaśnięcia umowy, o której mowa §1 ust.1 i niniejszej umowy niezwłocznie, ale nie później niż w terminie do 5 dni kalendarzowych, zobowiązuje się zwrócić lub usunąć wszelkie dane osobowe, których przetwarzanie zostało mu powierzone, w tym skutecznie usunąć je również z nośników elektronicznych pozostających w jego dyspozycji i potwierdzić powyższe przekazaniem Zleceniodawcy protokołem.

## §8

### **Postanowienia końcowe**

1. Wszelkie zmiany niniejszej umowy wymagają formy pisemnej pod rygorem nieważności.
2. W sprawach nieuregulowanych w niniejszej umowie mają zastosowanie przepisy Kodeksu cywilnego.
3. Spory wynikłe z tytułu Umowy będzie rozstrzygał Sąd właściwy dla miejsca siedziby Zleceniodawcy.
4. Umowę sporządzono w dwóch jednobrzmiących egzemplarzach, po jednym dla każdej ze stron.

.....  
za Zleceniodawcę

.....  
za Wykonawcę

Załącznik Nr 2 do Zarządzenia Wójta Gminy Rogowo Nr 6.2016 z dnia 01.02.2016 r.

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



**§ 1.****POSTANOWIENIA OGÓLNE**

Instrukcja zarządzania systemem informatycznym, służącym do przetwarzania danych osobowych w URZĘDZIE GMINY ROGOWO, określa:

- 1) Instrukcja zarządzania systemem informatycznym służącym do przetwarzania danych osobowych w URZĘDZIE GMINY ROGOWO, zwana dalej „Instrukcją” określa zasady, tryb postępowania i zalecenia Administratora Danych Osobowych, które należy stosować w trakcie przetwarzania danych osobowych w systemach informatycznych,
- 2) sposób przydziału haseł dla użytkowników i częstotliwość ich zmiany oraz osoby odpowiedzialne za te czynności,
- 3) sposób rejestrowania i wyrejestrowywania użytkowników oraz osoby odpowiedzialne za te czynności,
- 4) zasady i procedury rozpoczynania i kończenia pracy,
- 5) zasady i częstotliwość tworzenia kopii bezpieczeństwa.
- 6) zasady i częstotliwość kontroli obecności wirusów komputerowych oraz metodę ich usuwania,
- 7) zasady i czas przechowywania nośników informacji, w tym kopii informatycznych,
- 8) zasady dokonywania przeglądów i konserwacji systemu i zbioru danych osobowych,
- 9) zasady postępowania w zakresie komunikacji w sieci komputerowej,
- 10) instrukcja opracowana została zgodnie z wymogami § 5 Rozporządzenia Ministra Spraw Wewnętrznych i Administracji z dnia 29 kwietnia 2004 roku w sprawie dokumentacji przetwarzania danych osobowych oraz warunków technicznych i organizacyjnych, jakim powinny odpowiadać urządzenia i systemy informatyczne służące do przetwarzania danych osobowych w systemach informatycznych.

**§ 2.****DEFINICJE ZAWARTE W INSTRUKCJI**

Ilekroć w instrukcji jest mowa o :

- 1) **ustawa** - rozumie się przez to ustawę z dnia 29 sierpnia 1997 r. o ochronie danych osobowych ( Dz. U. z 2014 r. , poz. 1182 ), zwaną dalej „ustawą”;
- 2) **Jednostka (Firma, Urząd)** – rozumie się przez to URZĄD GMINY w ROGOWIE

- 3) **identyfikator użytkownika** - rozumie się przez to ciąg znaków literowych, cyfrowych lub innych jednoznacznie identyfikujący osobę upoważnioną do przetwarzania danych osobowych w systemie informatycznym;
- 4) **hasło** - rozumie się przez to ciąg znaków literowych, cyfrowych lub innych, znany jedynie osobie uprawnionej do pracy w systemie informatycznym;
- 5) **sieć telekomunikacyjna** - rozumie się przez to sieć telekomunikacyjną w rozumieniu art. 2 pkt 35 ustawy z dnia 16 lipca 2004 r. - Prawo telekomunikacyjne (Dz. U. Nr 171, poz. 1800, z późn. zm.)
- 6) **sieć publiczna** - rozumie się przez to sieć publiczną w rozumieniu art. 2 pkt 29 ustawy z dnia 16 lipca 2004 r. - Prawo telekomunikacyjne;
- 7) **teletransmisja** - rozumie się przez to przesyłanie informacji za pośrednictwem sieci telekomunikacyjnej;
- 8) **rozliczalność** - rozumie się przez to właściwość zapewniającą, że działania podmiotu mogą być przypisane w sposób jednoznaczny tylko temu podmiotowi;
- 9) **integralność danych** - rozumie się przez to właściwość zapewniającą, że dane osobowe nie zostały zmienione lub zniszczone w sposób nieautoryzowany;
- 10) **raport** - rozumie się przez to przygotowane przez system informatyczny zestawienia zakresu i treści przetwarzanych danych;
- 11) **poufność danych** - rozumie się przez to właściwość zapewniającą, że dane nie są udostępniane nieupoważnionym podmiotom;
- 12) **uwierzytelnianie** - rozumie się przez to działanie, którego celem jest weryfikacja deklarowanej tożsamości podmiotu,
- 13) **Administrator Danych (AD)** - w świetle przepisów ustawy o ochronie danych osobowych, art. 3 i 7 pkt 4 rozumie się przez to kierownika jednostki URZĘDU GMINY w ROGOWIE, który decyduje o celach i środkach przetwarzania danych osobowych;
- 14) **Administrator Bezpieczeństwa Informacji (ABI)** - rozumie się przez to osobę wyznaczoną przez Administratora Danych (kierownika jednostki), nadzorującą przestrzeganie zasad ochrony danych osobowych, w szczególności zabezpieczenia danych przed ich udostępnieniem osobom nieupoważnionym, zabraniam przez osobę nieuprawnioną, przetwarzaniem z naruszeniem ustawy oraz zmianą, utratą, uszkodzeniem lub zniszczeniem;

- 15) **Administrator Systemu Informatycznego (ASI)**, zwanego też **Administratorem Systemu** - rozumie się przez to osobę zatrudnioną przez WÓJTA GMINY BARBARĘ NOWAKOWSKA kierownika jednostki, upoważnioną do realizacji zadań związanych z zarządzaniem systemem informatycznym;
- 16) **użytkownik systemu informatycznego** - rozumie się przez to upoważnioną przez kierownika jednostki WÓJTA GMINY - BARBARĘ NOWAKOWSKĄ, pracownika do przetwarzania danych osobowych w systemie informatycznym, który odbył stosowne szkolenie w zakresie ochrony danych.

### § 3.

#### ZASADY DOSTĘPU UŻYTKOWNIKA DO SYSTEMU

1. Dostęp do systemu informatycznego służącego do przetwarzania danych osobowych, zwanego dalej „systemem” może uzyskać wyłącznie osoba (użytkownik) zarejestrowana w tym systemie przez Administratora Systemu na wniosek kierownika referatu i po akceptacji Administratora Bezpieczeństwa Informacji.

3. Rejestracja, o której mowa w ust. 1, polega na nadaniu identyfikatora i przydziale hasła oraz wprowadzeniu tych danych do bazy użytkowników systemu.

### § 4.

#### IDENTYFIKATOR

1. Identyfikator składa się z minimum sześciu znaków.
2. W identyfikatorze pomija się polskie znaki diakrytyczne.
3. W przypadku zbieżności nadawanego identyfikatora z identyfikatorem wcześniej zarejestrowanego użytkownika Administrator Systemu po uzgodnieniu z ABl nadaje inny identyfikator.

### § 5.

#### HASŁA

1. Hasło powinno składać się z unikalnego zestawu co najmniej ośmiu znaków, zawierać małe i wielkie litery oraz cyfry lub znaki specjalne.
2. Hasło nie może być identyczne z identyfikatorem użytkownika, ani z jego imieniem lub nazwiskiem.

3. Zmiana hasła następuje nie rzadziej niż co 30 dni z zastrzeżeniem § 6.

4. Zabrania się użytkownikom systemu udostępniania swojego identyfikatora i hasła innym osobom.

## § 6.

### WYREJESTROWANIE UŻYTKOWNIKA

1. Wyrejestrowania użytkownika z systemu informatycznego dokonuje Administrator Systemu na wniosek kierownika referatu.

2. Wyrejestrowanie, o którym mowa w ust. 1, może mieć charakter czasowy lub trwały.

3. Wyrejestrowanie następuje poprzez:

- 1) zablokowanie konta użytkownika do czasu ustania przyczyny uzasadniającej blokadę (wyrejestrowanie czasowe),
- 2) usunięcie danych użytkownika z bazy użytkowników systemu (wyrejestrowanie trwałe).

4. Przyczyną czasowego wyrejestrowania użytkownika z systemu informatycznego jest:

- 3) nieobecność w pracy trwająca dłużej niż 31 dni kalendarzowych,
- 4) zawieszenie w pełnieniu obowiązków służbowych,
- 5) zwolnienie z pełnienia obowiązków służbowych.

5. Przyczyną trwałego wyrejestrowania użytkownika z systemu informatycznego jest rozwiązanie lub wygaśnięcie stosunku pracy użytkownika.

## § 7.

### ROZPOCZĘCIE PRACY W SYSTEMIE

Rozpoczęcie pracy w systemie odbywa się poprzez:

- 1) przygotowanie stanowiska pracy,
- 2) włączenie stacji roboczej,
- 3) wprowadzenie swojego identyfikatora i hasła.

## § 8.

### ZAKOŃCZENIE PRACY W SYSTEMIE

Zakończenie pracy w systemie odbywa się poprzez:

- 1) zamknięcie aplikacji,
- 2) odłączenie się od zasobów systemowych,

- 3) zamknięcie systemu operacyjnego,
- 4) wyłączenie stacji roboczej.

#### § 9.

##### ZASADY PRACY W SYSTEMIE

1. Zabrania się użytkownikom pracującym w systemie:
  - 1) udostępniania stacji roboczej osobom niezarejestrowanym z zastrzeżeniem pkt 2,
  - 2) udostępniania stacji roboczej do konserwacji lub naprawy bez porozumienia z Administratorem Systemu Informatycznego,
  - 3) używania nielicencjonowanego oprogramowania.
  - 4) Używania oprogramowania niewiadomego pochodzenia.

#### § 10.

##### NARUSZENIE BEZPIECZEŃSTWA SYSTEMU

1. Każdy przypadek naruszenia ochrony danych osobowych, które mogą wskazywać na naruszenie bezpieczeństwa podlega zgłoszeniu do Administratora Bezpieczeństwa Informacji, a w szczególności:

- 1) naruszenia bezpieczeństwa systemu informatycznego,
- 2) stwierdzenia objawów (stanu urządzeń, sposobu działania programu lub jakości komunikacji w sieci).

2. Administratorowi Bezpieczeństwa Informacji zgłasza się w szczególności przypadki:

- 1) użytkownika stacji roboczej przez osobę nie będącą użytkownikiem systemu,
- 2) usiłowania logowania się do systemu (sieci) przez osobę nieuprawnioną,
- 3) usuwania, dodawania lub modyfikowania bez wiedzy i zgody użytkownika jego dokumentów (rekordów),
- 4) przebywania osób nieuprawnionych w obszarze, w którym przetwarzane są dane osobowe, w trakcie nieobecności osoby zatrudnionej przy przetwarzaniu tych danych i bez zgody Administratora Danych, pozostawiania bez nadzoru otwartych pomieszczeń, w których przetwarzane są dane osobowe,
- 5) udostępniania osobom nieuprawnionym stacji roboczej lub komputera przenośnego, służących do przetwarzania danych osobowych,

- 6) niezabezpieczenia hasłem dostępu do komputera służącego do przetwarzania danych osobowych,
- 7) przechowywania kopii awaryjnych w tych samych pomieszczeniach, w których przechowywane są zbiory danych osobowych eksploatowane na bieżąco,
- 8) przechowywania nośników informacji oraz wydruków z danymi osobowymi, nieprzeznaczonymi do udostępniania, w warunkach umożliwiających do nich dostęp osobom nieuprawnionym.

3. Obowiązek dokonania zgłoszenia, o którym mowa w ust 1, spoczywa na każdym użytkowniku, który powziął wiadomość o naruszeniu ochrony danych osobowych.

4. W przypadku naruszenia integralności bezpieczeństwa sieciowego, obowiązkiem Administratora Systemu jest natychmiastowe wstrzymanie udostępniania zasobów dla użytkowników i odłączenie serwerów od sieci.

5. Użytkownik sieci i Administrator Systemu w porozumieniu z Administratorem Bezpieczeństwa Informacji ustalają przyczyny naruszenia integralności bezpieczeństwa sieciowego.

6. Przywrócenie udostępniania zasobów użytkownikom może nastąpić dopiero po ustaleniu i usunięciu przyczyny naruszenia integralności bezpieczeństwa sieciowego.

## § 11.

### KOPIE ZAPASOWE

1. Kopie awaryjne tworzy się z następującą częstotliwością:

- 1) kopie systemu finansowo - księgowego – dwa razy w miesiącu,
- 2) kopie pozostałe - nie rzadziej niż raz na miesiąc.

2. Każdą kopię tworzy się na oddzielnym nośniku informatycznym.

3. Zabrania się przechowywania kopii awaryjnych w pomieszczeniach przeznaczonych do przechowywania zbiorów danych pozostających w bieżącym użytkowaniu.

4. Administrator Systemu przegląda okresowo kopie awaryjne i ocenia ich przydatność do odtworzenia zasobów systemu w przypadku jego awarii.

5. Stwierdzenie utraty przez kopie awaryjne waloru przydatności do celu, o którym mowa w ust. 4, upoważnia Administratora Systemu do ich zniszczenia.

## § 12.

1. Sprawdzanie obecności wirusów komputerowych w systemie oraz ich usuwanie odbywa się przy wykorzystaniu licencjonowanego oprogramowania w oparciu o serwer dystrybucji aktualnych sygnatur i wersji oprogramowania.

2. Oprogramowanie, o którym mowa w ust. 1, sprawuje ciągły nadzór (ciągła praca w tle) nad pracą systemu i jego zasobami oraz serwerami i stacjami roboczymi.

3. Niezależnie od ciągłego nadzoru, o którym mowa w ust. 2, Administrator Systemu nie rzadziej niż raz na dwa miesiące przeprowadza pełną kontrolę obecności wirusów komputerowych w systemie oraz jego zasobach, jak również w serwerach i stacjach roboczych.

4. Do obowiązków Administratora Systemu należy aktualizacja oprogramowania służącego do sprawdzania w systemie obecności wirusów komputerowych.

### **§ 13.**

#### **ZASILANIE AWARYJNE**

1. System i urządzenia informatyczne służące do przetwarzania danych osobowych, zasilane energią elektryczną, zabezpiecza się przed utratą danych osobowych spowodowaną awarią zasilania lub zakłóceniami w sieci zasilającej.

2. Minimalne zabezpieczenie systemu i urządzeń informatycznych, o których mowa w ust. 1, polega na wyposażeniu serwera (serwerów) oraz stacji roboczych w zasilacze awaryjne (UPS).

### **§ 14.**

#### **NAPRAWA, SERWIS URZĄDZEŃ**

1. Urządzenia informatyczne służące do przetwarzania danych osobowych można przekazać do naprawy, do likwidacji dopiero po uprzednim uzyskaniu zgody Administratora Bezpieczeństwa Informacji.

2. Urządzenia, o których mowa w ust. 1 przed ich przekazaniem pozbawia się zapisu danych osobowych poprzez wymontowanie dysku twardego z zastrzeżeniem ust. 3.

3. Jeżeli nie jest to możliwe, urządzenie to może być naprawiane wyłącznie pod nadzorem Administratora Systemu.

4. Jeżeli nie jest możliwe pozbawienie urządzenia przekazywanego do likwidacji zapisu danych osobowych, urządzenie - przed przekazaniem - uszkadza się w sposób uniemożliwiający odczytanie tych danych.

#### § 15.

##### **PRZEGLĄD , KONSERWACJE**

1. Przeglądu i konserwacji systemu dokonuje Administrator Systemu doraźnie.
2. Przeglądu pliku zawierającego raport dotyczący działalności aplikacji bądź systemu (log systemowy) Administrator Systemu dokonuje nie rzadziej niż raz na dwa tygodnie.
3. Przeglądu i sprawdzenia poprawności zbiorów danych zawierających dane osobowe dokonuje użytkownik przy współudziale Administratora Systemu nie rzadziej niż raz na dwa tygodnie.

#### § 16.

##### **BEZPIECZEŃSTWO KOMUNIKACJI**

1. Bezpieczeństwo komunikacji w obrębie systemów przetwarzających dane osobowe Administrator Systemu zapewnia przy użyciu narzędzi w obrębie systemu.
2. W systemach działających sieciowo, na zasadzie udostępnienia zasobów na serwerze, Administrator Systemu powinien uwzględniać dedykowane przyzwolenia dostępu.

#### § 17

##### **KOMUNIKACJA WEWNĘTRZNA**

1. Przesyłanie danych osobowych w komunikacji wewnętrznej (LAN) musi być oznaczone w sposób dostępny jedynie dla uprawnionych użytkowników przy użyciu narzędzi zabezpieczeń w obrębie systemu informatycznego.
2. W sytuacji, gdy dostępne narzędzia informatyczne nie będą wystarczające do działania w komunikacji wewnętrznej, użytkownik systemu wyznacza sposób postępowania, mając w szczególności na uwadze ochronę danych osobowych.

#### § 18.

Do przesyłania danych przy połączeniach w sieci publicznej (Internet), z uwagi na przekazywane dane osobowe, powinny być wykorzystywane tylko kanały transmisji

wykorzystywane przez autoryzowane programy wykorzystywane również w innych urzędach oraz instytucjach państwowych i w oparciu o przepisy prawne regulujące sposób wysyłania tych danych.

### § 19.

#### OZNACZANIE NOŚNIKÓW DANYCH

Nośniki informatyczne zawierające dane osobowe powinny być opisane w sposób czytelny i zrozumiały dla użytkownika, a zarazem nie powinny ułatwiać rozpoznania zawartości przez osoby nieupoważnione.

### § 20.

#### BEZPIECZEŃSTWO NOSNIKÓW, URZĄDZEŃ

1. Nośniki informatyczne przechowywane są w miejscach, do których dostęp mają wyłącznie osoby upoważnione.

2. W pomieszczeniach, gdzie nie jest możliwe ograniczenie dostępu osób postronnych, monitory stanowisk dostępu do danych osobowych ustawia się w taki sposób, aby uniemożliwić tym osobom wgląd w dane.

3. Ekran monitorów stanowisk dostępu do danych osobowych są zaopatrzone w wygaszacze z ustawioną opcją wymagania hasła, które po upływie maksymalnie 10 minut nieaktywności użytkownika automatycznie wyłączają możliwość eksploracji ekranu.

### § 21.

#### PRZENOŚNE NOŚNIKI INFORMATYCZNE

Osoby użytkujące przenośne nośniki informatyczne, służące do przetwarzania danych osobowych, obowiązane są niezwłocznie informować na piśmie Administratora Bezpieczeństwa Informacji o zakresie, rodzaju zbieranych danych osobowych oraz celu ich przetwarzania. Administrator Bezpieczeństwa Informacji może żądać usunięcia danych, co do których zachodzi uzasadnione podejrzenie, że nie są przetwarzane zgodnie z zasadami określonymi w przepisach o ochronie danych osobowych.

### § 22.

#### PRZENOSNY KOMPUTER

Osoba użytkująca przenośny komputer, służący do przetwarzania danych osobowych, obowiązana jest zachować szczególną ostrożność podczas transportu i przechowywania tego komputera poza obszarem ochrony danych w celu zapobieżenia dostępowi do tych danych osobie niepowołanej.

### § 23.

#### WYDRUKI

1. Użytkownik sporządzający wydruki, które zawierają dane osobowe jest odpowiedzialny za zachowanie szczególnej ostrożności przy korzystaniu z nich, a zwłaszcza za zabezpieczenie ich przed dostępem osób nie posiadających imiennego upoważnienia oraz nieuprawnionych do wglądu.

2. Wydruki zawierające dane osobowe, które są przeznaczone do usunięcia, należy zniszczyć w stopniu uniemożliwiającym ich odczytanie.

### § 24.

#### DANE UŻYTKOWNIKA

System powinien umożliwić udostępnienie na piśmie, w zrozumiałej formie, treści danych o każdej osobie, której dane są przetwarzane, a w szczególności:

- a) daty pierwszego wprowadzenia danych tej osoby,
- b) źródła pochodzenia danych,
- c) nazwy użytkownika wprowadzającego dane,
- d) informacji - komu, kiedy i w jakim zakresie dane zostały udostępnione,
- e) sprzeciwu, o którym mowa w art. 32 ust. 1 pkt 7, po jego uwzględnieniu, oraz sprzeciwu określonego w art. 32 ust. 1 pkt 8 ustawy o ochronie danych osobowych.

### § 25.

#### ODPOWIEDZIALNOŚĆ

Naruszenie obowiązków wynikających z niniejszej Polityki Bezpieczeństwa oraz przepisów ustawy o ochronie danych osobowych może być uznane za ciężkie naruszenie obowiązków pracowniczych, podlegające sankcjom dyscyplinarnym oraz sankcjom karnym w szczególności wynikającym z przepisów tejże ustawy.

**§ 26.****OBOWIĄZKI ADMINISTRATORA BEZPIECZEŃSTWA INFORMACJI**

Do obowiązków Administratora Bezpieczeństwa Informacji w zakresie ochrony danych osobowych przetwarzanych w systemach informatycznych należy w szczególności:

- 1) nadzór nad stosowaniem środków ochrony,
- 2) nadzór nad przestrzeganiem przez Administratora Systemów Informatycznych i użytkowników systemu - procedur bezpieczeństwa,
- 3) wskazywanie zagrożeń oraz reagowanie na naruszenia ochrony danych osobowych i usuwanie ich skutków,
- 4) prowadzenie ewidencji użytkowników systemów informatycznych, w których przetwarzane są dane osobowe, która jest j częścią ewidencji osób upoważnionych do przetwarzania danych osobowych oraz wszelkiej dokumentacji opisującej sposób realizacji i zasady ochrony danych osobowych w URZĘDZIE GMINY ROGOWO,
- 5) kontrolowanie nadanych w systemach informatycznych uprawnień do przetwarzania danych osobowych pod kątem ich zgodności z wpisami umieszczonymi w ewidencji osób upoważnionych do przetwarzania danych osobowych.
- 6) prowadzenie szkoleń dla użytkowników w zakresie stosowanych w systemach informatycznych środków ochrony danych osobowych,
- 7) prowadzenie rejestru zbiorów będących w zasobach Administratora danych ,
- 8) współdziałanie z Generalnym Inspektorem Ochrony Danych Osobowych w zakresie sprawdzeń zleconych przez GIODO ,
- 9) uzgadnianie z Administratorem Systemów Informatycznych procedur regulujących wykonywanie czynności w systemach lub aplikacjach służących do przetwarzania danych osobowych.

**§ 27.****OBOWIĄZKI ADMINISTRATORA SYSTEMÓW INFORMATYCZNYCH**

Do obowiązków Administratora Systemów Informatycznych w zakresie ochrony danych osobowych przetwarzanych w systemach informatycznych należy w szczególności:

- 1) realizacja zadań związanych z przeszkoleniem użytkowników w zakresie obsługi sprzętu informatycznego, oprogramowania systemowego oraz oprogramowania do obsługi aplikacji , którą będą wykorzystywali,
  - 2) zapoznanie użytkowników z treścią Instrukcji,
  - 3) operacyjne zarządzanie systemami informatycznymi w sposób zapewniający ochronę danych osobowych w nich przetwarzanych,
  - 4) przestrzeganie opracowanych dla systemu procedur operacyjnych i bezpieczeństwa,
  - 5) kontrola przepływu informacji pomiędzy systemem informatycznym a siecią publiczną oraz kontrola działań inicjowanych z sieci publicznej a systemem informatycznym,
  - 6) zarządzanie stosowanymi w systemach informatycznym środkami uwierzytelnienia, w tym rejestrowanie i wyrejestrowywanie użytkowników oraz dokonywanie zmiany uprawnień ,
- 10) utrzymanie systemu w należytej sprawności technicznej,
- 11) regularne tworzenie kopii zapasowych zasobów danych osobowych oraz programów służących do ich przetwarzania oraz okresowe sprawdzanie poprawności wykonania kopii zapasowych,
- 12) Wykonywanie lub nadzór nad wykonywaniem okresowych przeglądów i konserwacji, zgodnie z odrębnymi procedurami, sprzętu IT, systemów informatycznych, aplikacji oraz elektronicznych nośników informacji, na których przetwarzane są dane osobowe.

#### PRZEPISY KOŃCOWE

W sprawach nieuregulowanych w niniejszej Instrukcji mają zastosowanie przepisy ustawy z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (T. J. Dz. U. 2015 r. poz. 2135, z późn. zm.) oraz 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. z 2004 r. Nr 100, poz. 1024).