# Zarządzenie nr 46/2018

## Wójta Gmin z dnia 25 maja 2018

### w sprawie ochrony danych osobowych w Urzędzie Gminy Rawa Mazowiecka

W związku z Rozporządzeniem Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 roku 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) Dz.U.UE.L.2016.119.1 oraz § 3 rozporządzenia Ministra Spraw Wewnętrznych i Administracji z dnia 29 kwietnia 2004 r. w sprawie dokumentacji przetwarzania danych osobowych oraz warunków technicznych i organizacyjnych, jakim powinny odpowiadać urządzenia i systemy informatyczne służące do przetwarzania danych osobowych (Dz.U. Nr 100, poz. 1024), zarządza się, co następuje:

**§ 1**

W Urzędzie Gminy Rawa Mazowiecka wprowadza się:

1) Politykę Bezpieczeństwa, stanowiącą załącznik nr 1 do zarządzenia;
2) Instrukcję Zarządzania Systemem Informatycznym służącym do przetwarzania danych osobowych, stanowiącą załącznik nr 2 do zarządzenia.

**§ 2**

Zobowiązuje się wszystkich pracowników Urzędu Gminy Rawa Mazowiecka do zapoznania się z niniejszym zarządzeniem i załącznikami do zarządzenia w terminie do 30 maja 2018 oraz do przestrzegania zasad zawartych w tych dokumentach. Oświadczenie o zapoznaniu się należy wpiąć do akt osobowych pracowników Urzędu Gminy Rawa Mazowiecka.

**§ 3**

Nadzór nad wykonaniem zarządzenia powierzam Sekretarzowi Gminy Rawa Mazowiecka

**§ 4**

Zarządzenie wchodzi w życie z dniem 25 maja 2018 roku.

WÓJT
Krzysztof Starczewski

Załącznik Nr 2
do zarządzenia Nr 46/2018
Wójta Gminy Rawa Mazowiecka
z dnia 25 maja 2018

# Instrukcja
# zarządzania systemem informatycznym służącym do przetwarzania danych osobowych w Urzędzie Gminy Rawa Mazowiecka

## Rozdział 1
## Postanowienia ogólne

### § 1

Stosownie do postanowień § 3 i § 5 rozporządzenia Ministra Spraw Wewnętrznych i Administracji z 29 kwietnia 2004 r. w sprawie dokumentacji przetwarzania danych osobowych oraz warunków technicznych i organizacyjnych, jakim powinny odpowiadać urządzenia i systemy informatyczne służące do przetwarzania danych osobowych (Dz.U. z 2004 r., nr 100, poz. 1024), ustala się treść Instrukcji zarządzania systemem informatycznym służącym do przetwarzania danych osobowych w Urzędzie Gminy Rawa Mazowiecka zwaną dalej Instrukcją. *Opracowany dokument jest zgodny z Rozporządzeniem Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 roku w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/UE.L.2016.119.1 – RODO*

### § 2

Instrukcja ma zastosowanie na obszarze wskazanym w Polityce Bezpieczeństwa Przetwarzania Danych Osobowych w Urzędzie Gminy Rawa Mazowiecka (dalej Polityka Bezpieczeństwa), w którym przetwarzane są dane osobowe w systemie informatycznym.

# I. Wstęp

§ 1

Celem Polityki Bezpieczeństwa przetwarzania danych osobowych w **Urzędzie Gminy Rawa Mazowiecka** , zwanej dalej Polityką Bezpieczeństwa, jest uzyskanie optymalnego i zgodnego z wymogami obowiązujących aktów prawnych, sposobu przetwarzania w Urzędzie Gminy informacji zawierających dane osobowe, a przede wszystkim zapewnienie ochrony danych osobowych przetwarzanych w Urzędzie Gminy przed wszelkiego rodzaju zagrożeniami, tak zewnętrznymi jak i wewnętrznymi.

§ 2

Polityka Bezpieczeństwa została utworzona w związku z wymaganiami zawartymi w ustawie z dnia 10 maja 2018 r. o ochronie danych osobowych (Dz.U. z 2018 r poz...) 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. *Opracowany dokument jest zgodny również z Rozporządzeniem Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 roku w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/UE.L.2016.119.1 – RODO*

§ 3

Obszarem przetwarzania danych osobowych w **Urzędzie Gminy Rawa Mazowiecka** są wydzielone pomieszczenia w budynku, w którym mieści się biuro, tj. **przy ul. Konstytucji 3 Maja 32, 96-200 Rawie Mazowieckiej.**

§ 4

Ochrona danych osobowych realizowana jest poprzez zabezpieczenia fizyczne, procedury organizacyjne, oprogramowanie systemowe, aplikacje oraz użytkowników.

§ 5

1. Utrzymanie bezpieczeństwa przetwarzanych danych osobowych w Urzędzie Gminy rozumiane jest jako zapewnienie ich poufności, integralności, rozliczalności oraz dostępności na odpowiednim poziomie. Miarą bezpieczeństwa jest wielkość ryzyka związanego z ochroną danych osobowych.
2. Zastosowane zabezpieczenia mają służyć osiągnięciu powyższych celów i zapewnić:
   1) poufność danych – rozumianą jako właściwość zapewniającą, że dane nie są udostępniane nieupoważnionym osobom;
   2) integralność danych – rozumianą jako właściwość zapewniającą, że dane osobowe nie zostały zmienione lub zniszczone w sposób nieautoryzowany;
   3) rozliczalność danych - rozumianą jako właściwość zapewniającą, że działania osoby mogą być przypisane w sposób jednoznaczny tylko tej osobie;
   4) integralność systemu - rozumianą jako nienaruszalność systemu, niemożność jakiejkolwiek manipulacji, zarówno zamierzonej, jak i przypadkowej;
   5) dostępność informacji - rozumianą jako zapewnienie, że osoby upoważnione mają dostęp do informacji i związanych z nią zasobów wtedy, gdy jest to potrzebne;
   6) zarządzanie ryzykiem - rozumiane jako proces identyfikowania, kontrolowania i minimalizowania lub eliminowania ryzyka dotyczącego bezpieczeństwa, które może dotyczyć systemów informacyjnych służących do przetwarzania danych osobowych.

**§ 6**

**Administratorem Danych Osobowych** przetwarzanych w Urzędzie Gminy Rawa Mazowiecka jest **Wójt Gminy**

§ 7

**Inspektorem Ochrony Danych zwany dalej IOD** – jest osoba powołana na to stanowisko przez Administratora Danych odrębnym zarządzeniem.

# II. Definicje

§ 8

Przez użyte w Polityce Bezpieczeństwa określenia należy rozumieć:

1) **Polityka Bezpieczeństwa** – rozumie się przez to Politykę Bezpieczeństwa Ochrony Danych Osobowych w Urzędzie Gminy Rawa Mazowiecka ;

2) **Administrator Danych Osobowych** – dalej jako Administrator danych; rozumie się przez to Wójta Gminy

3) **Inspektor Ochrony Danych (IOD)** - rozumie się przez to osobę wyznaczoną przez Administratora Danych Osobowych, nadzorującą przestrzeganie zasad ochrony danych osobowych, w szczególności zabezpieczenia danych przed ich udostępnieniem osobom nieupoważnionym, zabraniem przez osobę nieuprawnioną, przetwarzaniem z naruszeniem ustawy oraz zmianą, utratą, uszkodzeniem lub zniszczeniem;

4) **Biuro** – siedzibę Urzędu Gminy Rawa Mazowiecka

5) **Ustawa** – ustawa z dnia 10 maja 2018 r o ochronie danych osobowych

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

7) **RODO - Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2016/679 -** z dnia 27 kwietnia 2016 roku w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych.

8) **Dane osobowe** – wszelkie informacje dotyczące zidentyfikowanej lub możliwej do zidentyfikowania osoby fizycznej;

9) **Zbiór 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;

10) **Baza danych osobowych** – zbiór uporządkowanych powiązanych ze sobą tematycznie zapisanych np. w pamięci wewnętrznej komputera. Baza danych jest złożona z elementów o określonej strukturze – rekordów lub obiektów, w których są zapisywane dane osobowe;

11) **Usuwanie danych** – rozumie się przez to zniszczenie danych osobowych lub taką ich modyfikację, która nie pozwoli na ustalenie tożsamości osoby, której dotyczą

12) **Przetwarzane danych** - rozumie się przez to jakiekolwiek operacje wykonywane na danych osobowych, takie jak zbieranie, utrwalanie, przechowywanie, opracowywanie, zmienianie, udostępnianie i usuwanie, a zwłaszcza te, które wykonuje się w systemach informatycznych;

13) **System informatyczny** - rozumie się przez to zespół współpracujących ze sobą urządzeń, programów, procedur przetwarzania informacji i narzędzi programowych zastosowanych w celu przetwarzania danych osobowych;

14) **System tradycyjny** - rozumie się przez to zespół procedur organizacyjnych, związanych z mechanicznym przetwarzaniem informacji i wyposażenia i środków trwałych w celu przetwarzania danych osobowych na papierze;

15) **Zabezpieczenie danych w systemie informatycznym** - rozumie się przez to wdrożenie i eksploatację stosownych środków technicznych i organizacyjnych zapewniających ochronę danych przed ich nieuprawnionym przetwarzaniem;

16) **Administrator systemu informatycznego** – rozumie się przez to osobę lub osoby, upoważnione przez administratora danych osobowych do administrowania i zarządzania systemami informatycznymi w Urzędzie Gminy Rawa Mazowiecka

17) **Użytkownik** - rozumie się przez to upoważnionego przez Administratora danych lub Inspektora Ochrony Danych, wyznaczonego do przetwarzania danych osobowych pracownika Urzędu Gminy Rawa Mazowiecka , który odbył stosowne szkolenie w zakresie ochrony tych danych.

# III. Zakres stosowania

§ 9

1. W Urzędzie Gminy przetwarzane są przede wszystkim informacje służące do realizacji zadań własnych i zleconych gminy .
2. Informacje te są przetwarzane i składowane zarówno w postaci dokumentacji tradycyjnej jak i elektronicznej.
3. Polityka Bezpieczeństwa zawiera dokumenty dotyczące wprowadzonych zabezpieczeń technicznych i organizacyjnych zapewniających ochronę przetwarzanych danych osobowych.

§ 10

Politykę Bezpieczeństwa stosuje się przede wszystkim do:

1) Danych osobowych przetwarzanych w systemach informatycznych. Wykaz systemów zainstalowanych w Urzędzie wyszczególniony w § 14 niniejszej Polityki Bezpieczeństwa
2) Wszystkich informacji dotyczących danych pracowników Urzędu Gminy, w tym danych osobowych pracowników i treści zawieranych umów o pracę.
3) Wszystkich danych kandydatów do pracy zbieranych na etapie rekrutacji.
4) Informacji dotyczących zabezpieczenia danych osobowych, w tym w szczególności nazw kont i haseł w systemach przetwarzania danych osobowych.

5) Rejestru osób dopuszczonych do przetwarzania danych osobowych.

6) Innych dokumentów zawierających dane osobowe.

§ 11

1. Zakresy ochrony danych osobowych określone przez dokumenty Polityki Bezpieczeństwa mają zastosowanie do systemów informatycznych , w których są przetwarzane dane osobowe, a w szczególności do:

    1) wszystkich istniejących, wdrażanych obecnie lub w przyszłości systemów informatycznych oraz papierowych, w których przetwarzane są dane osobowe podlegające ochronie;

    2) wszystkich lokalizacji - budynków i pomieszczeń, w których są lub będą przetwarzane informacje podlegające ochronie;

    3) wszystkich pracowników w rozumieniu przepisów Kodeksu Pracy, stażystów, praktykantów i innych osób mających dostęp do informacji podlegających ochronie Urzędzie.

2. Do stosowania zasad określonych przez dokumenty Polityki Bezpieczeństwa zobowiązani są wszyscy pracownicy w rozumieniu Kodeksu Pracy, stażyści, praktykanci oraz inne osoby mające dostęp do informacji podlegających ochronie.

§ 12

Informacje niejawne nie są objęte zakresem niniejszej Polityki Bezpieczeństwa.

# IV. Wykaz budynków, pomieszczeń lub części pomieszczeń, tworzących obszar, w którym przetwarzane są dane osobowe oraz sposobów ich zabezpieczeń

§ 13

1. Polityka obowiązuje w Urzędzie Gminy , w pomieszczeniach lub częściach pomieszczeń, w których przetwarzane są dane osobowe, a których wykaz został zamieszczony poniżej.
2. Główna i jedyna siedziba Urzędu Gminy mieści się pod adresem: al. Konstytucji 3 Maja 32, 96-200 Rawa Mazowiecka

| | | |
|---|---|---|
| 1. | Wykaz pomieszczeń, w których przetwarzane są dane osobowe | Pokój nr 101, 102 103,,105, 107, 109, 201,202,203,204,205,206,207.,208, 304, 305, |
| 2. | Wykaz pomieszczeń, w których znajdują się komputery stanowiące element systemu informatycznego | 204, 205, 206, 207, 208, 109, 107,102,101 |
| 3. | Wykaz pomieszczeń, gdzie przechowuje się wszelkie nośniki informacji zawierające dane osobowe (szafy z dokumentacją papierową, szafy zawierające komputerowe nośniki informacji z kopiami zapasowymi danych, stacje komputerowe, serwery i inne urządzenia komputerowe) | Pokój 111 |
| 4. | Wykaz pomieszczeń, w których składowane są uszkodzone komputerowe nośniki danych (taśmy, dyski, płyty CD, dyski przenośne, uszkodzone komputery) | Pokój 111 |
| 5. | Wykaz pomieszczeń archiwum | Piwnica 001,002 |

| | | |
|---|---|---|
| 6. | Wykaz programów, w których przetwarzane są dane osobowe | Pok.111, 208, |
| 7. | Wykaz podmiotów zewnętrznych, które mają dostęp do danych osobowych lub je przetwarzają na podstawie podpisanych umów (np. informatyk) – nazwa firmy, imię, nazwisko, adres, funkcja. | Pok.111, 103 ( umowy powierzenia) |
| 8. | Inne informacje dotyczące pomieszczeń, w których przetwarzane są dane osobowe oraz ich zabezpieczeń | Budynek monitorowany, szafy zamykane na klucz, pokoje zamykane, system alarmowy |

# V. Wykaz zbiorów danych osobowych przetwarzanych w systemach informatycznych wraz ze wskazaniem programów zastosowanych do ich przetwarzania

§ 14

Zbiory danych wytworzone w Urzędzie Gminy Rawa Mazowiecka

| Lp | Zbiór Danych | Dział/ jednostka organizacyjna | Program | Lokalizacja bazy danych | Miejsce przetwarzania danych |
|---|---|---|---|---|---|
| 1. | Dane petentów, interesantów, stron postepowania | Sekretariat<br>Archiwum | Docusafe<br>EXRTRANET | Serwer,<br>Archiwum, | Sekretariat pok. 203<br>Archiwum<br>Serwerownia |
| 2. | Dane kadrowe | Kadry | Płace INFO SYSTEM Roman i Tadeusz Groszek sp.j. | Serwer,<br>Archiwum, | Pok. 204<br>Pok.206, 208 |

| | | | | | |
|---|---|---|---|---|---|
| 3. | Dane ubezpieczonych w ZUS | Referat Finansowy | Płace, INFO SYSTEM Roman i Tadeusz Groszek sp.j.<br>Płatnik ZUS | Serwer,<br>Archiwum, | Pok. 206<br>Pok.208 |
| 4. | Dane płacowe | Referat Finansowy | Płace INFO SYSTEM Roman i Tadeusz Groszek sp.j. | Serwer,<br>Archiwum, | Pok. 206<br>Pok.208 |
| 5. | Dane kontrahentów | Referat Finansowy | Podatki, Budżet, Przelewy INFO SYSTEM Roman i Tadeusz Groszek sp.j. | Serwer,<br>Archiwum, | Pok. 208 |
| 6. | Dane mieszkańców | Sprawy obywatelskie | Źródło;<br>WYBORY+ ELUD+ Radix | Serwer | Pok. 205 |
| 7. | Dane osób uiszczających opłatę za wywóz nieczystości | Finansowy | GOMIG odpady<br>GOMIG integracja | Serwer | Pok.,107<br>206,107 |
| 8 | Dane mieszkańców | Kasa | KASA System obsługi kasy | Serwer | Pok. 109 |
| 9. | Dane właścicieli pojazdów | Referat Finansowy | AUTA INFO SYSTEM Roman i Tadeusz Groszek sp.j. | Serwer | Pok. 206 |
| 10. | Dane podatników podatek rolny, leśny od nieruchomości i akcyzowy | Referat Finansowy | Podatki, Budżet, INFO SYSTEM Roman i Tadeusz Groszek sp.j. | Serwer | Pok.206, 204 |

# VI. Środki techniczne i organizacyjne niezbędne dla zapewnienia poufności, integralności i rozliczalności przetwarzania danych

§ 16

1. Zabezpieczenia organizacyjne

   1) sporządzono i wdrożono Politykę Bezpieczeństwa;

   2) sporządzono i wdrożono Instrukcję Zarządzania Systemem Informatycznym

   3) wyznaczono IOD

   4) wyznaczono ASI

   5) do przetwarzania danych zostały dopuszczone wyłącznie osoby posiadające upoważnienia nadane przez Administratora danych bądź osobę przez niego upoważnioną;

   6) stworzono procedurę postępowania w sytuacji naruszenia ochrony danych osobowych;

   7) osoby zatrudnione przy przetwarzaniu danych zostały zaznajomione z przepisami dotyczącymi ochrony danych osobowych oraz w zakresie zabezpieczeń systemu informatycznego;

   8) osoby zatrudnione przy przetwarzaniu danych osobowych obowiązane zostały do zachowania ich w tajemnicy;

   9) przetwarzanie danych osobowych dokonywane jest w warunkach zabezpieczających dane przed dostępem osób nieupoważnionych;

10) przebywanie osób nieuprawnionych w pomieszczeniach, gdzie przetwarzane są dane osobowe jest dopuszczalne tylko w obecności osoby zatrudnionej przy przetwarzaniu danych osobowych oraz w warunkach zapewniających bezpieczeństwo danych;

11) dokumenty i nośniki informacji zawierające dane osobowe, które podlegają zniszczeniu, neutralizuje się za pomocą urządzeń do tego przeznaczonych lub dokonując takiej ich modyfikacji, która nie pozwoli na odtworzenie ich treści, aby po dokonaniu usunięcia danych niemożliwa była identyfikacja osób.

2. Zabezpieczenia techniczne

1) wewnętrzną sieć komputerową zabezpieczono poprzez odseparowanie od sieci publicznej za pomocą sprzętowego systemu zabezpieczeń FORTIGATE 90 D, który obejmuje :

   a. system wykrywania włamań (IPS)

   b. kontrolę aplikacji

   c. antywirus

   d. firewall

   e. filtrowanie sieci

   f. filtrowanie poczty e-mail

   g. szyfrowane połączenia VPN

2) stanowiska komputerowe wyposażono w indywidualną ochronę antywirusową,

3) komputery zabezpieczono przed możliwością użytkowania przez osoby nieuprawnione do przetwarzania danych osobowych, za pomocą indywidualnego identyfikatora użytkowania i cykliczne wymuszanie zmiany hasła,

3. Środki ochrony fizycznej:

   1) obszar, na którym przetwarzane są dane osobowe, poza godzinami pracy, chroniony jest alarmem,

   2) urządzenia służące do przetwarzania danych osobowych umieszcza się w zamykanych pomieszczeniach.

## VII. Instrukcja postępowania w przypadku zagrożeń i incydentów zagrażających bezpieczeństwu danych osobowych

§ 17

1. Instrukcja definiuje katalog zagrożeń i incydentów zagrażających bezpieczeństwu danych osobowych oraz opisuje sposób reagowania na nie. Celem instrukcji jest minimalizacja skutków wystąpienia incydentów bezpieczeństwa, ograniczenie ryzyka powstania zagrożeń i występowania incydentów w przyszłości.

2. Każdy pracownik Urzędu Gminy w przypadku stwierdzenia zagrożenia lub naruszenia ochrony danych osobowych, zobowiązany jest niezwłocznie poinformować Administratora Danych lub IOD.

3. Do typowych zagrożeń bezpieczeństwa danych osobowych należą:

   1) niewłaściwe zabezpieczenie fizyczne pomieszczeń, urządzeń i dokumentów,

   2) niewłaściwe zabezpieczenie sprzętu, oprogramowania przed wyciekiem, kradzieżą i utratą danych osobowych,

   3) nieprzestrzeganie zasad ochrony danych osobowych przez pracowników.

4. Do typowych incydentów zagrożenia bezpieczeństwa danych osobowych należą:

1) zdarzenia losowe zewnętrzne (pożar obiektu/pomieszczenia, zalanie wodą, utrata zasilania, utrata łączności),

2) zdarzenia losowe wewnętrzne (awarie serwera, komputerów, twardych dysków, oprogramowania, pomyłki informatyków, użytkowników, utrata/ zagubienie danych),

3) umyślne incydenty (włamanie do systemu informatycznego lub pomieszczeń, kradzież danych/sprzętu, wyciek informacji, ujawnienie danych osobom nieupoważnionym, świadome zniszczenie dokumentów/danych, działanie wirusów i innego szkodliwego oprogramowania).

5. W przypadku stwierdzenia wystąpienia zagrożenia, Administrator Danych lub IOD prowadzi postępowanie wyjaśniające w toku, którego:

   1) ustala zakres i przyczyny zagrożenia oraz jego ewentualne skutki,

   2) inicjuje ewentualne działania dyscyplinarne,

   3) rekomenduje działania prewencyjne (zapobiegawcze) zmierzające do eliminacji podobnych zagrożeń w przyszłości,

   4) dokumentuje prowadzone postępowania.

6. W przypadku stwierdzenia incydentu (naruszenia), Administrator Danych lub IOD prowadzi postępowanie wyjaśniające w toku, którego:

   1) ustala czas wystąpienia naruszenia, jego zakres, przyczyny, skutki oraz wielkość szkód, które zaistniały,

   2) zabezpiecza ewentualne dowody,

   3) ustala osoby odpowiedzialne za naruszenie,

   4) podejmuje działania naprawcze (usuwa skutki incydentu i ogranicza szkody),

   5) inicjuje działania dyscyplinarne,

6) wyciąga wnioski i rekomenduje działania korygujące zmierzające do eliminacji podobnych incydentów w przyszłości,

7) dokumentuje prowadzone postępowania.

8) Dokonuje zgłoszenia naruszenia danych osobowych do organu nadzorczego PUODO

## VIII. Zadania Administratora Danych i Inspektora Ochrony Danych Osobowych

§ 18

Do najważniejszych obowiązków Administratora Danych lub IOD należy:

1. organizacja bezpieczeństwa i ochrony danych osobowych zgodnie z wymogami ustawy o ochronie danych osobowych,

2. zapewnienie przetwarzania danych zgodnie z uregulowaniami Polityki,

3. wydawanie i anulowanie upoważnień do przetwarzania danych osobowych,

4. prowadzenie ewidencji osób upoważnionych do przetwarzania danych osobowych,

5. prowadzenie postępowania wyjaśniającego w przypadku naruszenia ochrony danych osobowych, prowadzenie postępowania wyjaśniającego w przypadku naruszenia ochrony danych osobowych,

6. nadzór nad bezpieczeństwem danych osobowych,

7. kontrola działań komórek organizacyjnych pod względem zgodności przetwarzania danych z przepisami o ochronie danych osobowych,

8. inicjowanie i podejmowanie przedsięwzięć w zakresie doskonalenia ochrony danych osobowych

§ 19

Inspektor Ochrony Danych (IOD) ma prawo:

1) wyznaczania, rekomendowania i egzekwowania wykonania zadań związanych z ochroną danych osobowych w Urzędzie Gminy Rawa Mazowiecka;

2) wstępu do pomieszczeń w których zlokalizowane są zbiory danych i przeprowadzenia niezbędnych badań lub innych czynności kontrolnych w celu oceny zgodności przetwarzania danych z ustawą;

3) żądania złożenia pisemnych lub ustnych wyjaśnień w zakresie niezbędnym do ustalenia stanu faktycznego;

4) żądania okazania dokumentów i wszelkich danych mających bezpośredni związek z problematyką kontroli;

5) żądania udostępnienia do kontroli urządzeń, nośników oraz systemów informatycznych służących do przetwarzania danych.

# IX. Zadania Administratora Systemu Informatycznego

§ 20

1. Administrator Systemu Informatycznego odpowiedzialny jest za:

   1) Bieżący monitoring i zapewnienie ciągłości działania systemu informatycznego oraz baz danych.

   2) Optymalizację wydajności systemu informatycznego, baz danych, instalacje i konfiguracje sprzętu sieciowego i serwerowego.

   3) Instalacje i konfiguracje oprogramowania systemowego, sieciowego, oprogramowania bazodanowego.

4) Konfigurację i administrowanie oprogramowaniem systemowym, sieciowym oraz bazodanowym zabezpieczającym dane chronione przed nieupoważnionym dostępem.

5) Nadzór nad zapewnieniem awaryjnego zasilania komputerów oraz innych urządzeń mających wpływ na bezpieczeństwo przetwarzania danych.

6) Współpracę z dostawcami usług oraz sprzętu sieciowego i serwerowego oraz zapewnienie zapisów dotyczących ochrony danych osobowych.

7) Zarządzanie kopiami awaryjnymi konfiguracji oprogramowania systemowego, sieciowego.

8) Zarządzanie kopiami awaryjnymi danych osobowych oraz zasobów umożliwiających ich przetwarzanie.

9) Przeciwdziałanie próbom naruszenia bezpieczeństwa informacji.

10) Przyznawanie na wniosek Administratora Danych lub IOD ściśle określonych praw dostępu do informacji w danym systemie.

11) Wnioskowanie do Administratora Danych lub IOD w sprawie zmian lub usprawnienia procedur bezpieczeństwa i standardów zabezpieczeń.

12) Zarządzanie licencjami, procedurami ich dotyczącymi.

13) Prowadzenie profilaktyki antywirusowej.

2. Praca Administratora Systemu Informatycznego jest nadzorowana pod względem przestrzegania ustawy o ochronie danych osobowych oraz Rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 roku 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) Dz.U.UE.L.2016.119.1 – dalej RODO oraz Polityki Bezpieczeństwa przez Administratora danych i IOD.

# X. Sprawozdanie roczne stanu systemu ochrony danych osobowych

§ 21

1. Corocznie do dnia 31 marca IOD lub wyznaczony przez Administratora danych pracownik przygotowuje sprawozdanie roczne stanu funkcjonowania systemu ochrony danych osobowych,
2. W spotkaniu sprawozdawczym uczestniczą: Administrator danych oraz IOD. Na wniosek co najmniej jednego z uczestników w spotkaniu mogą wziąć udział: informatyk, kierownicy działów/jednostek.
3. Sprawozdanie przygotowywane jest w formie pisemnej.

# XI. Szkolenia użytkowników

§ 22

1. Każdy użytkownik przed dopuszczeniem do pracy z systemem informatycznym przetwarzającym dane osobowe lub zbiorami danych osobowych w wersji papierowej winien być poddany przeszkoleniu w zakresie ochrony danych osobowych w zbiorach elektronicznych i papierowych.
2. Za przeprowadzenie szkolenia odpowiedzialny jest IOD.
3. Zakres szkolenia powinien obejmować zaznajomienie użytkownika z przepisami ustawy o ochronie danych osobowych oraz wydanymi na jej podstawie aktami wykonawczymi oraz instrukcjami obowiązującymi u Administratora Danych, a także o zobowiązaniu się do ich przestrzegania.

4. Szkolenie zostaje zakończone podpisaniem przez słuchacza oświadczenia o wzięciu udziału w szkoleniu i jego zrozumieniu oraz zobowiązaniu się do przestrzegania przedstawionych w trakcie szkolenia zasad ochrony danych osobowych.

5. Dokument ten jest przechowywany w aktach osobowych użytkowników i stanowi podstawę do podejmowania działań w celu nadania im uprawnień do korzystania z systemu informatycznego przetwarzającego dane osobowe.

# XII. Postanowienia końcowe

§ 23

1. Polityka jest dokumentem wewnętrznym i nie może być udostępniania osobom postronnym w żadnej formie.

2. Administrator Danych lub IOD ma obowiązek zapoznać z treścią Polityki każdego użytkownika.

3. Wszystkie regulacje dotyczące systemów informatycznych, określone w Polityce dotyczą również przetwarzania danych osobowych w bazach prowadzonych w jakiejkolwiek innej formie.

4. Użytkownicy zobowiązani są do stosowania przy przetwarzaniu danych osobowych postanowień zawartych w Polityce.

5. Wobec osoby, która w przypadku naruszenia zabezpieczeń systemu informatycznego lub uzasadnionego domniemania takiego naruszenia nie podjęła działania określonego w niniejszym dokumencie, a w szczególności nie powiadomiła odpowiedniej osoby zgodnie z określonymi zasadami, a także, gdy nie zrealizowała stosownego działania dokumentującego ten przypadek, można wszcząć postępowanie dyscyplinarne.

6. Kara dyscyplinarna orzeczona wobec osoby uchylającej się od powiadomienia nie wyklucza odpowiedzialności karnej tej osoby, zgodnie z ustawą oraz możliwości wniesienia wobec niej sprawy z powództwa cywilnego przez pracodawcę o zrekompensowanie poniesionych strat.

7. W sprawach nieuregulowanych w Polityce mają zastosowanie przepisy ustawy o ochronie danych oraz rozporządzenia.