ZATWIERDZAM

Wójt Gminy Grzegorzew
/-/ Bożena Dominiak

POLITYKA BEZPIECZEŃSTWA PRZETWARZANIA DANYCH OSOBOWYCH w Urzędzie Gminy Grzegorzew

Administrator Bezpieczeństwa Informacji

/-/ Janusz Poronin

SPIS TREŚCI : str.

I. POSTANOWIENIA OGÓLNE

1. **Polityka bezpieczeństwa** została opracowana w związku z wymaganiami zawartymi w ustawie z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (Dz. U. z 2016 r. poz. 922) 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.

Ponadto opracowana Polityka bezpieczeństwa uwzględnia przepisy:

- Rozporządzenie Ministra Administracji i Cyfryzacji z dnia 11 maja 2015r. w sprawie trybu i sposobu realizacji zadań w celu zapewniania przestrzegania przepisów o ochronie danych osobowych przez administratora bezpieczeństwa informacji (Dz.U. z 2016 r., poz. 745),
- Rozporządzenie Ministra Administracji i Cyfryzacji z dnia 11 maja 2015 r. w sprawie sposobu prowadzenia przez administratora bezpieczeństwa informacji rejestru zbiorów danych (Dz. U. z 2016 r. ,poz.719,
- Rozporządzenie Ministra Administracji i Cyfryzacji z dnia 10 grudnia 2014 r., w sprawie wzorów zgłoszeń powołania i odwołania administratora bezpieczeństwa informacji, (Dz.U. z 2014 r. ,poz.1934).

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

II. SŁOWNIK TERMINÓW

1. . Ilekroć w Polityce jest mowa o :

1) **Jednostka organizacyjna** – rozumie się przez to Urząd Gminy w Grzegorzewie ;

2) **Ustawa** – należy przez to rozumieć ustawę z dnia 29 sierpnia 1997 r. o ochronie danych osobowych ;

3) **zbiorze 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;

4) **danych osobowych** - rozumie się przez to wszelkie informacje dotyczące zidentyfikowanej lub możliwej do zidentyfikowania osoby fizycznej;
Osobą możliwą do zidentyfikowania jest osoba, której tożsamość można określić bezpośrednio lub pośrednio, w szczególności przez powołanie się na numer identyfikacyjny albo jeden lub kilka specyficznych czynników określających jej cechy fizyczne, fizjologiczne, umysłowe, ekonomiczne, kulturowe lub społeczne.
Informacji nie uważa się za umożliwiającą określenie tożsamości osoby, jeżeli wymagałoby to nadmiernych kosztów, czasu lub działań;

5) **przetwarzaniu 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;
6) **systemie informatycznym** - rozumie się przez to zespół współpracujących ze sobą urządzeń, programów, procedur przetwarzania informacji i narzędzi programowych zastosowanych w celu przetwarzania danych osobowych;

7) **systemie tradycyjnym** - rozumie się przez to zespół procedur organizacyjnych, związanych z mechanicznym przetwarzaniem informacji i wyposażenia i środków trwałych w celu przetwarzania danych osobowych w formie papierowej;

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

9) **usuwaniu danych** - rozumie się przez to zniszczenie danych osobowych lub taką ich modyfikację, która nie pozwoli na ustalenie tożsamości osoby, której dane dotyczą;

10) **Administratorze Danych Osobowych** zwanym też **Administratorem Danych (ADO)** - w świetle ustawy o ochronie danych osobowych rozumie się przez to kierownika jednostki który decyduje o celach i środkach przetwarzania danych osobowych;

11) **Administratorze Bezpieczeństwa Informacji** zwanym też **Administratorem Bezpieczeństwa (ABI)**- rozumie się przez to osobę wyznaczoną przez Wójta Gminy Grzegorzew, zgłoszonego do Krajowego Rejestru ABI prowadzonego przez GIODO, 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;

12) **GIODO** – Generalny Inspektor Ochrony Danych Osobowych – organ uprawniony do spraw ochrony danych osobowych;

13) **Administratorze Systemu Informatycznego** zwanym też **Administratorem Systemu (ASI)** - rozumie się przez to osobę zatrudnioną przez kierownika jednostki upoważnioną do realizacji zadań związanych z zarządzaniem systemem informatycznym;

14) **kierownik komórki organizacyjnej –** rozumie się również samodzielne stanowisko pracy,

15) **użytkowniku systemu** zwanym też **użytkownikiem systemu informatycznego** - rozumie się przez to upoważnionego przez Wójta Gminy Grzegorzew , wyznaczonego do przetwarzania danych osobowych w systemie informatycznym pracownika, który odbył szkolenie prowadzone przez ABI w zakresie ochrony tych danych;

16) **zgodzie 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.; zgoda może być w każdej chwili odwołana;

17) **sprawdzenie** – należy przez rozumieć czynności mające na celu weryfikowanie zgodności przetwarzania danych osobowych z przepisami o ochronie danych osobowych;

18) **sprawozdanie** – należy przez to rozumieć dokument , o którym mowa w srt.36c ustawy , opracowany przez administratora bezpieczeństwa informacji po dokonaniu sprawdzenia

III. CELE POLITYKI BEZPIECZEŃSTWA

1. Dane osobowe w Urzędzie Gminy Grzegorzew są gromadzone, przechowywane, edytowane, archiwizowane w kartotekach, skorowidzach, księgach, wykazach zestawieniach oraz w innych zestawach i zbiorach ewidencyjnych poszczególnych komórek organizacyjnych Urzędu Gminy Grzegorzew na dokumentach papierowych, jak również w systemach informatycznych na elektronicznych nośnikach informacji.

2. 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.
3. Celem opracowania Polityki bezpieczeństwa jest ochrona danych osobowych przed niepowołanym dostępem do zgromadzonych i przetwarzanych danych.
4. Procedury i zasady określone w niniejszej Polityce bezpieczeństwa stosuje się do wszystkich pracowników Urzędu Gminy jak i innych osób mających dostęp do danych osobowych przetwarzanych w Urzędzie Gminy Grzegorzew (np. osób realizujących zadania na podstawie umów zlecenia lub o dzieło, wolontariuszy, stażystów, praktykantów, serwisantów).
5. 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.
6. W sytuacji, gdy dane osobowe nie zostały uzyskane od osoby, której dotyczą, to ich przetwarzanie jest zgodne z prawem, gdy przepis szczególny zezwala na przetwarzanie danych osobowych bez zgody osoby , której dane dotyczą.
7. Usunięcie danych nie wymaga zgody osoby, której dotyczą.
8. Ocena niezbędności przetwarzania danych do wypełnienia usprawiedliwionych celów Administratora Danych powinna być dokonywana indywidualnie w każdej sytuacji .
9. 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.

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

11. 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.

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

12. Bezpośredni nadzór nad przetwarzaniem danych osobowych sprawują Kierownicy komórek organizacyjnych.

13. Z zasadami w Polityce bezpieczeństwa obowiązkowo są zapoznawani wszyscy użytkownicy systemów tradycyjnych i informatycznych, składając odpowiednie oświadczenie, którego wzór stanowi załącznik Nr 1 do Polityki.

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

14. Do informacji przechowywanych w systemach tradycyjnych jak i informatycznych mają dostęp jedynie upoważnieni pracownicy Urzędu Gminy Grzegorzew oraz osoby mające imienne zarejestrowane upoważnienie, którego wzór stanowi załącznik Nr 2, 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 komórek organizacyjnych Urzędu Gminy Grzegorzew*;*

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

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

Wzór ewidencji stanowi załącznik Nr 3 do Polityki bezpieczeństwa.

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

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

IV. ADMINISTRACJA I ORGANIZACJA BEZPIECZEŃSTWA

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

2. Kierownicy komórek organizacyjnych 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.

3.Administrator Danych Osobowych powołał Administratora Bezpieczeństwa Informacji, nadzorującego przestrzeganie zasad ochrony. Prowadzi on dokumentację opisującą sposób przetwarzania danych oraz środków technicznych i organizacyjnych zapewniających ochronę przetwarzanych danych osobowych.

4. Administrator bezpieczeństwa informacji został zgłoszony do Krajowego Rejestru ABI prowadzonego przez GIODO;

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

20. 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.

21. Administrator Bezpieczeństwa Informacji prowadzi bieżącą wykaz osób upoważnionych do przetwarzania danych osobowych.

22. 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,

/administrator danych jest zobowiązany zastosować środki techniczne i organizacyjne zapewniające ochronę przetwarzanych danych osobowych odpowiednia do zagrożeń oraz kategorii danych objętych ochroną ,a w szczególności powinien zabezpieczyć dane przed ich udostępnieniem osobom nieupoważnionym, zabraniem przez osobę nieuprawnioną, przetwarzaniem z naruszeniem ustawy oraz zmianą , utratą, uszkodzeniem lub zniszczeniem/.

c) zapewnianie zapoznania osób upoważnionych do przetwarzania danych osobowych z przepisami o ochronie danych osobowych (szkolenia);

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 – sprawdzenia planowe w zakresie bezpieczeństwa;

9) prowadzi postępowanie wyjaśniające w przypadku naruszenia ochrony danych osobowych,
10) przygotowuje wnioski pokontrolne dla Administratora Danych Osobowych,
11) prowadzi rejestr zbiorów danych osobowych przetwarzanych przez administratora danych.

23. 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.

24. 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.

25. 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.

11. Kierownik komórki organizacyjnej 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,
4) wnioskuje o nadanie upoważnień do przetwarzania danych osobowych pracownikom,
5) zgłasza potrzeby w zakresie zabezpieczenia danych osobowych w Urzędzie Gminy Grzegorzew .

12. 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.

V. WYKAZ ZBIORÓW DANYCH OSOBOWYCH

1. Dane osobowe są gromadzone, przechowywane i przetwarzane w kartotekach, skorowidzach, księgach, wykazach oraz w innych zbiorach ewidencyjnych poszczególnych komórek organizacyjnych jednostki organizacyjnej w postaci dokumentów papierowych i w systemie informatycznym, w którym stosowane są pakiety biurowe lub wyspecjalizowane aplikacje (programy).

2. Zestawienie zbiorów danych osobowych stanowi załącznik Nr 4 do polityki bezpieczeństwa.

3. Ze względu na rodzaj i charakter danych osobowych zawartych w zbiorach, w Urzędzie Gminy Grzegorzew 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.

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

VI. SPOSÓB PRZEPŁYWU DANYCH POMIĘDZY POSZCZEGÓLNYMI SYSTEMAMI

1. Obieg dokumentów zawierających dane osobowe, pomiędzy komórkami organizacyjnymi jednostki , 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 i sieci zewnętrznych (Plus , Era , Orange , Play, pozostałe sieci komórkowe, WiFi , itp.).

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

1. Dostęp do danych wprowadzonych przez użytkowników systemów informatycznych mają jedynie upoważnione osoby oraz Administrator Bezpieczeństwa Informacji 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.

VIII. PRAWO DO KONTROLI DANYCH OSOBOWYCH

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.

3. 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 .

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

4. 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.

5. Każda z osób zatrudnionych przy przetwarzaniu danych w razie powzięcia takie wiadomości ma obowiązek o wystąpieniu osoby, której dane dotyczą, poinformować ABI.

6. Do udostępniania posiadanych w zbiorze danych osobowych upoważniony jest kierownik jednostki lub pracownik posiadający wymagane prawem upoważnienie.

7. 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.

8. 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.

IX. ZACHOWANIE BEZPIECZEŃSTWA

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

2. Wszyscy użytkownicy systemu muszą stosować się do obowiązujących procedur bezpieczeństwa.

3. 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.

X. BEZPIECZEŃSTWO FIZYCZNE

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 niepowołanemu dostępowi do informacji, nieautoryzowanym operacjom w systemie, kontroli dostępu do zasobów oraz w celu zabezpieczenia sprzętu teleinformatycznego.

3 .Obszar systemów informatycznych w Urzędu Gminy Grzegorzew
obejmuje wszystkie pomieszczenia budynku: Urzędu Gminy przy Placu 1000-lecia Państwa Polskiego 1 , 62-640 Grzegorzew;

4. 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.

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

XI. BEZPIECZEŃSTWO SPRZĘTU I OPROGRAMOWANIA

1. 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.

2. 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 komórki organizacyjnej.

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

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

5. Każdorazowo po dokonaniu przetworzenia aplikacja powinna być zamknięta.

6.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.

7. Elektroniczne bazy danych osobowych są archiwizowane. Kopie są wykonywane na nośnikach magnetycznych.

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

XII. KONSERWACJE I NAPRAWY

1. Każde urządzenie użytkowane w systemie informatycznym, powinno podlegać rutynowym czynnościom konserwacyjnym oraz przeglądom wykonywanym przez uprawnione osoby.
2. Za konserwację oprogramowania systemowego oraz aplikacyjnego serwera systemu informatycznego odpowiedzialny jest Administrator Systemu Informatycznego. Konserwacja oprogramowania obejmuje także jego aktualizację.

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

4. 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.

XIII. PLANY AWARYJNE I ZAPOBIEGAWCZE

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

2. 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 magnetooptycznych, i przechowywane są przez Administratora Systemu Informatycznego. Użycie kopii zapasowych następuje na polecenie Administratora Systemu Informatycznego w przypadku odtwarzania systemu po awarii.

XIV. POLITYKA ANTYWIRUSOWA

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.

3. W przypadku jakichkolwiek wątpliwości odnośnie zagrożenia wirusowego należy sprawdzić zawartość całego dysku twardego programem antywirusowym. W przypadku dalszych niejasności należy kontaktować się z administratorem Systemu Informatycznego.

XV. SPRAWDZENIA I SPRAWOZDANIA

1. Administrator Bezpieczeństwa Informacji dokonuje sprawdzania zgodności przetwarzania danych osobowych z przepisami o ochronie danych osobowych oraz opracowuje sprawozdanie,
2. Sprawdzenie jest dokonywane dla:
   1) Administratora danych ,
   2) Generalnego Inspektora Ochrony Danych Osobowych jeżeli GIODO wystąpi o przeprowadzenie sprawdzenia,
3. Sprawdzenie jest przeprowadzane w trybie:
   1) sprawdzenia planowego – według planu sprawdzeń,
   2) sprawdzenia doraźnego – w przypadku nieprzewidzianym w planie sprawdzeń planowych , w sytuacji powzięcia przez administratora bezpieczeństwa informacji wiadomości o naruszeniu ochrony danych osobowych lub uzasadnionego podejrzenia wystąpienia takiego naruszenia,
   3) w przypadku zwrócenia się o dokonanie sprawdzenia przez Generalnego Inspektora.
4. Plan sprawdzeń określa przedmiot , zakres oraz termin przeprowadzenia poszczególnych sprawdzeń oraz sposób i zakres ich dokumentowania.
5. Administrator bezpieczeństwa informacji w planie sprawdzeń uwzględnia w szczególności zbiory danych osobowych i systemy informatyczne służące do przetwarzania danych osobowych oraz konieczność weryfikacji zgodności przetwarzania danych osobowych :

1) z zasadami i podstawami określonymi w przepisach ustawy,
2) z zasadami dotyczącymi zabezpieczenia danych osobowych ,
3) z zasadami przekazywania danych osobowych,
4) z obowiązkiem zgłoszenia zbioru danych do rejestracji i jego aktualizacji , jeżeli zbiór zawiera dane podlegające szczególnej ochronie wymienionymi w art.27 ustawy.

6. Plan sprawdzeń jest przygotowywany przez administratora bezpieczeństwa informacji na okres nie krótszy niż kwartał i nie dłuższy niż rok. Plan sprawdzeń jest przedstawiany Wójtowi Gminy Grzegorzew nie później niż dwa tygodnie przed dniem rozpoczęcia okresu objętemu planem.
7. Plan sprawdzeń obejmuje co najmniej jedno sprawdzenie,
8. Zbiory danych oraz systemy informatyczne służące do przetwarzania lub zabezpieczania danych osobowych powinny być objęte sprawdzeniem co najmniej raz na 5 lat.
9. Sprawdzenie doraźne jest przeprowadzane niezwłocznie po powzięciu wiadomości przez administratora bezpieczeństwa informacji o naruszeniu ochrony danych osobowych lub uzasadnionym podejrzeniu takiego naruszenia.
10. Administrator bezpieczeństwa informacji zawiadamia Wójta Gminy Grzegorzew o rozpoczęciu sprawdzenia doraźnego przed podjęciem pierwszej czynności w toku sprawdzenia.
11. Administrator bezpieczeństwa informacji dokumentuje czynności przeprowadzone w toku sprawdzenia w zakresie niezbędnym do oceny zgodności przetwarzania danych osobowych z przepisami o ochronie danych osobowych .
12. Dokumentowanie czynności w toku sprawdzenia może polegać , w szczególności ,na utrwaleniu danych z systemu informatycznego służącego do przetwarzania lub zabezpieczeniu danych na informatycznym nośniku danych lub dokonaniu wydruku tych danych oraz na:
    1) sporządzeniu notatki z czynności , w szczególności z zebranych wyjaśnień , przeprowadzonych oględzin oraz z czynności związanych z dostępem do urządzeń,

nośników oraz systemów informatycznych służących do przetwarzania danych osobowych ;

2) odebraniu wyjaśnień osoby , której czynności objęto sprawdzeniem;
3) sporządzeniem kopii otrzymanego dokumentu,
4) sporządzeniu kopii obrazu wyświetlonego na ekranie urządzenia stanowiącego część systemu informatycznego służącego do przetwarzania lub zabezpieczania danych osobowych;
5) sporządzanie kopii zapisów rejestrów systemu informatycznego służącego do przetwarzania danych osobowych lub zapisów konfiguracji technicznych środków zabezpieczeń systemu.

13. W systemie informatycznym służącym do przetwarzania danych osobowych lub ich zabezpieczaniu czynności administratora bezpieczeństwa informacji mogą być wykonywane przy udziale osób upoważnionych do przetwarzania danych osobowych , w szczególności osoby zarządzającej tym systemem..
14. Materiały są sporządzane w postaci papierowej lub w postaci elektronicznej.
15. Osoba odpowiedzialna za przetwarzanie danych osobowych , której dotyczy sprawdzenie bierze udział w sprawdzeniu lub umożliwia administratorowi bezpieczeństwa informacji przeprowadzenie czynności w toku sprawdzenia.
16. Administrator bezpieczeństwa informacji zawiadamia Wójta Gminy Grzegorzew o zakresie planowanych czynności w terminie co najmniej 7 dni przed dniem przeprowadzenia czynności , zawiadomienia nie przekazuje się w przypadku:
    1) sprawdzenia doraźnego , jeżeli niezwłoczne rozpoczęcie sprawdzenia jest niezbędne do przywrócenia stanu zgodnego z prawem lub weryfikacji , czy naruszenie miało miejsce;
    2) sprawdzenia , o którego dokonanie zwrócił się Generalny Inspektor , jeżeli na zawiadomienie nie pozwala wyznaczony przez niego termin;
    3) jeżeli Wójt Gminy Grzegorzew posiada informację o których mowa w pkt.2.

17. Po zakończeniu sprawdzenia administrator bezpieczeństwa informacji przygotowuje sprawozdanie .

18. Sprawozdanie jest sporządzane w postaci elektronicznej albo papierowej.
19. Administrator bezpieczeństwa informacji przekazuje sprawozdanie Wójtowi Gminy Grzegorzew:
    1) ze sprawdzenia planowego – nie później niż w terminie 30 dni od zakończenia sprawdzenia;
    2) ze sprawdzenia doraźnego – niezwłocznie po zakończeniu sprawdzenia;
    3) ze sprawdzenia , o które go dokonanie zwrócił się Generalny Inspektor – zachowując terminy wskazane przez GIODO.

XVI. TRYB I SPOSÓB NADZORU NAD DOKUMENTACJĄ

1. Nadzór administratora bezpieczeństwa informacji nad opracowaną dokumentacja polega na opracowaniu i aktualizacji dokumentacji opisującej sposób przetwarzania danych osobowych oraz środki techniczne i organizacyjne zapewniające ochronę przetwarzanych danych osobowych odpowiednią do zagrożeń oraz kategorii danych objętych ochroną poprzez weryfikację
    1) opracowania i kompletności dokumentacji przetwarzania danych ;
    2) zgodności dokumentacji przetwarzania danych z obowiązującymi przepisami prawa;
    3) stanu faktycznego w zakresie przetwarzania danych osobowych,
    4) zgodności ze stanem faktycznym przewidzianych w dokumentacji przetwarzania danych osobowych , środków technicznych i organizacyjnych służących przeciwdziałaniu zagrożeniom dla ochrony danych osobowych;
    5) przestrzegania zasad i obowiązków określonych w dokumentacji przetwarzania danych.
2. Administrator bezpieczeństwa informacji w Urzędzie Gminy Grzegorzew może przeprowadzić weryfikacje poza sprawdzeniem planowym na podstawie zgłoszenia osoby trzeciej. W przypadku wykrycia podczas weryfikacji nieprawidłowości administrator bezpieczeństwa informacji :
    1) zawiadamia Wójta Gminy Grzegorzew o nieopracowaniu lub brakach w dokumentacji przetwarzania danych lub jej elementach oraz działaniach

podjętych w celu doprowadzenia dokumentacji do wymaganego stanu, w szczególności może przedstawić mu do wdrożenia projekty dokumentów usuwające stan niezgodności;

2) zawiadamia Wójta Gminy Grzegorzew o nieaktualności dokumentacji przetwarzania danych osobowych oraz może przedstawić do wdrożenia projekty dokumentów aktualizujących ;
3) poucza lub instruuje osobę nieprzestrzegającą zasad określonych w dokumentacji przetwarzania danych osobowych o prawidłowym sposobie ich realizacji lub zawiadamia Wójta Gminy Grzegorzew , wskazując osobę odpowiedzialną za naruszenie tych zasad praz jego zakres.
4) zawiadomienia mogą być zawarte w sprawozdaniu albo odrębnym dokumencie;
5) wzór planu sprawdzenia planowego stanowi załącznik do niniejszej Polityki,
6) wzór sprawozdania dla Wójta Gminy Grzegorzew stanowi załącznik do niniejszej Polityki.

XVII. PRZEPISY KOŃCOWE

1. 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.

W sprawach nie uregulowanych w niniejszej Polityce bezpieczeństwa informacji mają zastosowanie przepisy ustawy z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (Dz. U. z 2016r. poz. 922, z późn. 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).

Niniejsza Polityka zostaje wprowadzona zarządzeniem Wójta Gminy Grzegorzew.

Każda Osoba upoważniona do Przetwarzania danych osobowych zobowiązana jest zapoznać się z dokumentem, przed dopuszczeniem do przetwarzania danych oraz złożyć stosowne oświadczenie, potwierdzające znajomość jego treści.

ZAŁĄCZNIKI DO POLITYKI BEZPIECZEŃSTWA PRZETWARZANIA DANYCH OSOBOWYCH

WZORY

1. Załącznik nr 1 - Oświadczenie ,
2. Załącznik nr 2 - Upoważnienie,
3. Załącznik nr 3 - Ewidencja osób upoważnionych,
4. Załącznik nr 4 - Plan sprawdzenia planowego,
5. Załącznik nr 5 - Sprawozdanie,
6. Załącznik nr 6 - Rejestr zbioru,
7. Załącznik nr 7 - Raport ,
8. Załącznik nr 8 - Obszar przetwarzania danych osobowych .