**Załącznik nr 1 do Zarządzenia nr 41/2018 z dnia 25.05.2018 r.**
**Wójta Gminy Trzyciąż w sprawie wprowadzenia Dokumentacji sposobu przetwarzania danych osobowych.**

# Polityka bezpieczeństwa przetwarzania danych osobowych w Urzędzie Gminy w Trzyciążu.

| | | | |
|---|---|---|---|
| Data wydania: | 25.05.2018 r. | Wydanie: | 1 |
| Dokument spełnia wymagania: | • Ustawa z dnia 29.08.1997 o ochronie danych osobowych (Dz.U. z 2016 r. poz.922),<br>• Rozporządzenie Ministra Spraw Wewnętrznych i Administracji z dnia 29.04.2004 r. sprawie dokumentacji przetwarzania danych osobowych oraz warunków technicznych, organizacyjnych, jakim powinny odpowiadać urządzenia i systemy informatyczne służące do przetwarzania danych osobowych (Dz.U. z 2004 r. 100 poz. 1024),<br>• ROZPORZĄDZENIE PARLAMENTU EUROPEJSKIEGO I RADY (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych) | | |

**Trzyciąż, 2018**

## Spis treści:

Niniejsza Polityka bezpieczeństwa, zwana dalej Polityką bezpieczeństwa przetwarzania danych osobowych w Urzędzie Gminy w Trzyciążu, została sporządzona w celu wykazania, że dane osobowe są przetwarzane i zabezpieczone zgodnie z wymogami prawa, dotyczącymi zasad przetwarzania i zabezpieczenia danych w Urzędzie, w tym z Rozporządzeniem Parlamentu Europejskiego i Rady (UE) 2016/679 z 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (dalej RODO).

**1. Definicje**

Ilekroć w niniejszym dokumencie jest mowa o:

1) **Ustawie** – rozumie się przez to ustawię z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (Dz. U. z 2016 poz. 922).
2) **RODO** – rozporządzenie Parlamentu Europejskiego i Rady /UE/ 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE /Dz. Urz. UE.L nr 119, str. 1/.
3) **„Polityce bezpieczeństwa", „dokumencie"** – należy przez to rozumieć „Politykę bezpieczeństwa w zakresie ochrony danych w Urzędzie Gminy w Trzyciążu".
4) **Urząd** – należy przez to rozumieć Urząd Gminy w Trzyciążu.
5) **Administratorze Danych („ADO")** – oznacza organ, jednostkę organizacyjną, podmiot lub osobę decydującą (samodzielnie) o celach i środkach przetwarzania danych.
6) **Inspektor Ochrony Danych („IOD")** – osoba wyznaczona przez administratora danych osobowych, nadzorująca przestrzeganie zasad i wymogów ochrony danych osobowych określonych w RODO i przepisach krajowych.
7) **Danych osobowych** – należy przez to rozumieć wszelkie informacje dotyczące zidentyfikowanej lub możliwej do zidentyfikowania osoby fizycznej.
8) **Zbiorze danych** – należy przez to rozumieć każdy posiadający strukturę zestaw danych o charakterze osobowym, dostępnych według określonych kryteriów, niezależnie od tego, czy zestaw ten jest rozproszony lub podzielony funkcjonalnie.
9) **Danych wrażliwych** – rozumie się przez to dane określone w artykule 27 ustawy, a więc dane ujawniające pochodzenie rasowe lub etniczne, poglądy polityczne, przekonania religijne lub filozoficzne, przynależność wyznaniową, partyjną lub związkową, jak również dane o stanie zdrowia, kodzie genetycznym, nałogach lub życiu seksualnym oraz dane dotyczące skazań, orzeczeń o ukaraniu i mandatach karnych, a także innych orzeczeń wydanych w postępowaniu sądowym lub administracyjnym.
10) **Dokumentacji bezpieczeństwa informacji** – rozumie się przez to dokument Polityki Bezpieczeństwa Danych Osobowych, Instrukcję Zarządzania Systemem Informatycznym oraz pozostałe polityki, regulaminu, procedury, instrukcje, formularze przyjęte do stosowania w Urzędzie, mające na celu wskazanie reguł i zasad postępowania w związku z przetwarzaniem informacji.
11) **Haśle** – rozumie się przez to co najmniej 8-znakowy ciąg znaków literowych, cyfrowych, zawierające wielkie i małe litery oraz znaki specjalne, znany jedynie osobie uprawnionej do pracy w systemie informatycznym.
12) **Incydencie bezpieczeństwa** – rozumie się przez to czynności, zdarzenia, zjawiska naruszające przepisy niniejszej polityki bezpieczeństwa ora pozostałych dokumentów bezpieczeństwa informacji, mogące zagrozić utracie aktywów informacyjnych Urzędu, ich integralności lub dostępności, a także dopuścić do nieuprawnionego dostępu do danych, mogące stanowić sytuację kryzysową.

13) **Przetwarzaniu danych** – rozumie się przez to jakiekolwiek operacje wykonywane na danych osobowych, takie jak zbieranie, wprowadzanie do systemu, przechowywanie, opracowywanie, zmienianie, usuwanie i udostępnianie.
14) **Rozliczalności** - rozumie się przez to właściwość zapewniającą, że działania podmiotu mogą być przypisane w sposób jednoznaczny tylko temu podmiotowi.
15) **Systemie informatycznym** – rozumie się przez to sprzęt komputerowy, oprogramowanie, dane eksploatowane w zespole współpracujących ze sobą urządzeń, programów procedur przetwarzania informacji i narzędzi programowych, w systemie tym pracuje co najmniej jeden komputer centralny i system ten tworzy siec teleinformatyczną.
16) **Użytkowniku** – rozumie się przez to pracownika Urzędu, zatrudnionego na podstawie, umowy o prace, umowy zlecenia, lub innej umowy przewidzianej przepisami prawa oraz osobę odbywającą staż, praktykę studencką, wolontariat, który przetwarza dane osobowe znajdujące się w zbiorach danych.
17) **odbiorca** – osoba fizyczna lub prawna, organ publiczny, jednostka lub inny podmiot, któremu ujawnia się dane osobowe w oparciu m. in. o umowę powierzenia,
18) **strona trzecia** – osoba fizyczna lub prawna, organ publiczny, jednostka lub podmiot inny niż osoba, której dane dotyczą, które z upoważnienia administratora danych osobowych mogą przetwarzać dane osobowe,

## 2. Wprowadzenie

Niniejszy dokument opisuje reguły dotyczące procedur zapewnienia bezpieczeństwa danych osobowych przetwarzanych tradycyjnie (ręcznie) oraz zawartych w systemach informatycznych w Urzędzie Gminy w Trzyciążu.
Opisane reguły określają granice dopuszczalnego zachowania wszystkich użytkowników systemów informatycznych wspomagających pracę Urzędu.
Dokument zwraca uwagę na konsekwencję, jakie mogą ponosić osoby przekraczające określone granice oraz procedury postępowania dla zapobiegania i minimalizowania skutków zagrożeń.

Odpowiednie zabezpieczenie, ochrona przetwarzanych danych oraz niezawodność funkcjonowania są podstawowymi wymogami stawianymi współczesnym systemom informatycznym.

Dokumenty „Polityka bezpieczeństwa w zakresie ochrony danych w Urzędzie Gminy w Trzyciążu". – zwany dalej: „Polityką bezpieczeństwa", „Dokumentem", wskazuje sposób postępowania w sytuacji naruszenia bezpieczeństwa danych osobowych i jest w szczególności przeznaczony dla osób pracujących przy przetwarzaniu danych osobowych w Urzędzie.
Potrzeba opracowania „Polityki bezpieczeństwa" wynika z przepisów **§ 3 i 4** 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 służące do przetwarzania danych osobowych (Dz. U. nr 100, poz. 1024).

## 3. Postanowienia ogólne

3.1 Dokumentacja przetwarzania danych osobowych obejmuje:
a) Politykę Bezpieczeństwa Danych Osobowych,

b) Instrukcję Zarządzania Systemem Informatycznym,
c) Procedurę nadzoru nad incydentami bezpieczeństwa.

3.2 Administratorem Danych Osobowych („ADO") przetwarzanych w Urzędzie Gminy w Trzyciążu jest Wójt.

3.3 W celu sprawnego nadzorowania prawidłowego przetwarzania danych osobowych w Urzędzie Gminy w Trzyciążu, Administrator Danych Osobowych powołuje Inspektora Ochrony Danych (IOD).

3.4 Osobą odpowiedzialną za bezpieczeństwo i utrzymanie ciągłości sieci teleinformatycznych oraz systemów i oprogramowania w Urzędzie Gminy w Trzyciążu jest wyznaczony pracownik.

3.5 Kierownicy Komórek organizacyjnych, pracownicy na samodzielnych stanowiskach pracy w Urzędzie (Zarządzający Zbiorami Danych Osobowych) odpowiadają za: zgłaszanie zmian w obrębie nowych i dotychczasowych zbiorów danych osobowych; wnioskowanie o nadanie, zmianę lub unieważnienie upoważnienia do przetwarzania danych osobowych dla podległych pracowników; zgłaszanie powierzania przetwarzania danych osobowych podmiotom zewnętrznym; przestrzeganie przepisów oraz ustalonych wewnątrz Urzędu zasad przetwarzania danych osobowych.

3.6 Niniejsza Polityka Bezpieczeństwa Danych Osobowych;
a) określa zasady postępowania w związku z przetwarzaniem danych osobowych w Urzędzie Gminy w Trzyciążu,
b) jest zbiorem zasad i procedur obowiązujących przy zbieraniu, przetwarzaniu i wykorzystywaniu danych osobowych we wszystkich zbiorach administrowanych przez Urząd Gminy w Trzyciążu,
c) obowiązuje wszystkich pracowników Urzędu Gminy w Trzyciążu,
d) odnosi się zarówno do przetwarzania danych osobowych w formie papierowej (tradycyjnej) jak i przetwarzanych w systemach informatycznych Urzędu,

3.7 Przetwarzanie danych osobowych w Urzędzie Gminy w Trzyciążu jest dopuszczalne tylko pod warunkiem przestrzegania ustawy z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (Dz. U. z 2016 poz. 922) oraz wydanych na jej podstawie przepisów wykonawczych oraz zarządzeń Wójta.

**4. Organizacja przetwarzania danych osobowych**

4.1 W Urzędzie Gminy w Trzyciążu dopuszcza się przetwarzanie danych osobowych gry:
a) jest to niezbędne dla ochrony żywotnych interesów osoby, której dane dotyczą, a wyrażenie zgody jest niemożliwe, można je przetwarzać do czasu, gdy uzyskanie zgody stanie się możliwe.
b) jest to konieczne w realizacji przepisów prawa.
c) wykonywania zadań dla dobra publicznego, usprawiedliwionych celów realizowanych przez administratorów danych osobowych.
d) osoba, której dotyczą dane wyrazi na to zgodę.

4.2 Dostęp do zbioru danych osobowych oraz ich przetwarzania mają tylko osoby, które posiadają ważne upoważnienie do przetwarzania danych osobowych. Z wnioskiem o upoważnienie pracownika do przetwarzania danych osobowych występuje jego

bezpośredni przełożony. Wzory wniosku oraz upoważnienia określone są w zał. nr 4 do niniejszej Polityki bezpieczeństwa przetwarzania danych osobowych.

4.3 Rejestracja zbiorów danych osobowych.
Dane osobowe przetwarzane przez Administratora Danych gromadzone są w zbiorach danych. Kierownicy komórek organizacyjnych, pracownicy na samodzielnych stanowiskach pracy w Urzędzie, mają obowiązek poinformować ADO/IOD o:

a) planowanym utworzeniu nowego zbioru danych osobowych.
b) Zmianie w obrębie zbioru już zgłoszonego.

Administrator danych nie podejmuje czynności przetwarzania, które mogłyby się wiązać z poważnym prawdopodobieństwem wystąpienia wysokiego ryzyka dla praw i wolności osób. W przypadku planowania takiego działania Administrator wykona czynności określone w art. 35 i nast. RODO.
W przypadku planowania nowych czynności przetwarzania Administrator dokonuje analizy ich skutków dla ochrony danych osobowych oraz uwzględnia kwestie ochrony danych w fazie ich projektowania.
Administrator danych prowadzi rejestr czynności przetwarzania. Wzór rejestru czynności przetwarzania stanowi Załącznik nr 2 do niniejszej polityki.

4.4 Gromadzenie danych osobowych
Pracownicy zatrudnieni przy przetwarzaniu danych osobowych są zobowiązani do przechowywania danych osobowych we właściwych zbiorach.
Dane osobowe przetwarzane w Urzędzie mogą być uzyskiwane w granicach dozwolonych przepisami prawa.
Zbierane dane osobowe mogą być wykorzystywane tylko do celów, w jakich są lub będą przetwarzane. Po ustaniu celu przetwarzania powinny być one usunięte lub przechowywane w postaci uniemożliwiającej identyfikację osób, których dotyczą.

4.5 W Urzędzie zabrania się przetwarzania danych wrażliwych, chyba że pozwalają na to obowiązujące przepisy prawa lub osoba, której powyższe dane dotyczą wyraziła na to pisemną zgodę.

4.6 Udzielanie informacji o przetwarzaniu danych osobowych
ADO ma obowiązek respektować prawa osób, których dane przetwarza. Każda osoba, której dane dotyczą ma prawo do kontroli przetwarzania danych jej dotyczących, a tym samym może nie częściej niż raz na 6 miesięcy skorzystać z prawa do uzyskania od administratora następujących informacji:
- o celu, zakresie i sposobie przetwarzania danych,
- od kiedy przetwarza się w zbiorze jej dane,
- o źródle z jakiego pochodzą dane jej dotyczące,
- o odbiorcach, którym dane są udostępnianie.

W przypadku kiedy do administratora wpłynie wniosek o udostępnienie takowych danych, musi otrzymać ją w nieprzekraczalnym terminie 30 dni od daty wpłynięcia wniosku.

Osoba, której dane dotyczą może również:
- żądać uzupełnienia, zaktualizowania i sprostowania danych, a także zaprzestania ich przetwarzania
O każdym wniosku o udzielenie informacji oraz ewentualnej konieczności sprostowania danych należy powiadomić Inspektora Ochrony Danych.

4.7 Powierzenie przetwarzania danych osobowych
Administrator Danych Osobowych może powierzyć przetwarzanie danych osobowych innemu podmiotowi wyłącznie w drodze umowy zawartej w formie pisemnej, zgodnie z wymogami wskazanymi dla takich umów w art. 28 RODO i tylko jeżeli są to dane, które może ujawnić bez naruszenia dobra osób których dane dotyczą.
Przed powierzeniem przetwarzania danych osobowych Administrator w miarę możliwości uzyskuje informacje o dotychczasowych praktykach procesora dotyczących zabezpieczenia danych osobowych.

4.8 Przekazywanie danych do państwa trzeciego.
Administrator Danych Osobowych nie będzie przekazywał danych osobowych do państwa trzeciego, poza sytuacjami w których następuje to na wniosek osoby, której dane dotyczą.

4.9 Pracownicy, którzy przetwarzają dane osobowe w systemach informatycznych, zobowiązani są do postępowania zgodnie z „Instrukcją Zarządzania Systemem Informatycznym".

4.10 Pracownicy zatrudnieni przy przetwarzaniu danych osobowych są zobowiązani powiadomić IOD o ewentualnych naruszeniach bezpieczeństwa systemu ochrony danych osobowych, tryb postępowania określa procedura zamieszczona w **pkt. 6 „ Naruszenia zasad ochrony danych osobowych".**

4.11 Konsekwencje naruszenia Polityki Bezpieczeństwa Danych Osobowych.
Wobec pracownika, który w przypadku naruszenia zabezpieczeń systemu informatycznego lub uzasadnionego domniemania takiego naruszenia nie podjął działań określonych w niniejszym dokumencie, a w szczególności nie powiadomił ADO lub IOD zgodnie z określonymi zasadami, wszczyna się postępowanie dotyczące odpowiedzialności służbowej oraz karnej zgodnie z ustawą o ochronie danych osobowych oraz przepisami Kodeksu pracy, w szczególności, gdy ten pracownik:

a) przetwarza w zbiorze dane osobowe do których przetwarzania nie jest upoważniony, których przetwarzanie jest zabronione, niezgodne z celem stworzenia zbioru danych.
b) udostępnia lub umożliwia dostęp do danych osobowych osobom nieupoważnionym,
c) nie zgłasza zmian w zakresie przetwarzanych zbiorów danych osobowych,

4.12 Wprowadzanie zmian do organizacji zabezpieczeń
Wprowadzanie, ustanawianie zabezpieczeń mających na celu ochronę danych osobowych musi uwzględniać normy prawne, normy zarządzania bezpieczeństwem informacji oraz pozostałe polityki przyjęte w Urzędzie.

**5. Organizacyjne i techniczne środki ochrony przetwarzanych danych**
5.1 Ochrona fizyczna pomieszczeń służbowych
Dane osobowe przetwarzane są w pomieszczeniach Urzędu Gminy w Trzyciążu w budynku zlokalizowanym w Trzyciążu, nr 99, 32-353 Trzyciąż.
Budynek Urzędu jest zabezpieczony systemem alarmowym oraz monitoringiem wizualnym, a także posiada zamontowane kraty na parterze.
Pomieszczenia, w których przetwarzane są dane, mają zabezpieczone wejścia za pomocą zamków w sposób uniemożliwiający dostęp do nich osób niepowołanych, a pracownicy sprawują nadzór nad powierzonymi kluczami.

5.2 Zabezpieczenia organizacyjne

a) sporządzono i wdrożono Politykę Bezpieczeństwa.
b) sporządzono i wdrożono Instrukcję zarządzania systemem informatycznym służącym do przetwarzania danych osobowych w Urzędzie Gminy w Trzyciążu.
c) wyznaczono IOD.
d) zbiory danych przetwarzane tradycyjnie (ręcznie) po godzinach pracy przechowywane winny być w szafkach zamkniętych (zamki, kłódki). Przetwarzanie danych osobowych w pomieszczeniach publicznie dostępnych musi odbywać się w sposób uniemożliwiający osobom niepowołanym podglądnięcie ich lub kradzież.
e) Kontrolowanie otwierania i zamykania pomieszczeń, w których są przetwarzane dane osobowe, polegające na otwarciu pomieszczenia przez pierwszą osobę, która rozpoczyna pracę oraz zamknięciu pomieszczenia przez ostatnią wychodzącą osobę, jak również zamykanie pomieszczeń na czas nieobecności osób w pomieszczeniu. Klucze należy przekazywać do sekretariatu Urzędu do specjalnej szafki w celu ich zabezpieczenia.
f) do przetwarzania danych zostały dopuszczone wyłącznie osoby posiadające upoważnienia nadane przez ADO bądź osobę przez niego upoważnioną - IOD, a także które zostały zaznajomione z przepisami dotyczącymi ochrony danych osobowych oraz w zakresie zabezpieczeń systemu informatycznego, osoby te zostały również obowiązane do zachowania ich w tajemnicy. Została stworzona procedura postępowania w sytuacji naruszenia ochrony danych osobowych.
g) 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.

5.3 Zabezpieczenie zbiorów przetwarzanych cyfrowo

a) dostęp do zasobów i usług informatycznych.

Stanowiska komputerowe w pomieszczeniach, gdzie przebywać mogą osoby nieupoważnione do przetwarzania danych – w tym danych osobowych (np. interesanci albo inni pracownicy Urzędu) – winny być umieszczone w sposób, który uniemożliwi takim osobom wgląd do tych danych.

W celu zapewnienia dostępu do danych każdy użytkownik systemu komputerowego korzysta z indywidualnego konta. Dostęp do konta możliwy jest po podaniu prawidłowego hasła o długości min. 8 znaków i terminie ważności.

Wymaga się, by w miejscu styku sieci komputerowej urzędowej z siecią publiczną zastosowane były mechanizmy logiczne lub fizyczne, zapewniające separację zasobów informacyjnych Urzędu, uniemożliwiające dostęp osób niepowołanych z zewnątrz do jej zasobów, a także pozwalające na kontrolę przepływających danych.

b) Zabezpieczenia techniczne

1. wewnętrzną sieć komputerową zabezpieczono poprzez odseparowanie od sieci publicznej za pomocą *urządzenie UTM, FireWall*, *Ochrona przed atakami IPS/IDS.*
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,

5.4 Przebywanie na terenie Urzędu
Pracownikom wolno przebywać na terenie Urzędu tylko w wyznaczonych godzinach pracy, a po nich jedynie po zawiadomieniu i uzyskaniu zgody Wójta. Przebywanie w budynku Urzędu w dni wolne od pracy możliwe jest jedynie po uzyskaniu zgody Wójta lub osoby przez niego upoważnionej.

5.5 Postępowanie w przypadku naruszenia bezpieczeństwa informacji.
Wszyscy pracownicy mają obowiązek natychmiastowego zgłaszania zauważonych incydentów oraz zdarzeń potencjalnie niebezpiecznych bezpośredniemu przełożonemu lub Inspektorowi Ochrony Danych.

**6. Naruszenia zasad ochrony danych osobowych**
6.1. W przypadku stwierdzenia naruszenia ochrony danych osobowych Administrator dokonuje oceny, czy zaistniałe naruszenie mogło powodować ryzyko naruszenia praw lub wolności osób fizycznych.

6.2. W każdej sytuacji, w której zaistniałe naruszenie mogło powodować ryzyko naruszenia praw lub wolności osób fizycznych, Administrator zgłasza incydent naruszenia ochrony danych organowi nadzorczemu bez zbędnej zwłoki – jeżeli to wykonalne, nie później niż w terminie 72 godzin po stwierdzeniu naruszenia. Wzór zgłoszenia określa załącznik nr 5 do niniejszej polityki.

6.3. Jeżeli ryzyko naruszenia praw i wolności jest wysokie, Administrator zawiadamia o incydencie także osobę, której dane dotyczą.

6.4. 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.

6.5. Do typowych zagrożeń 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).

**7. Zadania Administratora Danych lub Inspektor Ochrony Danych**
Do najważniejszych obowiązków Administratora Danych lub Inspektora Ochrony danych należy:
7.1. organizacja bezpieczeństwa i ochrony danych osobowych zgodnie z wymogami ustawy o ochronie danych osobowych,
7.2. zapewnienie przetwarzania danych zgodnie z uregulowaniami Polityki,
7.3. wydawanie i anulowanie upoważnień do przetwarzania danych osobowych,
7.4. prowadzenie ewidencji osób upoważnionych do przetwarzania danych osobowych,

7.5. prowadzenie postępowania wyjaśniającego w przypadku naruszenia ochrony danych osobowych, prowadzenie postępowania wyjaśniającego w przypadku naruszenia ochrony danych osobowych,
7.6. nadzór nad bezpieczeństwem danych osobowych,
7.7. kontrola działań komórek organizacyjnych pod względem zgodności przetwarzania danych z przepisami o ochronie danych osobowych,
7.8. inicjowanie i podejmowanie przedsięwzięć w zakresie doskonalenia ochrony danych osobowych

Inspektor Ochrony Danych ma prawo:
1) wyznaczania, rekomendowania i egzekwowania wykonania zadań związanych z ochroną danych osobowych w nazwa podmiotu,
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.

**8. Organizacja obowiązku prowadzenia ewidencji i rejestrów wymaganych przez ustawodawcę oraz dobre praktyki.**

8.1. Wykaz budynków, pomieszczeń lub części pomieszczeń tworzących obszar, w którym przetwarzane są danych osobowe w Urzędzie Gminy w Trzyciążu stanowi załącznik nr 1 do niniejszej Polityki Bezpieczeństwa Danych Osobowych.

8.2. Rejestr czynności przetwarzania ujęty został w załączniku nr 2 do niniejszej Polityki Bezpieczeństwa Danych Osobowych.

8.3. Sposób przepływu danych pomiędzy poszczególnymi systemami ujęty został w załączniku nr 3 do niniejszej Polityki Bezpieczeństwa Danych Osobowych.

8.4. Ewidencja osób upoważnionych do przetwarzania danych osobowych jest prowadzona na bieżąco oraz aktualizowana przez Inspektora Ochrony Danych, stanowi odrębny dokument.

8.5. Wzory upoważnień do przetwarzania danych osobowych stanowią zał. nr 4 do niniejszej Polityki Bezpieczeństwa Danych Osobowych.

8.6. Sprawozdanie ze sprawdzenia zgodności przestrzegania zasad ochrony danych osobowych - wzory sprawozdań wraz z wzorem zgłoszenia incydentu naruszenia ochrony danych osobowych stanowią załącznik nr 5 do niniejszej Polityki Bezpieczeństwa Danych Osobowych.

8.7. Rejestr zbiorów utworzony dnia 14.03.2016 r. przez ABI w sprawie sposobu prowadzenia przez administratora bezpieczeństwa informacji rejestru zbiorów danych osobowych – pozostaje bez zmian.