**Zarządzenie Nr 36/19**

**Wójta Gminy Brudzeń Duży**

**z dnia 30 kwietnia 2019 r.**

**w sprawie wprowadzenia dokumentacji ochrony danych osobowych**

Na podstawie art. 11a ust. 1 pkt 2, art. 31 i art. 33 ust. 3 ustawy z dnia 8 marca 1990 r. o samorządzie gminnym (Dz. U. z 2019 r. poz. 506) oraz art. 24 ust. 1 i 2 rozporządzenia 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) (Dz. Urz. UE L 119 poz. 1), **zarządza się, co następuje**:

**§ 1.**1. Wprowadza się do realizacji w Urzędzie Gminy w Brudzeniu Dużym dokumentację ochrony danych osobowych.

2. Na dokumentację, o której mowa w ust. 1 składa się:
   1) **Polityka bezpieczeństwa** danych osobowych stanowiąca załącznik nr 1 do niniejszego zarządzenia,
   2) **Instrukcja Zarządzania Systemem Informatycznym** stanowiąca załącznik nr 2 do niniejszego zarządzenia.

**§ 2.** Zobowiązuje się pracowników Urzędu Gminy w Brudzeniu Dużym przetwarzających dane osobowe do zapoznania się z powyższymi dokumentami i stosowania w pracy zawartych w nich zasad ochrony danych osobowych.

**§ 3.** Traci moc Zarządzenie Nr 218/18 Wójta Gminy Brudzeń Duży z dnia 23.05.2018 r. w sprawie wprowadzenia Polityki Bezpieczeństwa Informacji.

**§ 4.** Zarządzenie wchodzi w życie z dniem podpisania.

WÓJT
Andrzej Dużyński

Załącznik Nr 1 do Zarządzenia Nr 36/19
Wójta Gminy Brudzeń Duży
z dnia 30 kwietnia 2019 r.

# POLITYKA BEZPIECZEŃSTWA DANYCH OSOBOWYCH

**Urząd Gminy w Brudzeniu Dużym**
ul. Toruńska 2
09-414 Brudzeń Duży

| | |
|---|---|
| **Data i miejsce sporządzenia dokumentu:** | **Brudzeń Duży, dnia 30 kwietnia 2019 r.** |
| **Liczba stron:** | **51** |
| **Zatwierdził:** | WÓJT Andrzej Dwojnych |

# SPIS TREŚCI

# Rozdział 1. Wstęp

1. Niniejszy dokument został opracowany przez Administratora – Wójta Gminy Brudzeń Duży, ul Toruńska 2, 09-414 Brudzeń.
2. Celem opracowania i wdrożenia niniejszej dokumentacji jest zapewnienie zgodności działania Administratora z rozporządzeniem RODO oraz ustawą o ochronie danych osobowych.

## 1.1 Informacje ogólne

1. Dokument Polityki bezpieczeństwa danych osobowych powstał, aby szczegółowo określić środki techniczne i organizacyjne, procedury i zasady, które zapewnią ochronę przetwarzanych, przez Urząd Gminy w Brudzeniu Dużym, danych osobowych przed potencjalnym zagrożeniem. Określenie środków technicznych i organizacyjnych niezbędnych dla zapewnienia poufności, integralności i rozliczalności przetwarzanych danych stanowi **Załącznik nr 1** do niniejszej Polityki bezpieczeństwa.
2. Dokument Polityki bezpieczeństwa ochrony danych osobowych został opracowany w oparciu o wytyczne zawarte w następujących aktach prawnych:
   1) ustawy z dnia 10 maja 2018 r. o ochronie danych osobowych (Dz. U. z 2018 r. poz.1000, poz. 1669);
   2) rozporządzeniu 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) (Dz. Urz. UE L 119 z 04.05.2016, str. 1).
3. Polityka stanowi jeden ze środków organizacyjnych, mających na celu wykazanie, że przetwarzanie danych osobowych odbywa się zgodnie z RODO.
4. Każda osoba mającą dostęp do danych osobowych z upoważnienia Administratora, została zapoznana z niniejszym dokumentem i zobowiązana do jej przestrzegania w zakresie wynikającym z przydzielonych zadań. Dotyczy to w szczególności pracowników w rozumieniu przepisów Kodeksu pracy zatrudnionych przez Administratora, jak również stażystów, praktykantów, osób fizycznych współpracujących z Urzędem Gminy w Brudzeniu Dużym, którzy uzyskują dostęp do danych osobowych w związku ze świadczeniem na rzecz Urzędu usług na podstawie umów cywilnoprawnych.
5. Osoby, o których mowa w ust. 4, składają na piśmie oświadczenie o zachowaniu poufności danych osobowych oraz zobowiązanie do stosowania zawartych w Polityce postanowień, którego wzór stanowi odpowiednio **Załącznik nr 2a i 2b** do niniejszej Polityki bezpieczeństwa.
6. Za nadzorowanie wykonywania zadań wynikających z niniejszej Polityki bezpieczeństwa, jej prowadzenie, przechowywanie (zarówno w wersji papierowej jak i elektronicznej), jak również jej udostępnianie pracownikom odpowiedzialny jest Zastępca Wójta.
7. Polityka bezpieczeństwa danych osobowych podlega przeglądowi pod kątem przydatności, adekwatności i skuteczności, nie rzadziej niż raz do roku. Przeglądu dokonują wspólnie Administrator, Zastępca Wójta oraz Inspektor ochrony danych. Aktualizacja dokumentacji następuje w miarę potrzeb.
8. Wszelkie wątpliwości dotyczące sposobu interpretacji postanowień niniejszego dokumentu, tj. Polityki bezpieczeństwa danych osobowych, powinny być rozstrzygane na korzyść zapewnienia

możliwie najwyższego poziomu ochrony danych osobowych oraz realizacji praw osób, których dane dotyczą.

## 1.2 Zakres informacji objętych polityką

1. Polityka bezpieczeństwa danych osobowych obejmuje wszystkie dane osobowe oraz inne informacje podlegające ochronie, przetwarzane w Urzędzie Gminy w Brudzeniu Dużym, niezależnie od formy ich przetwarzania. Polityka w zakresie danych osobowych odnosi się:
   1) do danych przetwarzanych w zbiorach tradycyjnych (w wersji papierowej), w szczególności w kartotekach, skorowidzach, księgach, wykazach i w innych zbiorach ewidencyjnych,
   2) do danych przetwarzanych w systemach informatycznych.
2. Ma ona pomóc w zapewnieniu: poufności, integralności, dostępności oraz rozliczalności przetwarzanych danych osobowych i innych zidentyfikowanych aktywów informacyjnych.
3. Polityka bezpieczeństwa danych osobowych jest jednocześnie dokumentem określającym zadania osób funkcyjnych, pracowników oraz pracowników i współpracowników podmiotów trzecich, które na mocy zawartych umów mają dostęp do informacji chronionych.
4. Niniejsza Polityka bezpieczeństwa danych osobowych zawiera, w formie załączników, wzory dokumentów uszczegóławiających sposób prowadzenia dokumentacji dotyczącej przetwarzania danych osobowych w Urzędzie, np. instrukcje, wytyczne, tabele.
5. Polityka zawiera następujące załączniki:
   1) Określenie środków technicznych i organizacyjnych niezbędnych dla zapewnienia poufności, integralności i rozliczalności przetwarzanych danych – Załącznik nr 1
   2) Oświadczenie o zobowiązaniu do zachowania poufności – Załącznik 2a i 2b;
   3) Powołanie Administratora Systemów Informatycznych (ASI) – Załącznik nr 3;
   4) Upoważnienie do przetwarzania danych osobowych – Załącznik nr 4;
   5) Ewidencję wydanych upoważnień do przetwarzania danych osobowych – Załącznik nr 5;
   6) Rejestr zbiorów danych osobowych – Załącznik nr 6;
   7) Wykaz zagrożeń mogących prowadzić do naruszeń – Załącznik nr 7;
   8) Wykaz przykładowych zabezpieczeń – Załącznik nr 8;
   9) Arkusz analizy ryzyka – Załącznik nr 9;
   10) Raport z naruszeń zasad bezpieczeństwa ochrony danych osobowych – Załącznik nr 10;
   11) Rejestr naruszeń i incydentów – Załącznik nr 11;
   12) Zgłoszenie naruszenia ochrony danych osobowych organowi nadzorczemu – Załącznik nr 12;
   13) Upoważnienie do zarządzania kluczami oraz kodem cyfrowym do systemu alarmowego – Załącznik nr 13;
   14) Wykaz budynków, pomieszczeń lub części pomieszczeń tworzących obszar, w którym przetwarzane są dane osobowe – Załącznik nr 14;
   15) Wykaz zawartych umów o powierzeniu przetwarzania danych osobowych – Załącznik nr 15;
   16) Rejestr czynności przetwarzania – Załącznik nr 16.

## 1.3 Wyjaśnienie terminów używanych w dokumencie Polityki ochrony danych osobowych

Przez użyte w Polityce określenia należy rozumieć:

1) **ustawa** – rozumie się przez to ustawę z dnia 10 maja 2018 r. o ochronie danych osobowych (Dz. U. z 2018 r. poz. 1000), zwana dalej „ustawą";
2) **RODO** – rozumie się przez to 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) (Dz. Urz. UE L 119 z 04.05.2016, str. 1), zwane dalej „RODO";
3) **Administrator (danych)** - oznacza osobę fizyczną lub prawną, organ publiczny, jednostkę lub inny podmiot, który samodzielnie lub wspólnie z innymi ustala cele i sposoby przetwarzania danych osobowych, w ramach niniejszego dokumentu jest to Wójt Gminy Brudzeń Duży, ul. Toruńska 2, 09-414 Brudzeń Duży;
4) **Administrator Systemów Informatycznych (ASI)** – rozumie się przez to osobę odpowiedzialną za bezpieczeństwo danych osobowych przetwarzanych w systemach informatycznych, w tym w szczególności za przeciwdziałanie dostępowi osób nieupoważnionych do systemów oraz podejmowanie odpowiednich działań w przypadku stwierdzenia naruszeń w tych systemach. Administratora Systemów Informatycznych w Urzędzie Gminy powołuje Wójt;
5) **Inspektor ochrony danych (IOD)** – to osoba wyznaczona przez Administratora w celu informowania i doradzania Administratorowi i pracownikom w zakresie obowiązującego prawa o ochronie danych i niniejszej Polityki oraz w celu monitorowania ich przestrzegania oraz działania jako punkt kontaktowy dla osób przetwarzanych i organu nadzorczego. Inspektor ochrony danych może być członkiem personelu Administratora lub wykonywać zadania na podstawie umowy o świadczenie usług;
6) **Polityka bezpieczeństwa** – rozumie się dokument Polityka bezpieczeństwa danych osobowych wdrożony przez Administratora;
7) **Instrukcja** – Instrukcja zarządzania systemem informatycznym służącym do przetwarzania danych osobowych w Urzędzie Gminy w Brudzeniu Dużym;
8) **dane osobowe** – oznaczają informacje o zidentyfikowanej lub możliwej do zidentyfikowania osobie fizycznej („osobie, której dane dotyczą"); możliwa do zidentyfikowania osoba fizyczna to osoba, którą można bezpośrednio lub pośrednio zidentyfikować, w szczególności na podstawie identyfikatora takiego jak imię i nazwisko, numer identyfikacyjny, dane o lokalizacji, identyfikator internetowy lub jeden bądź kilka szczególnych czynników określających fizyczną, fizjologiczną, genetyczną, psychiczną, ekonomiczną, kulturową lub społeczną tożsamość osoby fizycznej;
9) **zbiór danych** – oznacza uporządkowany zestaw danych osobowych dostępnych według określonych kryteriów, niezależnie od tego, czy zestaw ten jest scentralizowany, zdecentralizowany czy rozproszony funkcjonalnie lub geograficznie;
10) **przetwarzanie danych osobowych** – to dowolna zautomatyzowana lub niezautomatyzowana operacja lub zestaw operacji wykonywanych na danych osobowych lub w zestawach danych osobowych i obejmuje zbieranie, rejestrowanie, organizowanie, strukturyzowanie, przechowywanie, adaptację lub zmianę, wyszukiwanie, konsultacje, wykorzystanie, ujawnianie poprzez transmisję, rozpowszechnianie lub udostępnianie

w inny sposób, wyrównanie lub połączenie, ograniczenie, usunięcie lub zniszczenie danych osobowych;

11) **ograniczenie przetwarzania** – polega na oznaczeniu przetwarzanych danych osobowych w celu ograniczenia ich przyszłego przetwarzania;
12) **odbiorca** – oznacza osobę fizyczną lub prawną, organ publiczny, jednostkę lub inny podmiot, któremu ujawnia się dane osobowe, niezależnie od tego, czy jest stroną trzecią;
13) **podmiot przetwarzający (procesor)** – to osoba fizyczna lub prawna, organ publiczny, agencja lub jakikolwiek inny organ przetwarzający dane osobowe w imieniu Administratora;
14) **uwierzytelnianie** – działanie, którego celem jest weryfikacja deklarowanej tożsamości podmiotu;
15) **użytkownik systemu lub osoba upoważniona** – osoba dopuszczona do obsługi systemu informatycznego oraz urządzeń wchodzących w jego skład, służących do przetwarzania danych osobowych, która posiada aktualne, imienne upoważnienie wydane przez Administratora;
16) **szczególne kategorie danych osobowych** – ujawniają pochodzenie rasowe lub etniczne, poglądy polityczne, przekonania religijne lub filozoficzne, członkostwo w związkach zawodowych i obejmują przetwarzanie danych genetycznych, dane biometryczne w celu jednoznacznej identyfikacji osoby fizycznej, dane dotyczące zdrowia, dane dotyczące naturalnego życie seksualne osoby lub orientację seksualną. W zależności od obowiązującego prawa, specjalne kategorie danych osobowych mogą również zawierać informacje o środkach zabezpieczenia społecznego lub postępowaniach administracyjnych i karnych oraz o sankcjach;
17) **naruszenie ochrony danych osobowych** – jest to przypadkowy lub niezgodny z prawem incydent prowadzący do zniszczenia, utracenia, zmodyfikowania, nieuprawnionego ujawnienia lub nieuprawnionego dostępu do danych osobowych;
18) **organ nadzorczy** – rozumie się przez to Prezesa Urzędu Ochrony Danych Osobowych, ul. Stawki 2, 00-193 Warszawa.

# ROZDZIAŁ 2. Osoby odpowiedzialne za ochronę danych osobowych

## 2.1 Informacje ogólne

Za przetwarzanie danych osobowych oraz ich ochronę zgodnie z postanowieniami rozporządzenia RODO, ustawy, Polityki bezpieczeństwa danych osobowych w Urzędzie Gminy w Brudzeniu Dużym oraz Instrukcji Zarządzania Systemem Informatycznym odpowiadają:

1) Administrator – Wójt Gminy Brudzeń Duży;
2) Zastępca Wójta;
3) Inspektor ochrony danych (IOD);
4) Administrator Systemów Informatycznych (ASI);
5) Kierownicy Referatów Urzędu Gminy w Brudzeniu Dużym;
6) Każda osoba wykonująca pracę bądź świadcząca usługi cywilnoprawne na rzecz Administratora, która uzyskała upoważnienie do przetwarzania danych osobowych.

## 2.2 Administrator

**1.** Administratorem w Urzędzie Gminy w Brudzeniu Dużym, ul. Toruńska 2, 09-414 Brudzeń Duży jest Wójt Gminy.
**2.** Administrator wyznacza Inspektora ochrony danych (IOD) oraz powołuje Administratora Systemów Informatycznych (ASI).
**3.** Administrator nadzoruje działania IOD, Zastępcy Wójta oraz ASI oraz wydaje im zalecenia, co do sposobu wykonywania obowiązków wynikających z niniejszej Polityki bezpieczeństwa.
**4.** Administrator jest odpowiedzialny za przestrzeganie przepisów RODO i musi być w stanie wykazać ich przestrzeganie (tzw. zasada „rozliczalności"). Administrator zapewnia:

1) przetwarzanie danych osobowych zgodnie z prawem, rzetelnie i w sposób przejrzysty dla osoby, której dane dotyczą („zgodność z prawem, rzetelność i przejrzystość"),
2) zbieranie danych osobowych w konkretnych, wyraźnych i prawnie uzasadnionych celach i nieprzetwarzane dalej w sposób niezgodny z tymi celami; dalsze przetwarzanie do celów archiwalnych w interesie publicznym, do celów badań naukowych lub historycznych lub do celów statystycznych nie jest uznawane za niezgodne z pierwotnymi celami („ograniczenie celu");
3) adekwatność danych osobowych; dane osobowe powinny być stosowne oraz ograniczone do tego, co niezbędne do celów, w których są przetwarzane („minimalizacja danych");
4) prawidłowość danych osobowych i w razie potrzeby ich uaktualnianie; podejmuje wszelkie rozsądne działania, aby dane osobowe, które są nieprawidłowe w świetle celów ich przetwarzania, zostały niezwłocznie usunięte lub sprostowane („prawidłowość");
5) przechowywanie danych osobowych w formie umożliwiającej identyfikację osoby, której dane dotyczą, przez okres nie dłuższy, niż jest to niezbędne do celów, w których dane te są przetwarzane; dane osobowe można przechowywać przez okres dłuższy, o ile będą one przetwarzane wyłącznie do celów archiwalnych w interesie publicznym, do celów badań naukowych lub historycznych lub do celów statystycznych, z zastrzeżeniem że wdrożone zostaną odpowiednie środki techniczne i organizacyjne wymagane na mocy niniejszego rozporządzenia w celu ochrony praw i wolności osób, których dane dotyczą („ograniczenie przechowywania");
6) przetwarzanie w sposób zapewniający odpowiednie bezpieczeństwo danych osobowych, w tym ochronę przed niedozwolonym lub niezgodnym z prawem przetwarzaniem oraz przypadkową utratą, zniszczeniem lub uszkodzeniem, za pomocą odpowiednich środków technicznych lub organizacyjnych („integralność i poufność");
7) wykonanie tzw. obowiązku informacyjnego (art. 12, 13, 14 RODO) wraz ze wskazaniem, wobec osób, których dane są przetwarzane przez Administrator, ich praw (np. prawa dostępu do danych, przenoszenia, sprostowania, usunięcia, ograniczenia przetwarzania, sprzeciwu, odwołania zgody);
8) opracowanie klauzul informacyjnych dla powyższych osób.

Ponadto Urząd zawarł umowy powierzenia z podmiotami przetwarzającymi (art. 28 RODO).
**5.** Administrator wdraża odpowiednie środki techniczne i organizacyjne, aby przetwarzanie odbywało się zgodnie z rozporządzeniem RODO, tzn. aby przetwarzane były wyłącznie te dane osobowe, które są niezbędne dla osiągnięcia każdego konkretnego celu przetwarzania. Środki te są poddawane przeglądom i uaktualniane.

## 2.3 Zastępca Wójta

**1.** Zastępca Wójta Gminy Brudzeń Duży nadzoruje wykonywanie w Urzędzie Gminy zadań wynikających z rozporządzenia RODO, ustawy, Polityki bezpieczeństwa danych osobowych w Urzędzie Gminy w Brudzeniu Dużym oraz Instrukcji Zarządzania Systemem Informatycznym, w szczególności:

1) nadzoruje treść Polityki bezpieczeństwa i Instrukcji;
2) prowadzi nadzór nad fizycznym i organizacyjnym zabezpieczeniem obszarów, w których przetwarzane są dane osobowe;
3) monitoruje działanie i skuteczność zabezpieczeń wdrożonych w celu ochrony danych osobowych;
4) opiniuje w sprawach możliwości oraz prawidłowości zbierania danych osobowych w celu utworzenia zbioru danych osobowych, zbierania nowych kategorii danych do istniejącego już zbioru lub przetwarzania danych w innym celu niż ten, dla którego dane zostały zebrane;
5) opiniuje w sprawach konieczności i stosowanej formie wykonywania obowiązku informacyjnego;
6) wydaje pisemne zalecenia wszelkim osobom przetwarzającym dane osobowe celem przetwarzania ich zgodnie z ustawą, rozporządzeniem, Polityką bezpieczeństwa, Instrukcją;
7) nadzoruje wdrażanie w Urzędzie nowych rozwiązań w zakresie zabezpieczenia danych osobowych;
8) organizuje lub zleca pracownikom Urzędu udział w szkoleniach dotyczących przetwarzania i ochrony danych osobowych;
9) wypełnia obowiązki kontrolne i naprawcze w sytuacjach naruszenia zasad bezpieczeństwa ochrony danych osobowych;
10) nadzoruje pracę Kierowników Referatu pod względem bezpieczeństwa ochrony danych;
11) wykonuje inne czynności przewidziane w niniejszej Polityce bezpieczeństwa.

**2.** Zastępca Wójta jest zobowiązany do współpracy z Administratorem, IOD, ASI, Kierownikami Referatów w zakresie nadawania, przygotowywania, rejestrowania, zbierania, ewidencjonowania i przechowywania:

1) imiennych upoważnień osób do przetwarzania danych osobowych;
2) ewidencji wydanych upoważnień do przetwarzania danych osobowych w Urzędzie;
3) oświadczeń o zobowiązaniu do zachowaniu poufności;
4) umów powierzenia przetwarzania danych osobowych, w których Gmina jest stroną;
5) wniosków o udostępnienie danych ze zbioru danych osobowych;
6) rejestru zbiorów danych osobowych;
7) dokumentacji dotyczącej analizy ryzyka;
8) raportów naruszeń zasad bezpieczeństwa ochrony danych osobowych;
9) rejestru naruszeń i incydentów;
10) innych pism, dokumentów wymaganych Polityką, Instrukcją, ustawą, rozporządzeniem.

**3.** Szczegółowy zakres obowiązków Zastępcy Wójta w zakresie ochrony danych osobowych w Urzędzie Gminy w Brudzeniu Dużym określa Regulamin Organizacyjny.

## 2.4 Inspektor Ochrony Danych

**1.** W Urzędzie Gminy, zgodnie z art. 37 RODO, Administrator wyznaczył Inspektora ochrony danych.
**2.** Inspektor ochrony danych może być członkiem personelu Administratora lub wykonywać zadania na podstawie umowy o świadczenie usług.
**3.** Szczegółowy zakres obowiązków Inspektora ochrony danych określa rozporządzenie RODO. Inspektor ochrony danych ma następujące zadania:

1) informowanie Administratora, podmiotu przetwarzającego oraz pracowników, którzy przetwarzają dane osobowe, o obowiązkach spoczywających na nich na mocy niniejszego rozporządzenia oraz innych przepisów Unii lub państw członkowskich o ochronie danych i doradzanie im w tej sprawie;
2) monitorowanie przestrzegania rozporządzenia RODO, innych przepisów Unii lub państw członkowskich o ochronie danych oraz polityk Administratora w dziedzinie ochrony danych osobowych, w tym podział obowiązków, działania zwiększające świadomość, szkolenia personelu uczestniczącego w operacjach przetwarzania oraz powiązane z tym audyty;
3) udzielanie na żądanie zaleceń co do oceny skutków dla ochrony danych oraz monitorowanie jej wykonania zgodnie z art. 35 RODO;
4) współpraca z organem nadzorczym;
5) pełnienie funkcji punktu kontaktowego dla organu nadzorczego w kwestiach związanych z przetwarzaniem, w tym z uprzednimi konsultacjami, o których mowa w art. 36 RODO, oraz w stosownych przypadkach prowadzenie konsultacji we wszelkich innych sprawach.

Ponadto Inspektor ochrony danych osobowych wykonuje czynności wynikające z niniejszej Polityki bezpieczeństwa.
**4.** Inspektor ochrony danych wypełnia swoje zadania z należytym uwzględnieniem ryzyka związanego z operacjami przetwarzania, mając na uwadze charakter, zakres, kontekst i cele przetwarzania.
**5.** Inspektor ochrony danych może wykonywać również inne czynność zlecone przez Administratora. W przypadku pełnienia funkcji Inspektora ochrony danych na odstawie umowy o świadczenie usług szczegółowy zakres czynności IOD określa przedmiotowa umowa.

## 2.5 Administrator systemów informatycznych

**1.** Funkcję Administrator Systemów Informatycznych (ASI) w Urzędzie Gminy w Brudzeniu Dużym pełni osoba wyznaczona przez Administratora. Stosowny dokument powołania ASI znajduje się w **Załączniku nr 3** do niniejszej Polityki bezpieczeństwa. Administrator może każdorazowo odwołać ASI.
**2.** Celem działania ASI jest nadzorowanie i realizowanie zasad bezpieczeństwa przetwarzania i ochrony danych osobowych w systemach informatycznych Urzędu Gminy w Brudzeniu Dużym. ASI wykonuje czynności w imieniu Administratora.
**3.** Obszarem działania ASI jest serwerownia zlokalizowana w budynku Urzędu Gminy wraz z innymi pomieszczeniami, w których przetwarzane są dane osobowe w systemach informatycznych. ASI posiada uprawnienia dostępu do systemów informatycznych Urzędu Gminy,

w którym przetwarzane są dane osobowe, posługując się hasłem dostępu do wszystkich stacji roboczych z poziomu administratora.

4. Do uprawnień i obowiązków Administratora Systemów Informatycznych należy m. in.:
   1) nadawanie uprawnień do przetwarzania danych osobowych w systemach informatycznych – zakładanie, blokowanie, zawieszanie i uaktywnianie kont;
   2) prowadzenie rejestru nadanych uprawnień do przetwarzania danych w systemach informatycznych;
   3) nadzór nad stosowaniem środków zapewniających bezpieczeństwo przetwarzania danych osobowych w systemach informatycznych, a w szczególności przeciwdziałających dostępowi osób niepowołanych do tych systemów;
   4) nadzorowanie zabezpieczeń systemów informatycznych w zakresie: przepływu informacji pomiędzy systemem informatycznym a siecią publiczną oraz działań inicjowanych z sieci i z systemu informatycznego;
   5) nadzór nad procedurami przekazywania podmiotowi nieuprawnionemu urządzeń systemów informatycznych oraz elektronicznych nośników informacji zawierających dane osobowe;
   6) podejmowanie odpowiednich działań w przypadku wykrycia naruszeń w systemie zabezpieczeń;
   7) identyfikacja i analiza zagrożeń oraz ocena ryzyka, na które może być narażone przetwarzanie danych osobowych w systemach informatycznych;
   8) wyjaśnianie i dokumentowanie przypadków naruszania zasad bezpieczeństwa systemów informatycznych;
   9) wykonywanie kopii zapasowych zbiorów danych zgodnie z zasadami określonymi w Instrukcji oraz okresowo sprawdzanie ich pod kątem dalszej przydatności do odtwarzania danych w przypadku awarii systemu informatycznego;
   10) nadzór nad niszczonymi i przechowywanymi kopiami zapasowymi zbiorów danych osobowych oraz programów zastosowanych do ich przetwarzania;
   11) osobiste wykonywanie lub nadzorowanie nad wykonywaniem: napraw, konserwacji oraz likwidacji urządzeń komputerowych, które mogą zawierać dane osobowe;
   12) dokonywanie oceny zgodności aplikacji z przepisami bezpieczeństwa przetwarzania danych osobowych w systemach informatycznych;
   13) inicjowanie i nadzór nad wdrażaniem nowych narzędzi, procedur organizacyjnych oraz sposobów zarządzania systemami informatycznymi, które mają doprowadzić do wzmocnienia bezpieczeństwa przy przetwarzaniu danych osobowych;
   14) podejmowanie innych czynności w zakresie zabezpieczenia przetwarzania danych w systemach informatycznych, o których mowa w Instrukcji Zarządzania Systemem Informatycznym;
   15) informowanie Zastępcę Wójta i/lub IOD/Administratora o konieczności wprowadzenia zmian w niniejszej Polityce bezpieczeństwa oraz Instrukcji (np. z powodu zmian procedur tworzenia kopii zapasowych lub zmiany zabezpieczeń systemów informatycznych).

Administrator Systemów Informatycznych ma obowiązek prowadzenia analizy i przedstawiania wniosków dotyczących zmiany czynności organizacyjnych Administratorowi, Zastępcy Wójta i/lub Inspektorowi ochrony danych i wdrażania w systemach informatycznych zabezpieczeń

technicznych mających na celu zapewnienie bezpieczeństwa przetwarzania danych osobowych w Urzędzie Gminy w Brudzeniu Dużym.

## 2.6 Kierownicy Referatów Urzędu Gminy w Brudzeniu Dużym

1. Kierownicy Referatów w zakresie podległych im pracowników zobowiązani są do:
   1) zarządzania zasobem danych osobowych w ramach zadań realizowanych przez kierowany referat;
   2) występowania z wnioskiem do Zastępcy Wójta o nadanie upoważnień do przetwarzania danych osobowych;
   3) wykonywania poleceń Administratora, Zastępcy Wójta, Inspektora ochrony danych w zakresie ochrony danych osobowych;
   4) wdrażania i nadzorowania przestrzegania Polityki bezpieczeństwa oraz Instrukcji;
   5) stwarzania warunków organizacyjnych i technicznych umożliwiających spełnienie wymogów wynikających z RODO;
   6) ciągłej kontroli poprawności merytorycznej danych gromadzonych w systemach informatycznych funkcjonujących w ramach danego referatu.
2. Kierownik Referatu obowiązany jest zgłaszać Zastępcy Wójta zamiar utworzenia nowego zbioru danych osobowych, który będzie funkcjonował w obrębie danego referatu.
3. Praca Kierowników Referatu jest nadzorowana pod względem bezpieczeństwa ochrony danych przez Zastępcę Wójta.

## 2.7 Osoby upoważnione do przetwarzania danych osobowych

1. Wszystkie osoby, których rodzaj wykonywanej pracy będzie wiązał się z dostępem do danych osobowych, przed przystąpieniem do pracy, podlegają przeszkoleniu w zakresie obowiązujących przepisów prawa dotyczących ochrony danych osobowych oraz obowiązujących w Urzędzie Gminy w Brudzeniu Dużym zasad ochrony danych osobowych wynikających z Polityki bezpieczeństwa danych osobowych.
2. Do przetwarzania danych osobowych mogą być dopuszczone wyłącznie osoby posiadające upoważnienie do przetwarzania danych osobowych nadane przez Administratora.
3. Każda osoba, która uzyskała upoważnienie do przetwarzania danych osobowych zobowiązana jest do ich ochrony w sposób zgodny z przepisami rozporządzenia RODO, ustawy, Polityki bezpieczeństwa danych osobowych oraz Instrukcji Zarządzania Systemem Informatycznym.
4. Wszystkie osoby upoważnione do przetwarzania danych osobowych są zobowiązane do:
   1) zachowania w tajemnicy danych osobowych oraz sposobów ich zabezpieczenia, również po ustaniu zatrudnienia/odwołania upoważnienia/upływie jego ważności. Stosowny zapis o przyjęciu zobowiązania do zachowania w tajemnicy przetwarzanych danych osobowych zawiera upoważnienie do przetwarzania danych osobowych;
   2) przetwarzania danych osobowych tylko w wyznaczonych do tego celu pomieszczeniach służbowych;
   3) przetwarzania danych osobowych wyłącznie z zakresie ustalonym przez Administratora, zawartym w upoważnieniu i tylko w celu wykonywania obowiązków służbowych;
   4) stosowania określonych przez Administratora procedur oraz wytycznych mających na celu przetwarzania danych zgodnie z zobowiązującym prawem;

5) zabezpieczania zbiorów danych osobowych oraz dokumentów zawierających dane osobowe przed dostępem osób nieupoważnionych za pomocą środków określonych w Polityce bezpieczeństwa oraz Instrukcji Zarządzania Systemem Informatycznym, niszczenia wszystkich zbędnych nośników zawierających dane osobowe w sposób uniemożliwiający ich odczytanie;
6) nieudzielania informacji o danych osobowych innym podmiotom, chyba że obowiązek taki wynika wprost z przepisów prawa i tylko w sytuacji, gdy przesłanki określone w takich przepisach zostały spełnione;
7) niezwłocznego zawiadamiania Administratora/Inspektora ochrony danych o wszelkich przypadkach naruszenia bezpieczeństwa danych osobowych, a także o przypadkach utraty lub kradzieży dokumentów lub innych nośników zawierających te dane osobowe.

**5.** Naruszenie obowiązku ochrony danych osobowych, a w szczególności obowiązku zachowania danych osobowych w tajemnicy skutkuje poniesieniem odpowiedzialności karnej na podstawie przepisów ustawy oraz stanowi ciężkie naruszenie obowiązków pracowniczych i może być podstawą rozwiązania stosunku pracy w trybie art. 52 Kodeksu pracy, bądź rozwiązania stosunku cywilnoprawnego łączącego strony.

## ROZDZIAŁ 3. Upoważnienia do przetwarzania danych osobowych

**1.** Upoważnienie do przetwarzania danych osobowych jest dokumentem niezbędnym do tego, aby pracownik Urzędu Gminy w Brudzeniu Dużym mógł przetwarzać w systemie informatycznym lub w wersji papierowej dane osobowe. Upoważnienie nadawane jest indywidualnie, z wyraźnym wskazaniem, jakie zbiory danych obejmuje swoim zakresem. Upoważnienie do przetwarzania danych osobowych nadawane jest przez Administratora.

**2.** Upoważnienie do przetwarzania danych osobowych nadawane jest po przeprowadzeniu szkolenia z zakresu zasad ochrony danych osobowych, o którym mowa w **Rozdziale 11.** niniejszej Polityki bezpieczeństwa. Osoba, która odbyła szkolenie ma obowiązek złożyć zobowiązanie do zachowania danych w tajemnicy, którego wzór stanowi odpowiednio **Załącznik nr 2a i 2b** do niniejszej Polityki bezpieczeństwa.

**3.** Po złożeniu zobowiązania pracownikowi/stażyście/praktykantowi, jeżeli jest to konieczne, nadawane jest upoważnienie do przetwarzania danych osobowych. Wzór Upoważnienia do przetwarzania danych osobowych stanowi **Załącznik nr 4** do niniejszej Polityki bezpieczeństwa.

**4.** Upoważnienie nadawane jest na wniosek bezpośredniego przełożonego danego pracownika/stażysty/praktykanta. We wniosku należy określić indywidualne obowiązki i odpowiedzialności pracownika związane z przetwarzaniem danych osobowych, oraz wskazać do jakich zbiorów danych osobowych pracownik będzie miał dostęp. Wniosek może mieć postać dokumentu papierowego lub może zostać złożony w formie e-maila.

**5.** Wniosek, o którym mowa w ust. 4 należy przedłożyć do Zastępcy Wójta w celu przygotowania Upoważnienia do przetwarzania danych osobowych. Przygotowane Upoważnienie przedkładane jest Administratorowi w celu zatwierdzenia zakresu upoważnienia i podpisania.

**6.** Zastępca Wójta informuje ASI o treści podpisanego upoważnienia, o którym mowa w ust. 4 w celu przyznania dostępów do ściśle określonych systemów informatycznych.

7. Wszystkie osoby dopuszczone do przetwarzania danych są wpisywane do ewidencji osób dopuszczonych do przetwarzania danych osobowych. Wzór Ewidencji wydanych upoważnień do przetwarzania danych osobowych stanowi **Załącznik nr 5** do niniejszej Polityki bezpieczeństwa.
8. Ewidencję wydawanych upoważnień prowadzi Zastępca Wójta. Ewidencja prowadzona jest w wersji papierowej i elektronicznej. Dozwolone jest prowadzenie ewidencji tylko w formie elektronicznej z zachowaniem ciągłości archiwizacji i corocznym wydrukiem papierowym.
9. Ewidencja wydanych upoważnień zawiera:
   1) imię i nazwisko osoby upoważnionej;
   2) zajmowane stanowisko osoby upoważnionej do przetwarzania danych;
   3) datę nadania/odwołania/ustania upoważnienia do przetwarzania danych;
   4) identyfikator, jeżeli dane są przetwarzane w systemie informatycznym;
   5) zakres upoważnienia do przetwarzania danych osobowych (nazwa zbioru danych).
9. Zakres nadanego upoważnienia może ulegać zmianie (rozszerzeniu bądź zwężeniu) w związku z pełnieniem przez pracownika określonych zadań, w określonym przedziale czasu. W przypadku konieczności zmiany upoważnienia spowodowanego zmianą zakresu obowiązków służbowych pracownika/przeniesieniem do innego Referatu, Zastępca Wójta opracowuje nowe upoważnienie do przetwarzania danych osobowych. Zakres nowego Upoważnienia uzgadniany jest z Kierownikiem Referatu, w którym pracuje lub będzie pracować osoba upoważniana.
10. Konieczność odwołania upoważnienia może nastąpić w szczególności w przypadku:
   1) zmiany stanowiska pracy, na stanowisko, na którym nie ma konieczności posiadania dostępu do danych osobowych;
   2) umyślnego naruszenia zasad ochrony danych osobowych określonych w rozporządzeniu RODO, ustawie, Polityce bezpieczeństwa danych osobowych, Instrukcji Zarządzania Systemem Informatycznym;
   3) rozwiązania stosunku pracy;
   4) rozwiązania umowy cywilnoprawnej.
11. Każdorazowe odwołanie/ustanie upoważnienia jest odnotowywane w prowadzonej ewidencji wydanych upoważnień.
12. Odwołanie/ustanie upoważnienia oznacza automatyczną utratę wszystkich uprawnień dostępu do systemów informatycznych, w których są przetwarzane dane osobowe. Z tego powodu, Administrator, Zastępca Wójta lub bezpośredni przełożony pracownika informuje, drogą e-mail, ASI o konieczności zablokowania uprawnień dostępu do systemów informatycznych osobie, której zostało wycofane upoważnienie do przetwarzania danych osobowych.

## ROZDZIAŁ 4. Sposób postępowania z ryzykiem

1. Zarządzanie ryzykiem w ochronie danych to ciągły proces, wymagający stałej identyfikacji i szacowania poziomu ryzyka związanego z przetwarzaniem danych osobowych. Podlega on ciągłemu monitorowaniu i doskonaleniu skuteczności stosowanych zabezpieczeń organizacyjnych i technicznych, w celu utrzymania ryzyka na akceptowalnym poziomie.
2. Niniejsza procedura opisuje sposób przeprowadzenia analizy ryzyka w Urzędzie Gminy w Brudzeniu Dużym w celu zabezpieczenia danych osobowych adekwatnie do zidentyfikowanych zagrożeń.

## 4.1 Analiza ryzyka

W celu dokonania analizy ryzyka wymagane jest zidentyfikowanie danych osobowych, które należy zabezpieczyć. Dane osobowe przetwarzane przez Urząd Gminy w Brudzeniu Dużym zawarte są w postaci zbiorów danych osobowych i zostały wykazane w **Załączniku nr 6** do niniejszej Polityki bezpieczeństwa.

## 4.2 Określenia stosowane w procedurze

1) **Aktywa (zasoby) –** środki materialne i niematerialne mające wpływ na przetwarzanie danych osobowych. Aktywem jest każdy element, który ma wartość dla organizacji. Mogą to być m.in. pracownicy, outsourcing, sprzęt IT, oprogramowanie (programy i system operacyjny), dane osobowe, infrastruktura, informacje;
2) **Naruszenie (Incydent) ochrony danych osobowych** – to naruszenie bezpieczeństwa prowadzące do przypadkowego lub niezgodnego z prawem zniszczenia, utracenia, zmodyfikowania, nieuprawnionego ujawnienia lub nieuprawnionego dostępu do danych osobowych przesyłanych, przechowywanych lub w inny sposób przetwarzanych;
3) **Zagrożenie** – potencjalne naruszenie (potencjalny incydent), np. zagrożenie naturalne, losowe, zamierzone, administracyjne;
4) **Prawdopodobieństwo** – prawdopodobieństwo wystąpienia zagrożenia (incydentu) w danym zbiorze danych osobowych/w procesie przetwarzania;
5) **Skutek** – rezultat niepożądanego incydentu (straty jakie poniesie jednostka w wypadku urzeczywistnienia się zagrożenia);
6) **Ryzyko** – prawdopodobieństwo, że określone zagrożenie wystąpi i spowoduje straty lub zniszczenie zasobów (aktywów);
7) **Strata** – np. strata wizerunku jednostki lub zaufania, strata aktywów – w tym również niematerialnych.

## 4.3 Wyznaczenie zagrożeń

1. Administrator określa listę zagrożeń, które mogą wystąpić w przetwarzaniu danych w zbiorze danych osobowych/w procesie przetwarzania.
2. Zagrożenia są identyfikowane w odniesieniu do wcześniej zidentyfikowanych aktywów (zasobów).
3. Wykaz zagrożeń, które mogą wystąpić w Urzędzie Gminy w Brudzeniu Dużym stanowi **Załącznik nr** 7 do niniejszej Polityki bezpieczeństwa. Nie stanowi on zamkniętego katalogu zagrożeń, które mogą wystąpić w jednostce.

## 4.4 Wyliczenie ryzyka dla zagrożeń

1. Każde zidentyfikowane zagrożenie podlega analizie mającej na celu oszacowanie prawdopodobieństwa wystąpienia oraz skutku, jaki będzie miało ewentualne wystąpienie tego zagrożenia (ocena punktowa w skali od „1" do „3"):
   1) Administrator określa Prawdopodobieństwo (**P**) wystąpienia poszczególnych zagrożeń w zbiorze danych osobowych/w procesie przetwarzania. Sposób określenia prawdopodobieństwa wystąpienia ryzyka obrazuje poniższa tabela:

| Prawdopodobieństwo | Skala (punktacja) | Przesłanki |
|---|---|---|
| zagrożenie niskie | 1 punkt | Istnieją uzasadnione powody, by sądzić, że czynnik ryzyka zdarzy się **raz** w ciągu roku lub że nie zdarzy się w ciągu roku |
| zagrożenie średnie | 2 punkty | Istnieją uzasadnione powody, by sądzić, że czynnik ryzyka zdarzy się **kilkakrotnie** w ciągu roku |
| zagrożenie wysokie | 3 punkty | Istnieją uzasadnione powody, by sądzić, że czynnik ryzyka zdarzy się **wielokrotnie** w ciągu roku |

2) Administrator określa Skutki (**S**) wystąpienia incydentów (materializacji zagrożeń), uwzględniając straty finansowe, utratę reputacji, sankcje/skutki karne. Proponowaną Skalę skutków prezentuje poniższa tabela:

| Skutki | Skala (punktacja) | Przesłanki |
|---|---|---|
| niskie | 1 punkt | Niski wpływ na funkcjonowanie jednostki, skutki można łatwo usunąć |
| średnie | 2 punkty | Krótkotrwały wpływ na działanie jednostki |
| wysokie | 3 punkty | Zagrożenie dla ciągłości działania jednostki |

2. Administrator wylicza Ryzyko wystąpienia incydentu (R) dla wszystkich zagrożeń i ich skutków według wzoru: R = P * S

Oznaczenia we wzorze:

P – prawdopodobieństwo wystąpienia ryzyka,

S – wielkość skutku, jaki będzie miało ewentualne wystąpienie tego ryzyka

R – ryzyko wystąpienia incydentu (zagrożenia)

Matryca oceny ryzyka

| Skutek | | | | |
|---|---|---|---|---|
| **Wysoki** | 3 | 6 | 9 | |
| **Średni** | 2 | 4 | 6 | |
| **Niski** | 1 | 2 | 3 | |
| | **Niskie** | **Średnie** | **Wysokie** | Prawdopodobieństwo |

3. Administrator porównuje wyliczone ryzyka ze skalą i podejmuje decyzje dotyczące dalszego postępowania z ryzykiem. Ustala się następujące poziomy wystąpienia ryzyka:

1) **1-2 –ryzyko niskie** – ryzyko jest akceptowalne, należy monitorować i w miarę potrzeby kontrolować ryzyko, reakcja nie jest wymagana;

2) **3-4 – ryzyko średnie** – ryzyko jest opcjonalne, ryzyko możemy akceptować albo podjąć

działania w celu jego obniżenia, wymaga okresowego monitorowania;

3) **6-9 – ryzyko wysokie –** jest ryzykiem nieakceptowanym i wymaga podjęcia zdecydowanych działań w celu zmniejszenia ryzyka do akceptowalnego poziomu, poprzez zmniejszenie jego wpływu lub prawdopodobieństwa wystąpienia.

### 4.5 Reakcja na ryzyko

1. Administrator przyjmuje następujące sposoby postępowania z ryzykiem:
   1) **akceptacja ryzyka** – zabezpieczenia są wystarczające, nie ma potrzeby wprowadzania zmian w działaniu organizacji (zabezpieczeń);
   2) **transfer ryzyka (przeniesienie)** – przerzucenie ryzyka na podmiot zewnętrzny;
   3) **unikanie** – unikanie działań powodujących występowanie ryzyka;
   4) **redukcja** – działania pozwalające na obniżenie poziomu ryzyka do akceptowalnego.
2. Wykaz przykładowych zabezpieczeń stanowi **Załącznik nr 8** do niniejszej Polityki bezpieczeństwa.
3. Arkusz analizy ryzyka stanowi **Załącznik nr 9** do niniejszej Polityki bezpieczeństwa.

### 4.6 Ponowna analiza ryzyka

Administrator przeprowadza Analizę ryzyka cyklicznie, tj. raz na rok lub w przypadku wystąpienia znaczących zmian w przetwarzaniu danych (np. przetwarzanie nowych zbiorów danych osobowych, wystąpienie nowych procesów przetwarzania, zmian w przepisach prawnych, zmian w infrastrukturze jednostki).

### 4.7 Plan postępowania z ryzykiem

1. Tam, gdzie Administrator decyduje się obniżyć ryzyko, wyznacza listę zabezpieczeń do wdrożenia, termin realizacji oraz osoby odpowiedzialne.
2. Administrator wyznacza Administratora Systemów Informatycznych do monitorowania wdrożonych zabezpieczeń technicznych. Za monitorowanie zabezpieczeń organizacyjnych odpowiada Zastępca Wójta.

## ROZDZIAŁ 5. Postępowanie z incydentami

Zgodnie z art. 4 pkt 12 Rozporządzenia 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) „naruszenie ochrony danych osobowych" oznacza naruszenie bezpieczeństwa prowadzące do przypadkowego lub niezgodnego z prawem zniszczenia, utracenia, zmodyfikowania, nieuprawnionego ujawnienia lub nieuprawnionego dostępu do danych osobowych przesyłanych, przechowywanych lub w inny sposób przetwarzanych.

Niniejsza procedura definiuje katalog podatności i incydentów zagrażających bezpieczeństwu danych osobowych w Urzędzie Gminy w Brudzeniu Dużym oraz opisuje sposób reagowania na nie. Celem Procedury jest minimalizacja skutków wystąpienia incydentów bezpieczeństwa oraz ograniczenie ryzyka powstania zagrożeń i występowania incydentów w przyszłości. Incydentem w zakresie danych osobowych jest sytuacja powodująca utratę poufności, integralności lub dostępności przetwarzanych danych.

## 5.1 Istota naruszenia danych osobowych

**1.** Każda osoba upoważniona przez Administratora do przetwarzania danych osobowych zobowiązana jest do powiadomienia o stwierdzeniu podatności lub wystąpieniu incydentu bezpośredniego przełożonego, który zawiadamia Zastępcę Wójta, Inspektora ochrony danych (IOD) i Administratora Systemów Informatycznych (ASI).

**2.** Do podatności bezpieczeństwa danych osobowych należą:

- **a)** niewłaściwe (bądź brak) zabezpieczenie fizyczne budynku/pomieszczeń Urzędu, sprzętu IT oraz dokumentów,
- **b)** niewłaściwe zabezpieczenie sprzętu IT, oprogramowania przed wyciekiem – niezastosowanie oprogramowania antywirusowego, przesyłanie informacji przez niezabezpieczone łącza telekomunikacyjne,
- **c)** udostępnianie pomieszczeń, sprzętu IT, dokumentów zawierających dane osobowe osobom nieposiadającym upoważnienia nadanego przez Administratora,
- **d)** nieprzestrzeganie zasad ochrony danych osobowych przez pracowników (niestosowanie zasady czystego biurka/ekranu, ochrony haseł, pozostawianie otwartych pomieszczeń, szaf, biurek bądź udostępnianie ich osobom nieuprawnionym).

**3.** Naruszeniem danych osobowych jest każdy stwierdzony fakt nieuprawnionego ujawnienia danych, udostępnienia lub umożliwienia dostępu do nich osobom nieupoważnionym, zabrania danych przez osobę nieupoważnioną, uszkodzenia jakiegokolwiek elementu systemu informatycznego, a w szczególności:

- **a)** nieuprawniony dostęp lub próba dostępu do pomieszczeń, w których następuje proces przetwarzania danych (widoczne uszkodzenia bądź naruszenia zabezpieczeń),
- **b)** naruszenie lub próba naruszenia zbioru danych oraz integralności systemu,
- **c)** nieautoryzowane zniszczenie lub próba zniszczenia danych zgromadzonych w zbiorach papierowych oraz w systemie,
- **d)** zmiana lub utrata danych zapisanych na kopiach zapasowych lub archiwalnych dokonaną w sposób nieautoryzowany,
- **e)** nieuprawniony dostęp do systemu (sygnał o nielegalnym logowaniu lub inny objaw wskazujący na próbę lub działanie związane z nielegalnym dostępem do systemu),
- **f)** inny stan systemu lub pomieszczeń niż pozostawiony przez użytkownika po zakończeniu lub po przerwie w pracy z systemem.

**4.** Incydentem jest sytuacja naruszenia bezpieczeństwa informacji ze względu na dostępność, integralność i poufność. Incydenty powinny być wykrywane, rejestrowane i monitorowane w celu zapobieżenia ich ponownemu wystąpieniu. Do incydentów bezpieczeństwa danych osobowych należą:

- **a)** losowe zdarzenia zewnętrzne (pożar budynku/pomieszczenia, zalanie wodą, utrata zasilania, utrata łączności),

b) zdarzenia losowe wewnętrzne (możliwość awarii sprzętu IT (awarie serwera, komputerów, twardych dysków, brak lub awaria ups) lub oprogramowania ze względu na brak odpowiedniego serwisowania, pomyłki informatyków, użytkowników, utrata/zagubienie/przypadkowe zniszczenie danych,
c) umyślne działanie (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 poprzez samowolne instalowanie niedozwolonego oprogramowania na służbowym sprzęcie).

5. Procedurę stosuje się odpowiednio w przypadku stwierdzenia, że stan dokumentacji lub stan pomieszczeń bądź szaf biurowych, w których przechowywana jest dokumentacja wzbudzają podejrzenie, że dostęp do nich mogły mieć osoby nieupoważnione.

## 5.2 Postępowanie w przypadku naruszenia danych osobowych

1. Każdy pracownik, który stwierdzi fakt naruszenia danych osobowych ma obowiązek zgłosić przypadek naruszenia danych bezpośredniemu przełożonemu oraz podjąć czynności niezbędne do powstrzymania skutków naruszenia ochrony, zabezpieczyć dowody umożliwiające ustalenie przyczyn oraz skutków naruszenia. Bezpośredni przełożony niezwłocznie informuje o zaistniałej sytuacji Zastępcę Wójta, Inspektora ochrony danych (IOD) i Administratora Systemów Informatycznych (ASI). Do czasu przybycia IOD i (ASI), bądź innej osoby upoważnionej przez Administratora, pracownik:

a) zabezpiecza dostęp do miejsca lub urządzenia,
b) wstrzymuje pracę na komputerze, na którym zaistniało naruszenie ochrony oraz nie uruchamia bez koniecznej potrzeby komputerów i innych urządzeń, które w związku z naruszeniem ochrony zostały wstrzymane,
c) podejmuje, stosownie do zaistniałej sytuacji inne, niezbędne działania celem zapobieżenia dalszym zagrożeniom, które mogą skutkować utratą danych osobowych,
d) jest zobowiązany zaniechać wszelkich innych działań mogących utrudnić analizę wystąpienia naruszenia i udokumentowanie zdarzenia ,
e) nie opuszcza bez uzasadnionej potrzeby miejsca zdarzenia do czasu przybycia Inspektora ochrony danych (IOD) i/lub Administratora Systemów Informatycznych (ASI), bądź innej osoby upoważnionej przez Administratora.

2. Dokonywanie zmian w miejscu naruszenia ochrony danych, o których mowa w pkt 1, bez uzyskania zgody jest dopuszczalne, jeżeli zachodzi konieczność ratowania osób lub mienia albo zapobieżenia grożącemu niebezpieczeństwu.

3. Zgodę na ponowne uruchomienie komputerów i innych urządzeń oraz kontynuowanie pracy przy pomocy sprzętu IT wyraża Administrator Systemów Informatycznych.

4. Administrator Systemu Informatycznego jest zobowiązany do informowania Inspektora ochrony danych i Zastępcy Wójta o wszelkich anomaliach w pracy administrowanych przez siebie urządzeń, mogących być przyczyną lub skutkiem incydentu w zakresie danych osobowych.

5. Bezpośredni przełożony pracownika, Zastępca Wójta, IDO i ASI który wykrył lub został poinformowany o nieprawidłowościach przy przetwarzaniu danych osobowych powinien niezwłocznie zidentyfikować problem i przedsięwziąć wszelkie niezbędne kroki, aby uniknąć w przyszłości podobnych zdarzeń.

6. W przypadku stwierdzenia wystąpienia naruszenia/incydentu Inspektor ochrony danych prowadzi postępowanie wyjaśniające w toku, którego:

a) ustala czas zdarzenia będącego incydentem,
b) ustala zakres i przyczyny naruszenia/incydentu oraz jego ewentualne skutki,
c) zabezpiecza dowody,
d) ustala osoby odpowiedzialne za naruszenie,
e) działa na rzecz przywrócenia działań organizacji po wystąpieniu incydentu przy współpracy z ASI, który niezwłocznie zapewnia przywrócenie prawidłowego stanu działania systemu, a w przypadku uszkodzenia baz danych, odtwarza je z ostatnich kopii awaryjnych z zachowaniem należytych środków ostrożności; sprawdza jakość komunikacji w systemie informatycznym; dokonuje analizy stanu systemu wraz z oszacowaniem rozmiaru szkód powstałych wskutek naruszenia oraz poddaje analizie metody pracy osób upoważnionych do przetwarzania danych osobowych;
f) podejmuje działania zapobiegawcze zmierzające do eliminacji podobnych naruszeń/incydentów w przyszłości lub zmniejszenia strat w momencie ich zaistnienia,
g) podejmuje decyzję o toku dalszego postępowania, stosownie do zakresu naruszenia lub zasadności podejrzenia naruszenia ochrony danych osobowych i w przypadkach uzasadnionych niezwłocznie powiadamia właściwą osobę podejmującą decyzję w imieniu Administratora,
h) proponuje ewentualne działania dyscyplinarne.

7. Inspektor danych osobowych dokumentuje zaistniały przypadek naruszenia bezpieczeństwa danych sporządzając Raport z naruszeń zasad bezpieczeństwa ochrony danych osobowych wg wzoru stanowiącego **Załącznik nr 10** do niniejszej Polityki bezpieczeństwa, który następnie niezwłocznie przekazuje Administratorowi, a w przypadku jego nieobecności osobie wyznaczonej. Raport podpisuje również pracownik, który zgłosił naruszenie oraz bezpośredni przełożony pracownika.

8. Jeżeli przyczyną naruszenia były wadliwe metody pracy, błędy i zaniedbania osób zatrudnionych przy przetwarzaniu danych osobowych, jak również w przypadku pojawiających się nieprawidłowości przy przetwarzaniu danych osobowych IOD przy współpracy z ASI przeprowadza dodatkowe szkolenie uzupełniające dotyczące zasad ochrony danych osobowych w strukturze Administratora.

9. Administrator dokumentuje naruszenia ochrony danych osobowych, w tym okoliczności naruszenia ochrony danych osobowych, jego skutki oraz podjęte działania zaradcze w Rejestrze naruszeń i incydentów wg wzoru stanowiącego **Załącznik nr 11** do niniejszej Polityki bezpieczeństwa.

## 5.3 Odpowiedzialność za naruszenie danych osobowych

1. Wobec osoby, która w przypadku naruszenia danych osobowych nie podjęła działania określonego w niniejszym dokumencie, a w szczególności nie powiadomiła odpowiedniej osoby zgodnie z określonymi zasadami mogą zostać wyciągnięte konsekwencje dyscyplinarne przewidziane Kodeksem pracy oraz wewnętrznymi regulacjami obowiązującymi w strukturze Administratora.

2. Zabrania się świadomego wywoływania incydentów przez osoby upoważnione do przetwarzania danych.

## 5.4 Zgłaszanie naruszenia ochrony danych osobowych organowi nadzorczemu

**1.** W przypadku wykrycia naruszenia ochrony danych osobowych skutkującego wystąpieniem ryzyka naruszenia praw i/lub wolności osób fizycznych, Administrator bez zbędnej zwłoki – w miarę możliwości, nie później niż w terminie 72 godzin po stwierdzeniu naruszenia – zgłasza je organowi nadzorczemu. Do zgłoszenia przekazanego organowi nadzorczemu po upływie 72 godzin dołącza się wyjaśnienie przyczyn opóźnienia. Wzór Zgłoszenia naruszenia ochrony danych osobowych organowi nadzorczemu stanowi **Załącznik nr 12** do niniejszej Polityki bezpieczeństwa.

**2.** Zgłoszenie, o którym mowa w ust. 1, musi co najmniej:

- **a)** opisywać charakter naruszenia ochrony danych osobowych, w tym w miarę możliwości wskazywać kategorie i przybliżoną liczbę osób, których dane dotyczą, oraz kategorie i przybliżoną liczbę wpisów danych osobowych, których dotyczy naruszenie,
- **b)** zawierać imię i nazwisko oraz dane kontaktowe inspektora ochrony danych lub oznaczenie innego punktu kontaktowego, od którego można uzyskać więcej informacji,
- **c)** opisywać możliwe konsekwencje naruszenia ochrony danych osobowych,
- **d)** opisywać środki zastosowane lub proponowane przez administratora w celu zaradzenia naruszeniu ochrony danych osobowych, w tym w stosownych przypadkach środki w celu zminimalizowania jego ewentualnych negatywnych skutków.

Jeżeli – i w zakresie, w jakim – informacji nie da się udzielić w tym samym czasie, można je udzielać sukcesywnie bez zbędnej zwłoki.

**3.** Administrator dokumentuje wszelkie naruszenia ochrony danych osobowych, w tym okoliczności naruszenia ochrony danych osobowych, jego skutki oraz podjęte działania zaradcze. Dokumentacja ta musi pozwolić organowi nadzorczemu weryfikowanie przestrzegania niniejszego artykułu.

## 5.5 Zawiadamianie osoby, której dane dotyczą, o naruszeniu ochrony danych osobowych

**1.** Jeżeli naruszenie ochrony danych osobowych może powodować wysokie ryzyko naruszenia praw lub wolności osób fizycznych, Administrator bez zbędnej zwłoki zawiadamia osobę, której dane dotyczą, o takim naruszeniu.

**2.** Zawiadomienie, o którym mowa w ust. 1, jasnym i prostym językiem opisuje charakter naruszenia ochrony danych osobowych oraz zawiera przynajmniej informacje i środki, o których mowa w **dziale 5. 4** ust. 2 lit. b), c) i d).

**3.** Zawiadomienie, o którym mowa w ust. 1, nie jest wymagane, w następujących przypadkach:

- **a)** Administrator wdrożył odpowiednie techniczne i organizacyjne środki ochrony i środki te zostały zastosowane do danych osobowych, których dotyczy naruszenie, w szczególności środki takie jak szyfrowanie, uniemożliwiające odczyt osobom nieuprawnionym do dostępu do tych danych osobowych;
- **b)** Administrator zastosował następnie środki eliminujące prawdopodobieństwo wysokiego ryzyka naruszenia praw lub wolności osoby, której dane dotyczą, o którym mowa w ust. 1;
- **c)** wymagałoby ono niewspółmiernie dużego wysiłku. W takim przypadku wydany zostaje publiczny komunikat lub zastosowany zostaje podobny środek, za pomocą którego osoby, których dane dotyczą, zostają poinformowane w równie skuteczny sposób.

# ROZDZIAŁ 6. Zasady ochrony danych osobowych

Wprowadzenie odpowiednich zasad bezpieczeństwa przetwarzania danych pozwoli zwiększyć poziom ochrony danych osobowych przetwarzanych w Urzędzie.

**1.** Dostęp do danych osobowych mogą mieć tylko pracownicy posiadający upoważnienie do ich przetwarzania.
**2.** W miejscu przetwarzania danych osobowych utrwalonych w formie papierowej pracownicy zobowiązani są do stosowania zasady tzw. „czystego biurka". Zasada ta oznacza nie pozostawianie materiałów zawierających dane osobowe w miejscu umożliwiającym fizyczny dostęp do nich osobom nieuprawnionym. Za realizację powyższej zasady odpowiedzialny jest na swym stanowisku każdy z pracowników. Opuszczając miejsce pracy pracownik jest zobowiązany schować dokumenty zawierające dane osobowe do zamkniętej szafki, tak aby uniemożliwić ewentualnemu intruzowi zabranie informacji do których nie jest upoważniony.
**3.** Pracownik, który w trakcie wykonywanej pracy ma kontakt z osobami z zewnątrz powinien, w miarę możliwości, odwracać dokumenty, które zawierają dane osobowe na drugą stronę tak, aby osoba znajdująca się przy biurku nie miała wglądu w poufne zapiski.
**4.** Monitory komputerów, na których przetwarzane są dane osobowe powinny być ustawione są w sposób utrudniający wgląd osobom postronnym w przetwarzane dane.
**5.** W przypadku zaistnienia ryzyka podejrzenia przez osobę nieuprawnioną wyświetlanych danych na ekranach komputerów pracownik powinien zminimalizować wszystkie programy, tak aby interesant widział jedynie pulpit, stosując opcję „Pokaż pulpit" umieszczoną w prawym dolnym rogu ekranu na pasku zadań lub za pomocą kombinacji klawiszy „Windows+D".
**6.** Niszczenie brudnopisów, błędnych lub zbędnych kopii materiałów zawierających dane osobowe musi odbywać się w sposób uniemożliwiający odczytanie zawartej w nich treści, np. z wykorzystaniem niszczarek do dokumentów.
**7.** Pomieszczenia, w których przetwarzane są dane osobowe na czas nieobecności osób zatrudnionych należy zamykać, w sposób uniemożliwiający dostęp do nich osobom postronnym. Kategorycznie zabrania się pozostawiania kluczy w drzwiach, szafach, biurkach, a także pozostawiania otwartych lub nieprawidłowo zamkniętych drzwi pomieszczeń, w których przetwarzane są dane osobowe.

## 6.1. Zasady korzystania z Internetu

**1.** Użytkownik zobowiązany jest do korzystania z Internetu wyłącznie w celach służbowych.
**2.** Zabrania się pobierania na dysk twardy komputera oraz uruchamiania jakichkolwiek programów oraz plików pobranych z Internetu wymagających licencji, a na które Urząd Gminy nie posiada licencji.
**3.** Użytkownik ponosi odpowiedzialność za szkody spowodowane przez oprogramowanie instalowane z Internetu bez zgody ASI.
**4.** Zabrania się wchodzenia na strony, na których prezentowane są informacje o charakterze przestępczym, hackerskim, pornograficznym, lub innym zakazanym przez prawo.
**5.** Nie należy w opcjach przeglądarki internetowej włączać opcji autouzupełniania formularzy i zapamiętywania haseł.

6. W przypadku korzystania z szyfrowanego połączenia przez przeglądarkę, należy zwracać uwagę na pojawienie się odpowiedniej ikonki (kłódka) oraz adresu www rozpoczynającego się frazą "https:". Witryna internetowa powinna używać prawidłowego certyfikatu bezpieczeństwa.
7. Należy zachować szczególną ostrożność w przypadku podejrzanego żądania lub prośby zalogowania się na stronę (np. na stronę banku, portalu społecznościowego, e-sklepu, poczty mailowej) lub podania loginów i haseł, PIN-ów, numerów kart płatniczych przez Internet.
8. Zabrania się samowolnego podłączania do komputerów modemów, telefonów komórkowych i innych urządzeń dostępowych. Zabrania się łączenia, przy pomocy takich urządze,ń komputerów z Internetem.

## 6.2. Zasady korzystania z poczty elektronicznej

1. Pracownik może korzystać ze służbowej poczty e-mail tylko w celach związanych z wykonywaniem obowiązków służbowych. Zabrania się wykorzystywać służbowego konta e-mail do celów prywatnych.
2. W celu zalogowania się do służbowej poczty e-mail można wykorzystywać przeglądarkę internetową lub klienta poczty elektronicznej (np. program Microsoft Outlook). Logowanie się do służbowego konta e-mail (przez przeglądarkę internetową lub przez klienta poczty e-mail) musi odbywać się przy użyciu zaszyfrowanego połączenia.
3. Należy unikać przekazywania danych osobowych poprzez pocztę elektroniczną.
4. W przypadku przekazania dokumentu zawierającego dane osobowe pocztą elektroniczną należy dokument ten zabezpieczyć silnym hasłem (zawierającym min. 8 znaków, duże i małe litery oraz cyfry lub znaki specjalne), np. wykorzystując program do archiwizowania dokumentów umożliwiający zabezpieczenie utworzonego archiwum hasłem. Zabezpieczony dokument należy dodać jako załącznik do wiadomości e-mail. Hasło do otworzenia dokumentu należy przekazać inną drogą niż poprzez wiadomość e-mail (np. telefonicznie). Nie wolno przekazywać danych osobowych bezpośrednio w treści wiadomości e-mail, zabrania się umieszczać dokumentów zawierających dane osobowe „w chmurze" i udostępniać tych dokumentów w postaci przesłanego linku do pobrania pliku (lub w jakikolwiek inny sposób) za pośrednictwem poczty elektronicznej.
5. Zaleca się, aby pracownik podczas przesyłania danych osobowych e-mail'em zawarł w treści prośbę o potwierdzenie otrzymania i zapoznania się z informacją przez adresata.
6. Pracownicy są zobowiązani zwracać szczególną uwagę na poprawność adresu odbiorcy wysyłanej wiadomości.
7. Podczas wysyłania e-mail'i do wielu adresatów jednocześnie, należy użyć metody „Ukryte do wiadomości – UDW". Zabronione jest rozsyłanie e-maili do wielu adresatów z użyciem opcji „Do wiadomości".
8. Przypadki podejrzanych e-maili należy bezzwłocznie zgłaszać Administratorowi Systemów Informatycznych.
9. Pracownicy zobowiązani są okresowo kasować niepotrzebne e-maile.
10. Pracownicy nie mają prawa korzystać z e-maila w celu rozpowszechniania treści o charakterze obraźliwym, niemoralnym lub niestosownym wobec powszechnie obowiązujących zasad postępowania.
11. Zabrania się udostępniać innym pracownikom dostęp do swojej poczty elektronicznej bez zgody przełożonego.

## 6.3. Polityka kluczy

**1.** Polityka kluczy dotyczy wszystkich pomieszczeń budynku Urzędu Gminy w Brudzeniu Dużym położonego przy ulicy Toruńskiej 2, 09-414 Brudzeń Duży.
**2.** W Urzędzie Gminy w Brudzeniu Dużym obowiązuje pięciodniowy tydzień pracy – w poniedziałki od 9:00 do 17:00, a od wtorku do piątku w godzinach od 7:30 do 15:30.
**3.** Budynek Urzędu podlega całodobowej ochronie za pomocą systemu alarmowego zamontowanego w budynku.
**4.** Z uwagi na publiczny charakter Urzędu w czasie jego pracy nie obowiązuje system przepustek, ani też inny system określający uprawnienia do wejścia, przebywania i wyjścia z budynku.
**5.** Zastępca Wójta wyznacza osobę spośród pracowników obsługi, którzy są upoważnieni przez Administratora – Wójta Gminy Brudzeń Duży do rozkodowywania systemu alarmowego i otwierania budynku Urzędu przed rozpoczęciem pracy pracowników, jednak nie wcześniej niż 30 minut przed godziną rozpoczęcia pracy Urzędu. Upoważnienie dotyczy również zamykania budynku Urzędu oraz załączenia systemu alarmowego po zakończeniu pracy.
Wzór upoważnienia do zarządzania kluczami oraz kodem cyfrowym do systemu alarmowego stanowi **Załącznik nr 13** do niniejszej Polityki bezpieczeństwa.
**6.** Klucze do pomieszczeń biurowych, jak również do pomieszczeń szczególnie chronionych (serwerownia) zdawane i wydawane są w sekretariacie Urzędu.
**7.** Od momentu pobrania kluczy do momentu ich zdania na pracownikach urzędujących w tych pomieszczeniach spoczywa pełna odpowiedzialność za ich należyte zabezpieczenie.
**8.** Pracownikom zabrania się:

- wynoszenia kluczy poza Urząd,
- samodzielnego dorabiania kluczy do pomieszczeń i budynku Urzędu,
- pozostawiania kluczy w zamkach od strony korytarza podczas obecności i nieobecności pracownika w pomieszczeniu,
- udostępniania kluczy osobom nieupoważnionym.

**9.** Klucze od biurek i szaf biurowych są w posiadaniu pracowników, którzy ponoszą pełną odpowiedzialność za ich należyte zabezpieczenie. Klucze służące do zabezpieczenia biurek i szaf muszą być jednoznacznie opisane. Zabrania się pozostawiania kluczy w biurkach i szafach podczas chwilowej nieobecności osób upoważnionych w pomieszczeniu. Po zakończonej pracy, klucze służące do zabezpieczenia biurek i szaf muszą być przechowywane w zabezpieczonym miejscu.
**10.** Po zakończeniu pracy, pracownicy są zobowiązani do zabezpieczenia pomieszczeń, a w szczególności do:

- schowania i zabezpieczenia dokumentacji;
- zabezpieczenia komputerów i nośników informacji;
- wyłączenia wszystkich urządzeń zasilanych energią elektryczną (czajniki, wentylatory itp.) zgodnie z zasadami bhp;
- zamknięcia okien i drzwi;
- zdania, kluczy od pomieszczeń biurowych/serwerowni.

**11.** Do otwierania pomieszczeń dla potrzeb wykonania czynności związanych ze sprzątaniem wykorzystywane są klucze powierzone do tego celu pracownikom obsługi. Klucze po wykonanych czynnościach osoby sprzątające zamykają w szafce zlokalizowanej w sekretariacie Urzędu. Osobą

odpowiedzialną za zorganizowanie pracy pracowników obsługi (sprzątaczek) poza godzinami pracy Urzędu jest Zastępca Wójta.

**12.** Klucze zapasowe do wszystkich pomieszczeń Urzędu są zabezpieczone i przechowywane w zamkniętej szafce zlokalizowanej w sekretariacie Urzędu. Wydawanie kluczy zapasowych pracownikom może odbywać się tylko w uzasadnionych sytuacjach oraz w przypadkach awaryjnych. Klucze zapasowe po ich wykorzystaniu należy niezwłocznie zwrócić do sekretariatu.

**13.** Raz na kwartał Zastępca Wójta będzie zlecał przeprowadzenie kontroli kompletności kluczy do wszystkich pomieszczeń Urzędu.

**14.** Otwarcie Urzędu w soboty, niedziele oraz święta możliwe jest wyłącznie w uzasadnionych przypadkach za wiedzą i zgodą Administratora – Wójta Gminy lub Zastępcy Wójta oraz w związku z przeprowadzeniem ceremonii zawarcia małżeństwa.

**15.** Naruszenie zasad polityki kluczy może spowodować wyciągnięcie konsekwencji wynikających z art. 52 Kodeksu pracy oraz z art. 363 §1. Kodeksu cywilnego.

## ROZDZIAŁ 7. Obszar w którym przetwarzane są dane osobowe

**1.** Obszar, w których przetwarzane są dane osobowe obejmuje zarówno miejsca, w których wykonuje się operacje na danych osobowych (np. wpisuje, modyfikuje, kopiuje), jak również miejsca, gdzie przechowuje się wszelkie nośniki zawierające dane osobowe. Wskazując na obszar przetwarzania danych należy uwzględnić także obszar, w którym przetwarzane są dane powierzone przez Administratora odrębnym podmiotom.

**2.** Budynki i pomieszczenia lub ich części, w których przetwarzane są dane osobowe, powinny być zabezpieczone w sposób uniemożliwiający dostęp do nich osobom nieupoważnionym, na czas nieobecności osób upoważnionych.

**3.** Budynki, pomieszczenia lub ich części, o których mowa w ust. 2 posiadają następujące zabezpieczenia:

1) drzwi do pomieszczeń, w których przetwarzane są dane osobowe są zamykane na klucz – w Urzędzie wdrożono Politykę kluczy,
2) dokumenty z danymi osobowymi zamykane są na klucz w szafach,
3) budynek objęty jest monitoringiem: kamery znajdują się na zewnątrz budynku, jak również na korytarzach;
4) budynek objęty jest systemem sygnalizacji alarmu i włamania, do którego szyfr posiadają: Wójt Gminy, Zastępca Wójta, wskazani pracownicy obsługi – Urząd posiada podpisaną umowę z firmą ochroniarską;
5) system sygnalizacji o pożarze jest podłączony do jednostek Policji i Straży Pożarnej.

**4.** Osoby upoważnione do przetwarzania danych osobowych mogą przetwarzać dane tylko w wyznaczonych do tego miejscach.

**5.** Wzór Wykazu budynków, pomieszczeń lub części pomieszczeń tworzących obszar, w którym przetwarzane są dane osobowe stanowi **Załącznik nr 14** do niniejszej Polityki bezpieczeństwa.

**6.** Wykaz budynków, pomieszczeń lub części pomieszczeń tworzących obszar, w którym przetwarzane są dane osobowe powinien być każdorazowo aktualizowany po wprowadzaniu istotnych zmian w strukturze bazy danych, którą opisuje.

## ROZDZIAŁ 8. Umowy powierzenia przetwarzania danych osobowych

**1.** Administrator realizując zapisy niniejszej Polityki bezpieczeństwa dopuszcza możliwość powierzenia przetwarzania danych osobowych podmiotom zewnętrznym. Może się to jednak odbywać wyłącznie na drodze powierzenia danego zbioru – w określonym celu i zakresie – na mocy umowy powierzenia przetwarzania danych osobowych zgodnie z art. 28 RODO.
**2.** Powierzenie przetwarzania danych osobowych może nastąpić również na podstawie aneksu do umowy lub klauzuli do umowy.
**3.** W przypadku, gdy powierzenie danych osobowych wynika wprost z zawartej z danym podmiotem umowy, nie ma konieczności sporządzania dodatkowo pisemnej umowy o powierzeniu przetwarzania danych osobowych.
**4.** Umowa lub inny akt prawny, mają formę pisemną, w tym formę elektroniczną.
**5.** Umowa powierzenia powinna określać przedmiot i czas trwania przetwarzania, charakter i cele przetwarzania, rodzaj danych osobowych i kategorie osób, których dane dotyczą, oraz obowiązki i prawa Administratora.
**6.** Każdorazowe dokonanie powierzenia danych osobowych, o którym mowa w niniejszym Rozdziale musi obligatoryjnie zostać odnotowane w wykazie zawartych umów o powierzeniu przetwarzania danych osobowych stanowiącym **Załącznik nr 15** do niniejszej Polityki bezpieczeństwa.
**7.** Administrator w zakresie prowadzonej przez siebie działalności może przetwarzać również dane osobowe powierzone mu przez inne podmioty. Administratorem, powyższych danych są podmioty przekazujące dane osobowe w powierzenie, które zobowiązane są do zawarcia pisemnej umowy o powierzeniu przetwarzania ww. danych.

## ROZDZIAŁ 9. Rejestr czynności przetwarzania danych

**1.** Administrator – na podstawie art. 30 ust. 1 RODO, jest zobowiązany prowadzić Rejestr czynności przetwarzania danych osobowych, za które odpowiada.
**2.** Rejestr, o którym mowa w ust. 1, prowadzony jest w formie pisemnej, w tym w formie elektronicznej.
**3.** Rejestr czynności przetwarzania udostępniany jest na każde żądanie organu nadzorczego.
**4.** Za prowadzenie oraz aktualizację Rejestru czynności przetwarzania odpowiada Zastępca Wójta.
**5.** Wzór Rejestru stanowi **Załącznik nr 16** do niniejszej Polityki bezpieczeństwa.

## ROZDZIAŁ 10. Audyt – Procedura przeprowadzania audytu

**1.** Dla zabezpieczenia przetwarzanych w Urzędzie Gminy określonych danych osobowych Administrator wdrożył odpowiednie środki techniczne i organizacyjne.
**2.** Zgodnie z art. 32 RODO, Administrator powinien regularnie testować, mierzyć i oceniać skuteczność zastosowanych środków technicznych i organizacyjnych mających zapewnić

bezpieczeństwo przetwarzania w Urzędzie Gminy w Brudzeniu Dużym. W tym celu Administrator przeprowadza audyt wewnętrzny. Celem audytu wewnętrznego jest ocena, czy system ochrony danych osobowych jest skutecznie wdrożony i funkcjonuje zgodnie z wymaganiami RODO. Audyt prowadzony jest w sposób obiektywny i bezstronny.

**3.** Administrator przy współpracy z Inspektorem ochrony danych (IOD) opracowuje plan i program audytów biorąc pod uwagę ważność procesów przetwarzania oraz audytowanych obszarów, jak też wyniki wcześniejszych audytów, jeżeli były prowadzone. Określa on kryteria audytu, jego cel, zakres i ewentualnie metody.

**4.** Audyt w jednostce przeprowadza się raz na rok. W wyjątkowych sytuacjach Administrator może zażądać przeprowadzenie audytu wcześniej.

**5.** Audyt przeprowadza Inspektor ochrony danych. Audyt może przeprowadzić także inna osoba wyznaczona przez Administratora.

**6.** Audytor jest zobowiązany do przygotowania się do przeprowadzenia audytu, zapoznając się z opisem audytowanego obszaru, stosowanych procedur i wyników poprzednich audytów, jeżeli były prowadzone.

**7.** Audytor realizuje działania audytowe mające na celu uzyskanie obiektywnych dowodów potwierdzających poprawność realizowanych zadań, procedur, polityk, zabezpieczeń, celów, spełniania wymagań RODO.

**8.** W przypadku stwierdzenia uchybień mających wpływ na skuteczność działania systemu ochrony danych zgodnego z RODO, audytor identyfikuje tzw. uchybienia lub spostrzeżenia.

**9.** Po zakończeniu audytu audytor przygotowuje sprawozdanie z przeprowadzonego audytu oraz oceny systemu ochrony i przetwarzania danych osobowych. Sprawozdanie jest przedstawiane Administratorowi, a następnie – po pisemnym przyjęciu do wiadomości przez Administratora – zostaje przedstawione wszystkim pracownikom. Istotnym elementem sprawozdania jest wykaz czynności, które zostaną podjęte przez Administratora w celu wyeliminowania wykrytych nieprawidłowości oraz wdrożenia nowych procedur zgodnych z RODO. Mogą to być np. szkolenia, zakup sprzętu, mebli, niszczarek, ale także przemeblowanie czy przeniesienie dokumentów do innych pomieszczeń.

**10.** Administrator przy współpracy z Inspektorem ochrony danych dokonuje przeglądu i analizy wyniku audytu oraz decyduje o inicjowaniu działań korygujących, w przypadku zaistnienia poważnych uchybień.

**11.** Audytorzy nie audytują własnej pracy.

## ROZDZIAŁ 11. Szkolenia

1. Każda osoba przed dopuszczeniem do pracy z danymi osobowymi musi być poddana przeszkoleniu i zapoznana z przepisami rozporządzenia RODO, ustawą o ochronie danych osobowych oraz dokumentacją ochrony danych osobowych wdrożoną przez Administratora w Urzędzie, tj. Polityką bezpieczeństwa danych osobowych oraz Instrukcją Zarządzania Systemem Informatycznym.
2. Po przeszkoleniu z zasad ochrony danych osobowych, uczestnicy zobowiązani są do potwierdzenia znajomości tych zasad i deklaracji ich stosowania. W tym celu uczestnicy szkolenia podpisują odpowiednie Oświadczenie o zobowiązaniu do zachowania poufności, którego wzór stanowi **Załącznik nr 2a i 2b** do niniejszej Polityki bezpieczeństwa.

3. Szkolenie z zakresu ochrony danych osobowych przeprowadzane jest raz w roku.
4. Szkolenie może mieć formę szkolenia wewnętrznego lub zewnętrznego.
5. Za przeprowadzanie szkoleń wewnętrznych w jednostce odpowiada Inspektor ochrony danych (IOD). Dopuszcza się możliwość przeprowadzania szkolenia przez pracownika Urzędu wyznaczonego przez Administratora.
6. Udział w szkoleniu zewnętrznym należy potwierdzić poprzez złożenie otrzymanego zaświadczenia lub certyfikatu.

# ROZDZIAŁ 12. Załączniki

**Załącznik nr 1 do Polityki bezpieczeństwa danych osobowych**
Określenie środków technicznych i organizacyjnych niezbędnych dla zapewnienia poufności, integralności i rozliczalności przetwarzanych danych

**1.** W Urzędzie Gminy w Brudzeniu Dużym określono środki techniczne i organizacyjne niezbędne dla zapewnienia poufności, integralności i rozliczalności przetwarzanych danych osobowych.
**2.** W Urzędzie zastosowano nw. zabezpieczenia:

**I. Środki organizacyjne:**

1) Opracowano i wdrożono dokumentację ochrony danych osobowych – Politykę bezpieczeństwa danych osobowych, Instrukcję Zarządzania Systemem Informatycznym.
2) Powołano Inspektora ochrony danych (IOD).
3) Powołano Administratora Systemów Informatycznych (ASI).
4) Do przetwarzania danych osobowych dopuszczono tylko osoby posiadające ważne upoważnienia nadane przez Administratora.
5) Prowadzona jest ewidencja osób upoważnionych do przetwarzania danych.
6) Osoby zatrudnione przy przetwarzaniu danych zaznajomiono z przepisami dotyczącymi ochrony danych osobowych.
7) Przeszkolono osoby zatrudnione przy przetwarzaniu danych osobowych w zakresie zabezpieczeń systemu informatycznego.
8) Osoby zatrudnione przy przetwarzaniu danych osobowych zobowiązano do zachowania ich w tajemnicy.
9) Monitory komputerów, na których przetwarzane są dane osobowe, ustawione są w sposób uniemożliwiający wgląd osobom postronnym w przetwarzane dane.
10) Kopie zapasowe zbioru danych osobowych przechowywane są w innym pomieszczeniu niż to, w którym znajduje się serwer, na którym dane osobowe przetwarzane są na bieżąco.
11) Przetwarzanie danych osobowych dokonywane jest w warunkach zabezpieczających dane przed dostępem osób nieupoważnionych.
12) 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.
13) Stosuje się pisemne umowy powierzenia przetwarzania danych dla współpracy z podwykonawcami przetwarzającymi dane osobowe.
14) W jednostce prowadzi się politykę czystego biurka i ekranu.

**II. Środki ochrony fizycznej:**

1) Zbiór danych osobowych przechowywany jest w pomieszczeniu zabezpieczonym drzwiami zwykłymi (niewzmacnianymi, nie przeciwpożarowymi).
2) Dostęp do pomieszczeń, w których przetwarzany jest zbiory danych osobowych objęte są systemem kontroli dostępu.
3) Dostęp do pomieszczeń, w których przetwarzany jest zbiór danych osobowych kontrolowany jest przez system monitoringu z zastosowaniem kamer przemysłowych usytuowanych na korytarzach Urzędu.

4) Zbiór danych osobowych w formie papierowej jest przechowywany w zamkniętej metalowej szafie.
5) Kopie zapasowe/archiwalne zbioru danych osobowych są przechowywane w zamkniętej metalowej szafie
6) Zbiory danych osobowych przetwarzane są w kancelarii tajnej, prowadzonej zgodnie z wymogami określonymi w odrębnych przepisach.
7) Pomieszczenie, w którym przetwarzane są zbiory danych osobowych zabezpieczone jest przed skutkami pożaru za pomocą wolnostojących gaśnic.
8) Dokumenty zawierające dane osobowe po ustaniu przydatności są niszczone w sposób mechaniczny za pomocą niszczarek dokumentów.

## III. Środki sprzętowe infrastruktury informatycznej i telekomunikacyjnej:

1) Użyto system Firewall do ochrony dostępu do sieci komputerowej.
2) Zbiór danych osobowych przetwarzany jest przy użyciu komputerów stacjonarnych i komputerów przenośnych (laptopów).
3) Zastosowano urządzenia typu UPS, chroniące system informatyczny służący do przetwarzania danych osobowych przed skutkami awarii zasilania.
4) Dostęp do systemu operacyjnego komputera, w którym przetwarzane są dane osobowe zabezpieczony jest za pomocą procesu uwierzytelnienia z wykorzystaniem identyfikatora użytkownika oraz hasła.
5) Zastosowano środki uniemożliwiające wykonywanie nieautoryzowanych kopii danych osobowych przetwarzanych przy użyciu systemów informatycznych.
6) Zastosowano systemowe mechanizmy wymuszające okresową zmianę haseł.
7) Zastosowano system rejestracji dostępu do systemu/zbioru danych osobowych.
8) Zastosowano macierz dyskową w celu ochrony danych osobowych przed skutkami awarii pamięci dyskowej.
9) Zastosowano środki ochrony przed szkodliwym oprogramowaniem takim, jak np. robaki, wirusy, konie trojańskie, rootkity.
10) Użyto system IDS/IPS do ochrony dostępu do sieci komputerowej.

## IV. Środki ochrony w ramach narzędzie programowych i baz danych:

1) Wykorzystano środki pozwalające na rejestrację zmian wykonywanych na poszczególnych elementach zbiorów danych osobowych.
2) Zastosowano środki umożliwiające określenie praw dostępu do wskazanego zakresu danych w ramach przetwarzanego zbioru danych osobowych.
3) Dostęp do zbioru danych osobowych wymaga uwierzytelnienia z wykorzystaniem identyfikatora użytkownika oraz hasła.
4) Zastosowano systemowe środki pozwalające na określenie odpowiednich praw dostępu do zasobów informatycznych, w tym zbiorów danych osobowych dla poszczególnych użytkowników systemu informatycznego.
5) Zastosowano mechanizm wymuszający okresową zmianę haseł dostępu do zbioru danych osobowych.
6) Zainstalowano wygaszacze ekranów na stanowiskach, na których przetwarzane są dane osobowe.

7) Zastosowano mechanizm automatycznej blokady dostępu do systemu informatycznego służącego do przetwarzania danych osobowych w przypadku dłuższej nieaktywności pracy użytkownika.

## Oświadczenie o zobowiązaniu do zachowania poufności

Ja niżej podpisany/na .....

..... zatrudniony/(na) na stanowisku .....

w .....

oświadczam, iż zapoznano mnie z przepisami dotyczącymi ochrony danych osobowych, w szczególności z Rozporządzeniem 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) oraz dokumentacją ochrony danych osobowych obowiązującą w Urzędzie Gminy w Brudzeniu Dużym i zobowiązuję się do:

- przetwarzania danych osobowych wyłącznie w zakresie i celu przewidzianym w powierzonych przez Administratora zadaniach,
- zachowania w tajemnicy danych osobowych, do których mam lub będę mieć dostęp w związku z wykonywaniem zadań powierzonych przez Administratora,
- niewykorzystywania danych osobowych w celach niezgodnych z zakresem i celem powierzonych przez Administratora zadań,
- zachowania w tajemnicy sposobów zabezpieczenia danych osobowych,
- ochrony danych osobowych przed przypadkowym lub niezgodnym z prawem zniszczeniem, utratą, modyfikacją danych osobowych, nieuprawnionym ujawnieniem danych osobowych, nieuprawnionym dostępem do danych osobowych oraz przetwarzaniem,
- zgłaszania sytuacji (incydentów) naruszenia ochrony danych osobowych Inspektorowi ochrony danych lub bezpośredniemu przełożonemu.

Jednocześnie oświadczam, że uzyskane, w trakcie wykonywania pracy, informacje zachowam w poufności zarówno w trakcie zatrudnienia, jak i po jego ustaniu.

| | |
|---|---|
| ..... | ..... |
| miejscowość i data | podpis osoby składającej oświadczenie |

Rozdzielnik 3 egz. w oryginale:
1 x oryginał dokumentacja ochrony danych
1 x oryginał dokumentacja kadrowa
1 x oryginał osoba upoważniona

*) niepotrzebne skreślić

# Oświadczenie o zobowiązaniu do zachowania poufności

Ja niżej podpisany/na ..... zatrudniony/(na) na stanowisku ..... w .....
oświadczam, iż zapoznano mnie z przepisami dotyczącymi ochrony danych osobowych, w szczególności z Rozporządzeniem 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) oraz dokumentacją ochrony danych osobowych obowiązującą w Urzędzie Gminy w Brudzeniu Dużym i zobowiązuję się do:

- zachowania w tajemnicy danych osobowych w sytuacji dostępu do nich podczas pełnienia obowiązków służbowych w Urzędzie Gminy w Brudzeniu Dużym wynikających z umowy o pracę/umowy praktyki/umowy stażu/umowy cywilnoprawnej*),
- zabezpieczenia tych danych przed dostępem osób nieupoważnionych, a następnie przekazania ich do dyspozycji osób upoważnionych,
- zgłaszania sytuacji (incydentów) naruszenia ochrony danych osobowych Inspektorowi ochrony danych lub bezpośredniemu przełożonemu.

Jednocześnie oświadczam, że uzyskane, w trakcie wykonywania pracy, informacje zachowam w poufności zarówno w trakcie wykonywania umowy, jak i po jej rozwiązaniu/wygaśnięciu.

| | |
|---|---|
| ..... | ..... |
| miejscowość i data | podpis osoby składającej oświadczenie |

Rozdzielnik 3 egz. w oryginale:
1 x oryginał dokumentacja ochrony danych
1 x oryginał dokumentacja kadrowa
1 x oryginał osoba składająca oświadczenie

*) niepotrzebne skreślić

.....

miejscowość, data

# Powołanie Administratora Systemów Informatycznych (ASI)

Na podstawie Rozdziału 2. Dział 2.5. Polityki bezpieczeństwa danych osobowych w Urzędzie Gminy w Brudzeniu Dużym

**powołuję na**
**Administratora Systemów Informatycznych (ASI)**

**Panią/Pana**

.....

(imię i nazwisko)

zatrudnioną/nego na stanowisku .....

w .....

(nazwa jednostki / komórki organizacyjnej)

i upoważniam do nadawania uprawnień do przetwarzania danych osobowych w systemach informatycznych funkcjonujących w Urzędzie Gminy w Brudzeniu Dużym.

Pozostały zakres obowiązków oraz warunki pełnienia funkcji Administratora Systemów Informatycznych określone są dokumentacją ochrony danych osobowych.

.....
miejscowość i data

.....
podpis Administratora

---

Ja, niżej podpisany, zobowiązuję się do pełnienia obowiązków Administratora Systemów Informatycznych (ASI) w oparciu o przepisy wewnętrzne ochrony danych osobowych obowiązujących w Urzędzie Gminy w Brudzeniu Dużym.

.....
miejscowość i data

.....
podpis pracownika

## Upoważnienie do przetwarzania danych osobowych Nr .../...

Na podstawie art. 29 rozporządzenia 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) (Dz.U.UE.L.2016.119.1) jako Administrator w Urzędzie Gminy w Brudzeniu Dużym, ul. Toruńska 2, 09–414 Brudzeń Duży, **upoważniam:**

Panią/Pana*).....

zatrudnioną/nego*) na stanowisku pracy .....w Referacie .....

Urzędu Gminy w Brudzeniu Dużym do przetwarzania danych osobowych w zbiorach:

.....

.....

(nazwy zbiorów danych objętych zakresem upoważnienia)

**W zakresie:** wglądu, wprowadzania, modyfikacji, usuwania, archiwizacji, udostępniania innym podmiotom, koniecznym do wykonywania obowiązków pracowniczych.*)

Upoważnienie dotyczy przetwarzania danych osobowych w systemach informatycznych: .....

.....

(nawy systemów lub programów)

jak również ww. zbiorach, które są prowadzone wyłącznie w formie tradycyjnej (papierowej).

Osoba upoważniona obowiązana jest przetwarzać dane osobowe zawarte w ww. zbiorach danych osobowych w zakresie i w sposób wymagany do wypełnienia obowiązków służbowych względem Administratora.

Osoba upoważniona zobowiązuje się do przetwarzania danych osobowych zgodnie z udzielonym upoważnieniem oraz z przepisami rozporządzenia 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) (Dz. Urz. Dz.U.UE.L.2016.119.1), powszechnie obowiązującym prawem oraz obowiązującymi w Urzędzie Gminy w Brudzeniu Dużym wewnętrznymi regulacjami w sprawie ochrony danych osobowych.

Naruszenie ww. obowiązków stanowi naruszenie obowiązków pracowniczych, które może być podstawą rozwiązania umowy o pracę w trybie art. 52 Kodeksu pracy lub odpowiedzialności cywilnej.

Upoważnienie jest ważne do czasu zakończenia stosunku pracy, stosunku cywilnoprawnego lub odwołania.

miejscowość i data

podpis Administratora

**Oświadczenie**

Oświadczam, że zapoznałam/em się z obowiązującymi w zakresie ochrony danych osobowych przepisami prawa i regulacjami wewnętrznymi obowiązującymi w Urzędzie Gminy w Brudzeniu Dużym. Przyjmuję do wiadomości zawarte w nich obowiązki w zakresie ochrony danych osobowych i zobowiązuję się do ich stosowania.

Świadoma/y jestem obowiązku ochrony danych osobowych na zajmowanym stanowisku i w zakresie udzielonego mi upoważnienia do przetwarzania danych osobowych, a w szczególności obowiązku zachowania w tajemnicy danych osobowych i sposobów ich zabezpieczenia, również po odwołaniu upoważnienia, a także po ustaniu zatrudnienia.

miejscowość i data

podpis osoby upoważnionej

Z chwilą udzielenia niniejszego Upoważnienia traci moc Upoważnienie do przetwarzania danych osobowych Nr ..... z dnia.....

Rozdzielnik 3 egz. w oryginale:
1 x oryginał dokumentacja ochrony danych
1 x oryginał dokumentacja kadrowa
1 x oryginał osoba upoważniona

*) niepotrzebne skreślić

# Ewidencja wydanych upoważnień do przetwarzania danych osobowych

| L.p. | Imię i nazwisko osoby upoważnionej | Zajmowane stanowisko służbowe osoby upoważnionej | Numer upoważnienia | Data nadania upoważnienia | Data odwołania/ ustania upoważnienia | Identyfikator w systemie informatycznym | Nazwy zbiorów objętych zakresem upoważnienia |
|---|---|---|---|---|---|---|---|
| | 1 | 2 | 3 | 4 | 5 | 6 | 7 |
| 1. | | | | | | | |
| 2. | | | | | | | |
| 3. | | | | | | | |
| 4. | | | | | | | |
| 5. | | | | | | | |
| 6. | | | | | | | |
| 7. | | | | | | | |
| ... | | | | | | | |

# Rejestr zbiorów danych

| L.p. | Nazwa zbioru danych | Rejestr czynności przetwarzania (TAK/NIE) | Ocena skutków (TAK/NIE) | Cel przetwarzania danych w zbiorze | Opis kategorii osób, których dane są przetwarzane w zbiorze | Zakres danych przetwarzanych w zbiorze | Podstawa prawna upoważniająca do prowadzenia zbioru danych | Sposób zbierania danych do zbioru, w szczególności informacja, czy dane do zbioru są zbierane od osób, których dotyczą, czy z innych źródeł niż osoba, której dane dotyczą | Data wpisu zbioru danych do rejestru | Data ostatniej aktualizacji informacji dotyczących zbioru danych | Rodzaj ostatniej aktualizacji |
|---|---|---|---|---|---|---|---|---|---|---|---|
| 1. | | | | | | | | | | | |
| 2. | | | | | | | | | | | |
| 3. | | | | | | | | | | | |
| 4. | | | | | | | | | | | |
| 5. | | | | | | | | | | | |
| 6. | | | | | | | | | | | |
| 7. | | | | | | | | | | | |
| … | | | | | | | | | | | |

## Wykaz zagrożeń mogących prowadzić do naruszeń

**Najczęściej występujące zagrożenia prowadzące do naruszeń to :**

**1) Organizacyjne:**

- brak nadanych upoważnień osobom przetwarzającym dane osobowe,
- brak wdrożonych polityk i procedur dotyczących ochrony danych osobowych,
- brak powołania inspektora ochrony danych osobowych w sytuacji, gdy wyznaczenie jest obligatoryjne,
- nieuprawniony dostęp do pomieszczenia, w którym są przetwarzane dane osobowe.

**2) Techniczne:**

- atak hakerski,
- działanie złośliwego oprogramowania (wirusy),
- awaria nośników danych,
- awaria sprzętu sieciowego,
- awaria serwera,
- awaria zasilania – brak ups,
- celowe lub przypadkowe uszkodzenie, zniszczenie lub nieuprawniona modyfikacja danych,
- przesłanie danych drogą mailową do złego odbiorcy.

**3) Fizyczne:**

- pożar, zalanie
- kradzież sprzętu z danymi,
- kradzież danych w wersji papierowej,
- zniszczenie danych osobowych bez użycia niszczarki,
- atak terrorystyczny,
- zwarcie instalacji elektrycznej,
- nieodpowiednie przechowywanie danych,
- utrata przetwarzanych danych,
- niewystarczający poziom zabezpieczenia pomieszczeń.

**4) Personalne:**

- nieuprawnione przeniesienie informacji zawierających dane osobowe na inny nośnik,
- wejście w posiadanie danych osobowych przez osobę nieuprawnioną,
- udostępnianie danych osobowych osobom nieupoważnionym,
- udostępnianie haseł innym pracownikom,
- nie zachowanie tajemnicy służbowej dotyczącej danych osobowych przez pracowników podczas pracy, jak i po jej zakończeniu,
- otwieranie podejrzanych maili, mogących zawierać wirusy komputerowe,
- nieuprawnione wyniesienie danych osobowych zawartych na nośniku elektronicznym.

# Wykaz przykładowych zabezpieczeń

| L.p. | Potencjalne zagrożenia | Opis zagrożenia |
|---|---|---|
| 1 | nakłanianie do wykonania czynności | mail z fakturą od rzekomego "wykonawcy/dostawcy" z informacją o zmianie numeru konta bankowego do przelewu |
| 2 | instalacja szkodliwego oprogramowania (wirusy, trojany, bacdoory) | otwarcie zainfekowanego załącznika do maila np. faktury do opłacenia |
| | | kliknięcie na hiperlink w treści wiadomości, który przekierowuje do zarażonej strony |
| | | efekty wywołane przez szkodliwe oprogramowanie: zainfekowanie przejętego komputera, utrata danych/plików, użycie przejętych komputerów do śledzenia haseł użytkowników w celu uzyskania dostępu do systemów i plików, dostęp do wewnętrznej sieci i kopiowanie lub usuwanie baz danych |
| 3 | podrzucanie nośników danych | użycie niewiadomego pochodzenia nośnika danych (który ktoś podrzucił do biura) zawierającego wirusy |
| 4 | ataki telefoniczne | intruz podając się za kogoś innego prosi o podanie hasła lub przekazanie danych osobowych |
| 5 | łatwo dostępne, standardowe hasła | nieprawidłowe przechowywanie hasła (zapisane na karteczkach, w plikach nieszyfrowanych) |
| | | stosowanie popularnych haseł, np. składającego się z imienia, qwerty, 123456789 |
| 6 | włamania do urządzeń z nieaktualnym oprogramowaniem | ataki na urządzenia sieciowe, które działają dzięki umieszczonemu na nich oprogramowaniu |
| 7 | ataki na oprogramowanie | nieaktualizowane oprogramowanie jest podatne na ataki: systemy operacyjne, serwerowe, przeglądarki internetowe |
| 8 | Skanowanie sieci i usług | skanowanie adresów IP urządzeń udostępnianych w internecie (urządzenia sieciowe, aplikacje, serwery) |

| | | |
|---|---|---|
| 9 | włamanie do sieci WIFI | uzyskanie dostępu do sieci wewnętrznej poprzez włamanie się do niechronionej sieci WIFI |
| 10 | brak aktualnej dokumentacji | brak instrukcji obsługi, dokumentacji technicznej sprzętu, instrukcji instalacyjnych i konfiguracyjnych |
| 11 | nieprzestrzeganie procedur wprowadzonych w jednostce | świadome niestosowanie się do procedur zawartych w dokumentacji ochrony danych jednostki, przekazywanie haseł do aplikacji z danymi innym osobom |
| 12 | nieuprawniony dostęp lub włamanie do pomieszczeń | dostęp do budynku, pomieszczeń biurowych, archiwum, serwerowni, miejsc gdzie przechowywane są kopie zapasowe |
| | | dostęp do wersji papierowych dokumentów zawierających dane, do aplikacji, nośników typu pendrive |
| | | kradzież dokumentów, komputerów, dysków twardych, pendrive |
| 13 | kradzież bądź zgubienie nośników danych | kradzież laptopów, pendrive, dysków wymiennych zawierających dane osobowe |
| 14 | nieprawidłowe lub brak umowy gwarancyjnej, wsparcia serwisowego | nieprzedłużenie umowy, brak zapisów dotyczących okresu gwarancji, brak zapisów dotyczących reakcji firmy na zgłoszenie |
| 15 | eskalacja uprawnień | nadawanie szerszych uprawnień użytkownikom niż wynika to z zakresu czynności, przejęcie uprawnień administratora |
| 16 | awarie/uszkodzenia infrastruktury IT | awarie: dysków, stacji roboczych, urządzeń sieciowych, serwera |
| 17 | awarie oprogramowania | niedziałający program do spraw kadrowo-płacowych, awaria poczty, strony www, baz danych |
| 18 | pożar | pożar całego obiektu, pożar w pomieszczeniu serwerowni/serwera |
| 19 | powódź | zalanie pomieszczenia serwerowni, zalanie pomieszczenia archiwum |
| 20 | przegrzanie | wysoka temperatura w serwerowni - awaria klimatyzacji i przegrzanie serwera powodujące poważną awarię |
| 21 | awaria napięcia | skoki napięcia, przerwy w dostawie zasilania |

| | | |
|---|---|---|
| 22 | nieuprawnione kopiowanie danych | kopiowanie baz danych z dysków, aplikacji, kserowanie, robienie zdjęć dokumentom przez pracownika bądź osobę zewnętrzną |
| 23 | nieuprawnione modyfikowanie/usuwanie danych | nieświadome lub pomyłkowe zmodyfikowanie/usunięcie danych, fałszowanie danych |
| 24 | brak lub błędnie wykonywane kopie zapasowe | za rzadkie wykonywanie kopii zapasowych baz danych, błędy podczas procesu kopiowania, brak możliwości odtworzenia kopii zapasowych |
| 25 | nieprawidłowe/brak procedur napraw w serwisach zewnętrznych | naprawa sprzętu z danymi osobowymi bez umowy lub zasad bezpiecznej naprawy |

# Arkusz analizy ryzyka

| L.p. | Aktywa *(środki materialne i niematerialne)* | Zidentyfikowane zagrożenia | Opis zagrożenia | Prawdopodobieństwo incydentu | Skutki wystąpienia incydentu | Ryzyko wystąpienia incydentu | Zabezpieczenia | |
|---|---|---|---|---|---|---|---|---|
| | | | | P *(skala od 1 do 3)* | S *(skala od 1 do 3)* | P x S | *(wdrożone zabezpieczenia w jednostce)* | *(planowane do wdrożenia zabezpieczenia w jednostce)* |
| 1. | | | | | | | | |
| 2. | | | | | | | | |
| 3. | | | | | | | | |
| 4. | | | | | | | | |
| 5. | | | | | | | | |
| 6. | | | | | | | | |
| 7. | | | | | | | | |
| ... | | | | | | | | |

# Raport z naruszeń zasad bezpieczeństwa ochrony danych osobowych

1. Data: ..... Godzina: .....

2. Osoba powiadamiająca o zaistniałym zdarzeniu:

.....
(imię, nazwisko, stanowisko służbowe)

3. Lokalizacja zdarzenia:

.....

.....
(nr pokoju, nazwa pomieszczenia, określenie komputerowego stanowiska roboczego, nazwa programu lub aplikacji, itp.)

4. Rodzaj naruszenia bezpieczeństwa oraz okoliczności towarzyszące naruszeniu:

.....

.....

.....

.....

5. Przyczyny wystąpienia zdarzenia:

.....

.....

.....

.....

6. Podjęte działania:

.....

.....

.....

.....

7. Skutki zdarzenia:

.....

.....

.....

.....

8. Postępowanie wyjaśniające:

.....

.....

.....

.....

.....

.....

..... .....

(data i podpis osoby zgłaszającej) (data i podpis Inspektora ochrony danych)

.....

(data i podpis Administratora Systemów Informatycznych)

.....

(data i podpis Administratora)

# Rejestr naruszeń i incydentów

| L.p. | Opis okoliczności naruszenia/incydentu<br>Art. 33 ust. 5 | Kategoria oraz ilość osób dotkniętą naruszeniem/incydentem | Skutki i konsekwencje naruszenia/incydentu<br>Art. 33 ust. 5 | Działania zaradcze<br>Art. 33 ust. 5 | Data rozpoczęcia wdrożenia działań | Data zakończenia wdrażania działań | Osoba odpowiedzialna za wdrożenie działań | Naruszenie to skutkuje ryzykiem naruszenia praw lub wolności osób fizycznych<br>Tak/Nie | Decyzja o niezgłoszeniu naruszenia -należy podać przyczynę, dla której administrator uznaje ryzyko naruszenia praw i wolności osób fizycznych za mało prawdopodobne *(jeżeli udzielono odpowiedzi NIE w kolumnie 8)*<br>Grupa robocza Art. 29 |
|---|---|---|---|---|---|---|---|---|---|
| | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 |
| 1. | | | | | | | | | |
| 2. | | | | | | | | | |
| 3. | | | | | | | | | |
| ... | | | | | | | | | |

# Zgłoszenie naruszenia ochrony danych osobowych organowi nadzorczemu

1. Data: ..... Godzina: ..... (naruszenia)

2. Osoba powiadamiająca o naruszeniu oraz inne osoby zaangażowane lub odpytane w związku z naruszeniem:

.....

.....
(imię, nazwisko, stanowisko służbowe)

3. Lokalizacja zdarzenia:

.....

.....

.....
(nr. pokoju, nazwa pomieszczenia, określenie komputerowego stanowiska roboczego, nazwa programu lub aplikacji itp.)

4. Rodzaj naruszenia i określenie okoliczności towarzyszących naruszeniu *(opisywać charakter naruszenia ochrony danych osobowych, w tym w miarę możliwości wskazywać kategorie i przybliżoną liczbę osób, których dane dotyczą, oraz kategorie i przybliżoną liczbę wpisów danych osobowych, których dotyczy naruszenie):*

.....

.....

.....

5. Podjęte działania:

.....

.....

.....

6. Wstępna ocena przyczyn wystąpienia naruszenia *(opisywać możliwe konsekwencje naruszenia ochrony danych osobowych):*

.....

.....

.....

7. Postępowanie wyjaśniające i naprawcze (*opisywać środki zastosowane lub proponowane przez administratora w celu zaradzenia naruszeniu ochrony danych osobowych, w tym w stosownych przypadkach środki w celu zminimalizowania jego ewentualnych negatywnych skutków):*

.....

.....

8. Imię i nazwisko oraz dane kontaktowe Inspektora ochrony danych lub oznaczenie innego punktu kontaktowego, od którego można uzyskać więcej informacji:

.....

.....

.....
(data i podpis Administratora)

## Upoważnienie
## do zarządzania kluczami oraz kodem cyfrowym do systemu alarmowego

Na podstawie Rozdziału 6. Dział 6.3. Polityki bezpieczeństwa danych osobowych w Urzędzie Gminy w Brudzeniu Dużym powierzam Panu/Pani*) .....

zatrudnionemu(nej) na stanowisku .....

w .....

komplet kluczy do budynku Urzędu.

W skład kompletu wchodzą następujące klucze:
1. .....
2. .....
3. .....

Ponadto przydzielam Panu/Pani kod cyfrowy do systemu alarmowego, który należy zachować w ścisłej tajemnicy i wykorzystywać zgodnie z postanowieniami w/w Polityki. *)

| | |
|---|---|
| miejscowość i data | podpis Administratora |

Oświadczam, że przyjmuję pełną odpowiedzialność za powierzone klucze oraz *) kod cyfrowy do systemu alarmowego i zobowiązuję się do ich wykorzystywania jedynie w celach realizacji powierzonych mi zadań zgodnie z niniejszym upoważnieniem.

| | |
|---|---|
| miejscowość i data | podpis pracownika |

*) niepotrzebne skreślić

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

| L.p. | Dokładny adres siedziby | Lokalizacja w budynku | Numer pokoju lub pomieszczenia | Stanowiska pracy użytkujące pomieszczenie, w którym przetwarzane są dane osobowe |
|---|---|---|---|---|
| 1. | | | | |
| 2. | | | | |
| 3. | | | | |
| 4. | | | | |
| 5. | | | | |
| 6. | | | | |
| 7. | | | | |
| ... | | | | |

# Wykaz zawartych umów o powierzeniu przetwarzaniu danych osobowych

| L.p. | Podmioty, którym Administrator powierzył przetwarzanie danych osobowych | Data zawarcia umowy | Zakres powierzonych do przetwarzania danych osobowych | Okres obowiązywania umowy | Cel zawarcia umowy |
|---|---|---|---|---|---|
| 1. | | | | | |
| 2. | | | | | |
| 3. | | | | | |
| ... | | | | | |

# Rejestr czynności przetwarzania

| L.p. | Nazwa czynności przetwarzania | Cel przetwarzania<br>Art. 30 ust. 1 pkt b | Kategorie osób<br>Art. 30 ust. 1 pkt c | Kategorie danych<br>Art. 30 ust. 1 pkt c | Podstawa prawna | Źródło danych | Planowany termin usunięcia kategorii danych *(jeżeli jest to możliwe)*<br>Art. 30 ust. 1 pkt f | Nazwa współadministratora i dane kontaktowe *(jeśli dotyczy)*<br>Art. 30 ust. 1 pkt a | Nazwa podmiotu przetwarzającego i dane kontaktowe *(jeśli dotyczy)*<br>Art. 30 ust. 1 pkt d | Kategorie odbiorców *(innych niż podmiot przetwarzający)*<br>Art. 30 ust. 1 pkt d | Nazwa systemu lub oprogramowania | Ogólny opis technicznych i organizacyjnych środków bezpieczeństwa zgodnie z art. 32 ust. 1<br>Art. 30 ust. 1 pkt g | DPIA (jeśli tak, lokalizacja raportu) | Transfer do kraju trzeciego lub org. międzynarodowej | | Osoba odpowiedzialna (kierownik referatu, samodzielne stanowisko pracy, pracownik na stanowisku pracy, ds...) |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | | | | | | | | | | | | | | Transfer do kraju trzeciego lub organizacji międzynarodowej (nazwa kraju i podmiotu)<br>Art. 30 ust. 1 pkt e | Jeśli transfer i art. 49 ust. 1 akapit drugi - dokumentacja odpowiednich zabezpieczeń<br>Art. 30 ust. 1 pkt e | |
| | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 | 11 | 12 | 13 | 14 | 15 | 16 |
| 1. | | | | | | | | | | | | | | | | |
| 2. | | | | | | | | | | | | | | | | |
| 3. | | | | | | | | | | | | | | | | |
| ... | | | | | | | | | | | | | | | | |

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

| L.p. | Lokalizacja w budynku | Numer pokoju lub pomieszczenia | Stanowiska pracy użytkujące pomieszczenie, w którym przetwarzane są dane osobowe |
|---|---|---|---|
| 1. | parter | **Bez numeru** | – Sekretariat |
| | | **1** | – **Wójt** |
| | | **2** | – **Zastępca Wójta** |
| | | **3** | – Radca prawny Urzędu |
| | | **4** | – Stanowisko ds. obsługi Rady Gminy i organów samorządowych |
| | | **5** | – Stanowiska ds. podatkowych, wymiaru podatków i księgowości podatkowej |
| | | **6** | – **Kierownik Referatu Organizacyjnego i Nadzoru**<br>– Stanowisko ds. komunalnych oraz rozwoju działalności gospodarczej |
| | | **8** | – **Kierownik Urzędu Stanu Cywilnego**<br>– Stanowisko ds. ewidencji ludności |
| 2. | **I piętro** | **9** | – **Skarbnik Gminy** |
| | | **11** | – **serwerownia** |
| | | **12** | – Stanowisko ds. księgowości analitycznej<br>– Stanowisko ds. informatyki, organizacji wyborów oraz obsługi działalności gospodarczej |
| | | **13** | – **Kierownik Referatu Finansów**<br>– Stanowisko ds. płac, rozliczeń z ZUS i Urzędem Skarbowym |
| | | **14** | – **Pełnomocnik ds. Promocji Gminy**<br>– Stanowisko ds. zarządzania funduszem sołeckim oraz zarządzania kryzysowego |
| | | **15** | – **Kierownik Referatu Gospodarki Przestrzennej i Ochrony Środowiska**<br>– Stanowisko ds. ochrony środowiska i gospodarki wodnej |

| | | | |
|---|---|---|---|
| | | **16** | – Stanowisko ds. rolnych i leśnych<br>– Stanowisko ds. gospodarki nieruchomościami |
| | | **17** | – **Kierownik Referatu Inwestycji, Spraw Komunalnych i Rolnictwa**<br>– Stanowisko ds. rozwoju gminy<br>– Stanowisko ds. zamówień publicznych |
| **3.** | **piwnica** | **Bez numeru** | – **pomieszczenia archiwum** |

Administrator powierzył przetwarzanie danych osobowych **Gminnemu Ośrodkowi Pomocy Społecznej w Brudzeniu Dużym, ul. Jana Pawła II 2A, 09-414 Brudzeń Duży** w ramach zbioru danych **Karta Dużej Rodziny** – na podstawie podpisanej Umowy powierzenia. Dane osobowe w ramach zbioru danych przetwarzane są w siedzibie GOPS w Brudzeniu Dużym.