WÓJT GMINY W SŁUPNIE
pow. płocki
woj. mazowieckie

ZARZĄDZENIE NR 148/2019
Wójta Gminy Słupno
z dnia 21 października 2019 r.

w sprawie wdrożenia Polityki
Bezpieczeństwa Przetwarzania Danych Osobowych
w Urzędzie Gminy w Słupnie

Na podstawie art. 33 ust. 3 ustawy z dnia 8 marca 1990 r. o samorządzie gminnym (Dz. U. z 2019 r. poz. 506[1]) w związku z 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 2016 Nr 119 z dnia 4 maja 2016 r.) zarządzam, co następuje:

§ 1. Wprowadzam Politykę Bezpieczeństwa Przetwarzania Danych Osobowych w Urzędzie Gminy w Słupnie, która stanowi załącznik do niniejszego zarządzenia.

§ 2. Traci moc Zarządzenie nr 91/2018 r. Wójta Gminy w Słupnie z dnia 24 maja 2018 r. w sprawie wprowadzenia Polityki bezpieczeństwa przetwarzania danych osobowych w Urzędzie Gminy w Słupnie.

§ 3. Zarządzenie wchodzi w życie z dniem podpisania.

WÓJT
Marcin Zawadka

[1] Zmiany tekstu jednolitego wymienionej uchwały ogłoszone zostały w Dz. U. z 2019 r. poz. 1309, 1696, 1815.

Załącznik do Zarządzenia Nr 148 / 2019 Wójta Gminy w Słupnie
z dnia 21 października 2019 r.
w sprawie wdrożenia Polityki bezpieczeństwa przetwarzania danych osobowych
w Urzędzie Gminy w Słupnie

POLITYKA BEZPIECZEŃSTWA PRZETWARZANIA DANYCH OSOBOWYCH W URZĘDZIE GMINY W SŁUPNIE

Rozdział 1.

Postanowienia ogólne, definicje

§ 1. 1 Polityka bezpieczeństwa przetwarzania danych osobowych w Urzędzie Gminy w Słupnie jest zbiorem zasad i procedur obowiązujących przy przetwarzaniu i wykorzystywaniu danych osobowych we wszystkich zbiorach danych osobowych administrowanych przez Urząd Gminy w Słupnie.

2. Celem niniejszej Polityki jest określenie zasad ochrony danych osobowych w Urzędzie Gminy w Słupnie oraz zapoznanie z nimi pracowników urzędu.

3. Niniejsza Polityka stanowi najwyższej rangi dokument dotyczący ochrony danych osobowych w Urzędzie Gminy w Słupnie i jest wiążąca dla wszystkich pracowników urzędu.

4. Polityka określa wymogi, zasady i regulacje ochrony danych osobowych w Urzędzie Gminy w Słupnie i jest środkiem prawnym przewidzianym w art. 24 ust. 1 RODO.

5. Mając na uwadze, że przetwarzane dane mają być adekwatne, stosowne oraz ograniczone do tego co niezbędne do celów w których są przetwarzane, pracownicy urzędu są zobligowani do przetwarzania tylko tych danych, które są niezbędne do wykonywania powierzonych zadań.

6. Polityka bezpieczeństwa przetwarzania danych osobowych w Urzędzie Gminy w Słupnie została sporządzona w oparciu o 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), ustawę o ochronie danych osobowych z dnia 10 maja 2018 r. (Dz.U. z 2018 r. poz. 1000 z późn. zm.) oraz wydanych do niej aktów wykonawczych, wytycznych i rekomendacji Urzędu Ochrony Danych Osobowych.

§ 2. W Polityce przyjęto następującą terminologię:

1) **Administrator Danych Osobowych (ADO)** – osoba decydująca o celach i środkach przetwarzania danych w Urzędzie Gminy w Słupnie ul. Miszewska 8A, 09-472 Słupno. Funkcję Administratora Ochrony Danych Osobowych pełni wójt gminy;
2) **Inspektor Ochrony Danych Osobowych (IOD)** - osoba wyznaczona przez Administratora Danych Osobowych do wypełniania zadań przewidzianych w art. 39 ust. 1 RODO;
3) **Administrator Systemów Informatycznych (ASI)** - osoba wyznaczona przez Administratora Danych Osobowych, odpowiedzialna za funkcjonowanie i bezpieczeństwo systemów informatycznych;
4) **RODO** - oznacza Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2016/679 z 27.04.2016 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, s. 1);
5) **dane osobowe** - wszelkie informacje dotyczące zidentyfikowanej lub możliwej do zidentyfikowania osobie fizycznej;
6) **zbiór danych osobowych** - uporządkowany zestaw danych osobowych posiadający określoną strukturę, prowadzony według określonych kryteriów oraz celów;
7) **przetwarzanie danych osobowych** – wykonywanie jakichkolwiek operacji na danych osobowych np. zbieranie, utrwalanie, opracowywanie, udostępnianie, zmienianie, usuwanie;
8) **odbiorca danych osobowych** - osoba fizyczna lub prawna, organ publiczny, jednostka lub inny podmiot, któremu udostępnia się dane osobowe w oparciu m.in. o umowę powierzenia;
9) **dane niezidentyfikowane** - dane osobowe, których ADO nie identyfikuje w odniesieniu do konkretnych podmiotów danych (np. zapis z monitoringu, korespondencja e-mailowa zawierająca dane osób trzecich);
10) **dane wrażliwe** - dane osobowe ujawniające pochodzenie rasowe lub etniczne, poglądy polityczne, przekonania religijne lub światopoglądowe, przynależność do związków zawodowych; dane genetyczne; dane biometryczne w celu

jednoznacznego zidentyfikowania osoby fizycznej; dane dotyczące zdrowia, seksualności lub orientacji seksualnej osoby fizycznej;

11) **naruszenie ochrony danych osobowych** - 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;

12) **osoba upoważniona** - osoba upoważniona przez ADO do przetwarzania danych osobowych w określonym przez niego zakresie;

13) **podmiot przetwarzający** - osoba fizyczna lub prawna, organ publiczny, jednostka lub inny podmiot, który przetwarza dane osobowe w imieniu Administratora;

14) **system ochrony danych osobowych** - całokształt środków technicznych, organizacyjnych i prawnych wraz z niezbędną dokumentacją, wdrożonych przez Administratora Danych Osobowych, służących zapewnieniu, że przetwarzanie danych osobowych będzie odbywało się zgodnie z przepisami z zakresu ochrony danych osobowych;

15) **zgoda** - dobrowolne, konkretne, świadome i jednoznaczne okazanie woli, którym osoba, której dane dotyczą, w formie oświadczenia lub wyraźnego działania potwierdzającego, przyzwala na przetwarzanie dotyczących jej danych osobowych;

16) **usuwanie danych** – trwałe zniszczenie danych osobowych lub taka ich modyfikacja, która nie pozwoli na ustalenie tożsamości osoby, której dane dotyczą;

17) **poufność danych** – rozumie się przez to właściwość zapewniającą, że dane nie są udostępniane nieupoważnionym osobom;

18) **użytkownik** - osoba przetwarzająca dane w systemie informatycznym oraz poza nim (np. dokumentacji w formie tradycyjnej), niezależnie od formy zatrudnienia w Urzędzie Gminy Słupno lub formy prawnej wiążącej z tą osobą. W szczególności mogą być to osoby zatrudnione na umowę o pracę, stażyści, praktykanci, osoby realizujące zadania na podstawie podpisanej umowy cywilnoprawnej;

19) **zasada minimalizacji** - dane osobowe muszą być adekwatne, stosowne oraz ograniczone do tego, co niezbędne do celów, w których są przetwarzane;
20) **ryzyku** – należy przez to rozumieć prawdopodobieństwo wystąpienia zdarzenia mającego negatywny wpływ na wykonywanie zadań bądź osiąganie celów;
21) **ryzyku w bezpieczeństwie informacji** - należy przez to rozumieć potencjalną sytuację, gdzie określone zdarzenie wykorzysta podatność (słabość) aktywów powodując szkodę w organizacji;
22) **wpływie ryzyka** - należy przez to rozumieć skutki dla realizowania zadań i osiągania celów spowodowane przez zdarzenie objęte ryzykiem;
23) **prawdopodobieństwo wystąpienia ryzyka** - należy przez to rozumieć częstotliwość występowania zdarzenia objętego ryzykiem;
24) **istotności ryzyka** - należy przez to rozumieć kombinację wpływu ryzyka i prawdopodobieństwa jego wystąpienia;
25) **akceptowanym poziomie ryzyka** - należy przez to rozumieć ustalony w Polityce poziom istotności ryzyka, przy którym nie jest wymagane podejmowanie działań przeciwdziałających ryzyku;
26) **zarządzaniu ryzykiem** - należy przez to rozumieć proces identyfikacji, oceny i przeciwdziałaniu ryzyku; proces ten obejmuje także monitorowanie ryzyka i środków podejmowanych w celu jego ograniczenia;
27) **mechanizmach kontroli** - należy przez to rozumieć wszystkie działania i procedury podejmowane lub ustanawiane w celu zwiększenia prawdopodobieństwa realizacji zadań i osiągania celów, w tym zwłaszcza:
    a) dokumentację systemu zarządzania i systemu bezpieczeństwa informacji (procedury, instrukcje, wytyczne),
    b) dokumentowanie poszczególnych zdarzeń,
    c) zatwierdzanie operacji,
    d) podział obowiązków,
    e) nadzór,
    f) rejestrowanie istotnych odstępstw od zasad zapisanych w procedurach, instrukcjach czy wytycznych,
    g) ograniczenie dostępu do zasobów materialnych, finansowych
28) **aktywach** – należy przez to rozumieć wszystko co ma wartość dla organizacji tj. aktywa podstawowe: - procesy i działania - informacje, w tym dane osobowe;

aktywa wspierające: - sprzęt (np. laptop, serwer, komputer, drukarka, dysk wymienny CD ROM, inne nośniki: papier, slajd, mikrofilm, fax) - oprogramowanie (np. aplikacje, oprogramowanie systemowe) - sieć - personel - siedziba - struktura organizacyjna

29) **poufność informacji** – należy przez to rozumieć zapewnienie, że informacja nie jest udostępniana lub ujawniana nieautoryzowanym osobom, podmiotom lub procesom (tylko uprawnieni pracownicy mają dostęp do informacji);

30) **integralność informacji** – należy przez to rozumieć zapewnienie, że dane nie zostały zmienione lub zniszczone w sposób nieautoryzowany,

31) **dostępność informacji** – należy przez to rozumieć zapewnienie, że informacje są osiągalne i możliwe do wykorzystania na żądanie, w założonym czasie, przez autoryzowany podmiot (osoby upoważnione mają dostęp do informacji i związanych z nią zasobów wtedy, gdy jest to potrzebne);

32) **rozliczalność** – zapewnienie, że działania podmiotu mogą być przypisane w sposób jednoznaczny tylko temu podmiotowi (możliwość zidentyfikowania użytkownika) odpowiedzialnego za informację, jej przetwarzanie;

33) **wójcie** – rozumie się przez to Wójta Gminy Słupno;

34) **urzędzie** – rozumie się przez to Urząd Gminy w Słupnie.

Rozdział 2.

Podmioty tworzące system ochrony danych osobowych i ich obowiązki

§ 3. 1 Funkcję Administratora Danych Osobowych (ADO) sprawuje wójt.

2. ADO realizuje zadania w zakresie ochrony danych osobowych, w tym w szczególności:

1) podejmuje decyzje o celach i środkach przetwarzania danych osobowych z uwzględnieniem przede wszystkim zmian w obowiązującym prawie, organizacji administratora danych oraz technik zabezpieczenia danych osobowych;

2) upoważnia poszczególne osoby do przetwarzania danych osobowych w określonym zakresie, odpowiadającym zakresowi jej obowiązków, oraz

odwołuje te upoważnienia lub wyrejestrowuje użytkownika z systemu informatycznego;

3) wyznacza Inspektora Ochrony Danych Osobowych i Administratora Sieci Informatycznej oraz określa zakres ich zadań i czynności;
4) zapewnia użytkownikom we współpracy z inspektorem ochrony danych osobowych i administratorem sieci informatycznej odpowiednie stanowiska i warunki pracy, umożliwiające bezpieczne przetwarzanie danych;
5) podejmuje odpowiednie działania w przypadku naruszenia lub podejrzenia naruszenia procedur.

3. ADO ujawnia dane osobowe odbiorcom danych osobowych wyłącznie po zweryfikowaniu podstawy prawnej takiego ujawnienia. W przypadku braku podstawy prawnej odmawia ujawnienia danych osobowych.

4. ADO powierza przetwarzanie danych osobowych tylko takim podmiotom przetwarzającym, które zapewniają w jego ocenie wystarczające gwarancje wdrożenia odpowiednich środków technicznych i organizacyjnych, by przetwarzanie spełniało wymogi ochrony danych osobowych i chroniło prawa osób, których dane dotyczą.

5.Każdy użytkownik zobowiązany jest w ramach wykonywania swoich obowiązków służbowych ustalić, czy następuje powierzenie danych innemu podmiotowi i niezwłocznie poinformować o tym IOD.

§ 4. 1 IOD powołuje ADO zarządzeniem w sprawie wyznaczenia Inspektora Ochrony Danych Osobowych.

2. Dane Inspektora Ochrony Danych Osobowych (IOD) publikowane są na stronie Biuletynu Informacji Publicznej oraz stronie internetowej gminy.

3. Inspektor Ochrony Danych Osobowych (IOD) odpowiada za prowadzenie i aktualizacje dokumentacji ochrony danych osobowych.

4. Inspektor Ochrony Danych Osobowych (IOD) realizuje zadania w zakresie nadzoru nad przestrzeganiem ochrony danych osobowych, w tym w szczególności:

1) sprawuje nadzór nad wdrożeniem stosowanych środków fizycznych, a także organizacyjnych i technicznych w celu zapewnienia bezpieczeństwa danych;
2) prowadzi ewidencję osób upoważnionych do przetwarzania danych osobowych oraz pozostałą dokumentację z zakresu ochrony danych, o ile jako właściwą do jej prowadzenia nie wskaże inną osobę;

3) sprawuje nadzór nad funkcjonowaniem systemu zabezpieczeń, w tym także nad prowadzeniem ewidencji z zakresu ochrony danych osobowych;
4) koordynuje wewnętrzne audyty przestrzegania przepisów o ochronie danych osobowych;
5) nadzoruje udostępnianie danych osobowych odbiorcom danych i innym podmiotom;
6) zawiera wzory dokumentów (odpowiednie klauzule w dokumentach), dotyczących ochrony danych osobowych;
7) nadzoruje prowadzenie ewidencji i innej dokumentacji z zakresu ochrony danych osobowych;
8) prowadzi oraz aktualizuje dokumentację, opisującą sposób przetwarzanych danych osobowych oraz środki techniczne i organizacyjne, zapewniające ochronę przetwarzanych danych osobowych;
9) podejmuje odpowiednie działania w przypadku naruszenia lub podejrzenia naruszenia systemu informatycznego;
10) przygotowuje wyciągi z Polityki, dostosowane do zakresów obowiązków osób upoważnionych do przetwarzania danych osobowych;
11) przygotowuje materiały szkoleniowe z zakresu ochrony danych osobowych i prowadzi szkolenia osób upoważnionych do przetwarzania danych osobowych;

5. Inspektor Ochrony Danych Osobowych ma prawo w szczególności:
1) wyznaczania, rekomendowania i egzekwowania wykonania zadań związanych z ochroną danych osobowych w urzędzie;
2) wstępu do pomieszczeń w których zlokalizowane są zbiory danych i przeprowadzanie niezbędnych badań lub innych czynności kontrolnych w celu oceny zgodności przetwarzania danych z przepisami prawa;
3) żądania złożenia pisemnych lub ustnych wyjaśnień w zakresie niezbędnym do ustalenia stanu faktycznego;
4) żądania okazania dokumentów i wszelkich danych mających bezpośredni związek z problematyką kontroli;
5) żądania udostępnienia do kontroli urządzeń, nośników oraz systemów informatycznych służących do przetwarzania danych osobowych.

§ 5. 1 ADO powołuje zarządzeniem Administratora Systemów Informatycznych (ASI) jako zarządzającego oprogramowaniem, który do 31 grudnia przeprowadza okresową ewidencję oprogramowania.

2. ASI odpowiada za bezpieczeństwo danych osobowych przetwarzanych w systemach informatycznych urzędu oraz realizuje zadania w zakresie zarządzania i bieżącego nadzoru nad systemem informatycznym administratora danych, w tym w szczególności:

1) zarządza systemem informatycznym, w którym są przetwarzane dane osobowe, posługując się hasłem dostępu do wszystkich stacji roboczych z pozycji administratora;
2) przeciwdziała dostępowi osób niepowołanych do systemu informatycznego, w którym przetwarzane są dane osobowe;
3) na wniosek wójta przydziela każdemu użytkownikowi identyfikator oraz hasło do systemu informatycznego oraz dokonuje ewentualnych modyfikacji uprawnień, a także usuwa konta użytkowników zgodnie z zasadami określonymi w instrukcji zarządzania systemem informatycznym, służącym do przetwarzania danych osobowych;
4) nadzoruje działanie mechanizmów uwierzytelniania użytkowników oraz kontroli dostępu do danych osobowych;
5) podejmuje działania w zakresie ustalania i kontroli identyfikatorów dostępu do systemu informatycznego;
6) wyrejestrowuje użytkowników na polecenie administratora danych;
7) zmienia w poszczególnych stacjach roboczych hasła dostępu, ujawniając je wyłącznie danemu użytkownikowi oraz w razie potrzeby, administratorowi bezpieczeństwa informacji lub administratorowi danych;
8) w sytuacji stwierdzenia naruszenia zabezpieczeń systemu informatycznego informuje inspektora ochrony danych osobowych o naruszeniu i współdziała z nim przy usuwaniu skutków naruszenia;
9) prowadzi szczegółową dokumentację naruszeń bezpieczeństwa danych osobowych przetwarzanych w systemie informatycznym;
10) sprawuje nadzór nad wykonywaniem napraw, konserwacją oraz likwidacją urządzeń komputerowych, na których zapisane są dane osobowe, nad wykonywaniem kopii zapasowych, ich przechowywaniem oraz okresowym

sprawdzaniem pod katem ich dalszej przydatności do odtwarzania danych w przypadki awarii systemu informatycznego;

11) podejmuje działania, służące zapewnieniu niezawodności zasilania komputerów, innych urządzeń mających wpływ na bezpieczeństwo przetwarzania danych oraz zapewnieniu bezpiecznej wymiany danych w sieci wewnętrznej i bezpiecznej teletransmisji.

Rozdział 3.
Osoby przetwarzające dane osobowe i ich obowiązki

§ 6. 1. Przetwarzania danych osobowych w ramach urzędu mogą dokonywać wyłącznie osoby upoważnione przez ADO.

2. ADO na pisemny wniosek bezpośredniego przełożonego, nadaje upoważnienie do przetwarzania danych osobowych, którego wzór stanowi załącznik **Nr 1 do Polityki.**

3. Osoba upoważniona do przetwarzania danych osobowych zobowiązana jest zapoznać się z niniejszą Polityką oraz odbyć szkolenie z zakresu danych osobowych. Dokonanie powyższych czynności potwierdzane jest w **załączniku Nr 2 do Polityki.**

4. Osoba upoważniona do przetwarzania danych osobowych jest zobowiązana w szczególności do:

1) stosowania określonych w urzędzie procedur i środków przetwarzania oraz zabezpieczania danych osobowych;
2) zachowania wyjątkowej staranności przy przetwarzaniu danych osobowych, w szczególności danych wrażliwych w celu ochrony interesów osób, których dane dotyczą;
3) zabezpieczenia danych osobowych przed: ich utratą, uszkodzeniem lub zniszczeniem, zmianą lub ich udostępnieniem osobom nieupoważnionym;
4) dopilnowania, aby przebywanie osób nieupoważnionych w pomieszczeniach, w których przetwarzane są dane osobowe, miało miejsce wyłącznie w obecności osoby upoważnionej;

5) polityki „czystego biurka" – w trakcie pracy na biurku powinny być tylko te dokumenty, które są niezbędne do wykonywania obowiązków służbowych. W przypadku opuszczenia stanowiska pracy dokumenty zawierające dane, powinny być zabezpieczone przed dostępem osób nieuprawnionych;
6) polityki „czystego ekranu" – w przypadku chwilowego opuszczenia stanowiska pracy należy wylogować się z systemu, bądź zablokować dostęp do pulpitu stacji roboczej w celu uniemożliwienia dostępu do systemu operacyjnego lub aplikacji przez osoby nieuprawnione;
7) dopilnowania, aby przeznaczone do usunięcia dokumenty, nośniki zawierające dane osobowe niszczone były w stopniu uniemożliwiającym ich odczytanie - zabronione jest wyrzucanie dokumentów do koszy na śmieci bez ich właściwej anonimizacji;
8) przestrzegania procedur właściwego użytkowania systemów informatycznych, w których przetwarza się dane osobowe, w tym do nieujawniania innym użytkownikom swoich loginów i haseł;
9) zachowania należytej staranności podczas przekazywania danych osobowych drogą telefoniczną (konieczność właściwej identyfikacji rozmówcy, konieczność ustalenia, czy rozmówca jest uprawniony do pozyskania danych osobowych, przekazywanie jedynie niezbędnych informacji);
10) zachowania należytej ostrożności przy transporcie dokumentów oraz nośników informatycznych, zawierających dane osobowe, poza obszarem przetwarzania w urzędzie;
11) niepozostawiania dokumentów, zawierających dane osobowe na urządzeniach wielofunkcyjnych (np. drukarkach);
12) przetwarzania danych osobowych tylko w wyznaczonych do tego celu pomieszczeniach służbowych;
13) zabezpieczenia zbiorów oraz dokumentów zawierających dane osobowe przed dostępem osób nieupoważnionych;
14) nieudzielania informacji o danych osobowych przetwarzanych w urzędzie innym podmiotom i osobom, chyba, że obowiązek taki wynika wprost z przepisów prawa i tylko w sytuacji gdy przesłanki określone w tych przepisach zostały spełnione;

15) bezzwłocznego zawiadamiania w formie pisemnej ADO o wszelkich przypadkach naruszenia bezpieczeństwa danych osobowych i systemu informatycznego przetwarzającego dane osobowe, a także o przypadkach utraty lub kradzieży dokumentów lub innych nośników zawierających dane osobowe;
16) pisemnego wnioskowania o zewidencjonowanie nowych zbiorów danych osobowych w wykazie prowadzonym przez IOD;
17) występowania z wnioskami w sprawie wprowadzenia niezbędnych zmian w zakresie ochrony danych osobowych;
18) niezwłocznego tj. w ciągu 24 godzin od zaistnienia zdarzenia informowania ADO i IOD o naruszeniach ochrony danych osobowych w tym potencjalnych naruszeniach, lub w przypadku naruszeń bezpieczeństwa dotyczących systemów informatycznych ASI, oraz niezwłocznego tj. w ciągu 2 dni roboczych informowania IOD o żądaniach osób, których dane osobowe dotyczą;
19) niezwłocznego informowania IOD o wszelkich innych zdarzeniach mających wpływ na realizację obowiązków wynikających z niniejszej Polityki.

5. Osoba upoważniona do przetwarzania danych osobowych obowiązana jest dołożyć należytej staranności w celu ochrony interesu osób, których dane są gromadzone i przetwarzane, a w szczególności należy przestrzegać, aby dane te były:

1) przetwarzane zgodnie z powszechnie obowiązującym prawem i regulacjami wewnętrznymi;
2) poprzedzone obowiązkiem informacyjnym;
3) zbierane dla oznaczonych, zgodnych z prawem celów i nie poddawane dalszemu przetwarzaniu niezgodnemu z tymi celami;
4) merytorycznie poprawne i adekwatne w stosunku do celów, w jakich są przetwarzane;
5) przechowywane w postaci umożliwiającej identyfikację osób, których dotyczą, nie dłużej niż jest to niezbędne do osiągnięcia celu przetwarzania.

6. Naczelnicy wydziałów, dyrektorzy biur i osoby na samodzielnych stanowiskach urzędu zobowiązani są w szczególności do:

1) zarządzania zasobem danych osobowych w ramach zadań realizowanych przez podległych im pracowników;

2) występowania z wnioskiem do ADO o nadanie, zmianę i cofnięcie upoważnień dotyczących dostępu do zasobu danych osobowych podległym pracownikom;
3) zgłaszania do IOD zamiaru utworzenia zbioru danych osobowych oraz informacji dotyczących zmian w zakresie i sposobach przetwarzania tego zbioru;
4) przestrzegania obowiązków dotyczących obszaru przetwarzania, wykazu osób upoważnionych do przetwarzania danych osobowych, zastosowania zabezpieczeń zbiorów;

7. ADO prowadzi ewidencję osób upoważnionych do przetwarzania danych osobowych zgodnie z **załącznikiem Nr 3 do Polityki.**

8. Osoby, które zostały upoważnione do przetwarzania danych osobowych winny zachować je w tajemnicy, jak i sposoby ich zabezpieczania, w trakcie oraz po ustaniu zatrudnienia, co potwierdza się podpisaniem stosownego oświadczenia zawartego w upoważnieniu do przetwarzania danych osobowych **zgodnie z załącznikiem nr 1 do Polityki.**

Rozdział 4.
Obszary i zakres przetwarzania danych osobowych

§ 7. 1 Znajdujące się w zasobach urzędu wszelkie informacje o zidentyfikowanej lub możliwej do zidentyfikowania osobie fizycznej przetwarzane zarówno w formie tradycyjnej (papierowej), jak i elektronicznej stanowią dane osobowe i podlegają ochronie stosownie do przepisów RODO oraz przepisów krajowych regulujących ochronę danych osobowych.

2. Dane osobowe przetwarzane w urzędzie winny być przetwarzane wyłącznie w przypadkach o których mowa w art. 6 ust. 1.

3. Za aktualność określenia obszaru i zakresu przetwarzania danych osobowych odpowiadają naczelnicy wydziałów, dyrektorzy biur i osoby na samodzielnych stanowiskach urzędu, którzy niezwłocznie pisemnie o każdej zmianie informują IOD.

4. Obszar przetwarzania danych osobowych w urzędzie obejmuje budynek, pomieszczenia, w których przetwarzane są dane osobowe (miejsca, w których wykonuje się operacje na danych osobowych, tj. wpisuje, zmienia, kopiuje), oraz

miejsca, gdzie przechowuje się nośniki informacji zawierające dane osobowe (szafy z dokumentacją papierową, szafy zawierające elektroniczne nośniki informacji, pomieszczenia, w których składowane są uszkodzone nośniki danych).

5. Zakres przetwarzania danych osobowych w urzędzie obejmuje dane osobowe w zakresie zbioru danych osobowych.

6. Obszar i zakres przetwarzania danych osobowych określony jest w **załączniku Nr 4 do Polityki.**

§ 8. 1. W przypadku jeśli przetwarzanie danych osobowych odbywa się na podstawie art. 6 ust. 1 lit. a) RODO (czyli na podstawie zgody osoby, której dane dotyczą) pracownicy urzędu są zobligowani do uzyskania (przed przystąpieniem do przetwarzania) zgody osoby której dane dotyczą zgodnie z przepisami prawa w szczególności z art. 7 i 8 RODO.

2. Osoba o której mowa w ust. 1 składa stosowne oświadczenie stanowiące **załącznik nr 5 do Polityki.**

3. Zgoda może zostać wycofana w dowolnym momencie poprzez złożenie stosownego oświadczenia stanowiącego **załącznik nr 6 do Polityki** przez osobę, której dane dotyczą. Wycofanie zgody nie wpływa na zgodność z prawem przetwarzania, którego dokonano na podstawie zgody przed jej wycofaniem.

§ 9. 1. W momencie pozyskiwania danych osobowych ADO winien spełnić obowiązek informacyjny zgodnie z art. 13 i 14 RODO.

2. Obowiązek informacyjny o którym mowa w ust 1 przekazuje się w formie pisemnej klauzuli informacyjnej stanowiącej **załącznik nr 7 do Polityki**, która dostępna jest w szczególności:

1) w obszarach przetwarzania danych osobowych,
2) na stronie internetowej urzędu oraz w Biuletynie Informacji Publicznej Urzędu Gminy Słupno,
3) w przyjętych wzorach formularzy, dokumentów i oświadczeń,
4) w treści zawieranych umów, ogłoszeń i regulaminów.

3. Wzór klauzuli informacyjnej dla zbioru danych „monitoring wizyjny" stanowi **załącznik nr 8 do Polityki.**

§ 10. 1 ADO prowadzi rejestr kategorii czynności przetwarzania zgodny z art. 30 RODO.

2. Rejestr kategorii czynności przetwarzania prowadzony jest w formie elektronicznej.

3. Wzór rejestru kategorii czynności przetwarzania stanowi **załącznik nr 9 do Polityki.**

Rozdział 5.
Środki techniczne i organizacyjne niezbędne dla zabezpieczenia obszarów i zakresów przetwarzania danych osobowych

§ 11. 1. 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 urzędu.

2. Budynek urzędu podlega ochronie polegającej na całodobowym monitorowaniu przez systemy alarmowe zamontowane w obszarach oraz monitoring wewnętrzny.

3. ADO w porozumieniu z ASI wyznacza i upoważnia osoby do kodowania i rozkodowywania systemu alarmowego oraz otwierania i zamykania budynku urzędu przez rozpoczęciem i po zakończeniu pracy przez użytkowników.

4. Osoby upoważnione do otwierania i zamykania budynku urzędu odpowiedzialne są za wydawanie kluczy użytkownikom danych obszarów przetwarzania.

5. Klucze do pomieszczeń biurowych przechowywane są w skrzynce zamykanej na klucz.

6. Upoważnieni przez ADO użytkownicy danych obszarów przetwarzania odbierając klucze poświadczają ten fakt w książce ewidencji wydawania kluczy. Klucze do obszarów wielostanowiskowych pobiera użytkownik, który jako pierwszy przybywa do pracy, a zdaje który jako ostatni kończy pracę.

7. Wzór książki ewidencji książki do wydawania kluczy, o którym mowa w ust. 6 stanowi **załącznik nr 10 do Polityki.**

8. Na użytkowniku danego obszaru przetwarzania od momentu pobrania kluczy do momentu ich zdania spoczywa pełną odpowiedzialność za jego zabezpieczenie.

9. Po zakończeniu pracy osoby upoważnione do kodowania i rozkodowywania systemu alarmowego oraz otwierania i zamykania budynku urzędu przez rozpoczęciem i po zakończeniu pracy przez użytkowników sprawdzają kompletność

zadanych kluczy. W przypadku stwierdzenia braków, sporządza notatkę i przekazuje ją do ADO.

§ 12. 1. Duplikaty kluczy, będące kluczami zapasowymi do obszarów przetwarzania są przechowywane w osobnej zamkniętej szafce metalowej i podlegają zabezpieczeniu przez upoważnionego użytkownika w sposób uniemożliwiający pobranie ich przez nieupoważnionych użytkowników.
2. Wydawanie kluczy zapasowych o którym mowa w ust. 1 może odbywać się tylko w sytuacjach awaryjnych za zgodą ADO – za pokwitowaniem w odpowiednim rejestrze wraz z uzasadnieniem konieczności wydania kluczy zapasowych.
3. Klucze zapasowe po ich wykorzystaniu należy niezwłocznie zwrócić do depozytu za poświadczeniem zwrotu w rejestrze.
4. Wzór rejestru, o którym mowa w ust. 3 – „Książka ewidencji kluczy zapasowych" stanowi **załącznik nr 11 do Polityki.**

Rozdział 6.
Powierzenie przetwarzania danych

§ 13. 1. ADO może powierzyć innemu podmiotowi przetwarzanie danych osobowych.
2. ADO Korzysta wyłącznie z usług takich podmiotów przetwarzających, które zapewniają wystarczające gwarancje wdrożenia odpowiednich środków technicznych i organizacyjnych by przetwarzanie spełniało wymogi RODO i chroniło prawa osób, których dane dotyczą.
3. Powierzenie przetwarzania danych osobowych odbywa się na podstawie umowy zawartej na piśmie pomiędzy ADO a danym podmiotem, któremu zleca się czynności związane z przetwarzaniem danych osobowych.
4. Właściciel zasobów danych osobowych przygotowuje projekt umowy powierzenia danych osobowych innemu podmiotowi, który przekazuje IOD do akceptacji. Pomocniczy wzór umowy stanowi **załącznik nr 12 do Polityki.**

§ 14. 1. Podmiot przetwarzający dane osobowe jest zobowiązany do zastosowania środków organizacyjnych i technicznych, zabezpieczających zbiór

przed dostępem osób nieupoważnionych na zasadach określonych w przepisach o ochronie danych osobowych.

2. Podmiot, o którym mowa w ust. 1, jest zobowiązany przetwarzać dane osobowe wyłącznie w zakresie określonym w umowie.

3. Podmiot przetwarzający dane osobowe ponosi odpowiedzialność za ochronę przetwarzanych danych osobowych.

4. ADO prowadzi ewidencję podmiotów przetwarzających, z którymi zawarł umowy o powierzenie przetwarzania danych osobowych stanowiącą **załącznik nr 13 do Polityki**.

Rozdział 7.
Zarządzanie ryzykiem

§ 15. 1 Celem zarządzania ryzykiem w urzędzie jest:

1) usprawnienie procesu planowania;
2) zwiększenie prawdopodobieństwa realizacji zadań i osiągania celów;
3) uzyskanie bezpieczeństwa informacji, w tym danych osobowych;
4) zapewnienie odpowiednich mechanizmów kontroli;
5) zapewnienie ADO wczesnej informacji o zagrożeniach dla realizacji wyznaczonych celów i zadań.

2. Zarządzanie ryzykiem odbywa się według zasad:

1) integracji z procesem zarządzania;
2) powiązania z celami i zadaniami urzędu;
3) przypisania odpowiedzialności;
4) proporcjonalności działań przeciwdziałających ryzyku do jego istotności.

§ 16. 1 Proces zarządzania ryzykiem obejmuje:

1) identyfikację i ocenę ryzyka oraz odniesienie go do akceptowanego poziomu ryzyka;
2) ustalenie metody przeciwdziałania ryzyku;
3) przeciwdziałanie ryzyku;
4) monitorowanie procesu i dokonywanie zmian.

2. Identyfikacja i ocena ryzyka oraz ustalenie metody przeciwdziałania ryzyku dokonywane jest podczas przygotowywania do realizacji zadań urzędu w danym roku.

§ 17. 1 Identyfikacja ryzyka polega na ustaleniu ryzyka zagrażającego poszczególnym celom i zadaniom realizowanym przez urząd oraz na ustaleniu ryzyk zagrażających utracie poufności, integralności, dostępności i rozliczalności aktywów (w tym m.in. informacji, danych osobowych, sprzętu).

2. Podczas identyfikacji należy przeanalizować:

1) cele i zadania proponowane do realizacji w danym roku przez urząd;
2) zagrożenia, związane z osiąganiem celów i realizowaniem zadań przez urząd, wraz z ich wewnętrznymi i zewnętrznymi przyczynami oraz możliwymi scenariuszami rozwoju zdarzeń;
3) zagrożenia związane z utratą poufności, integralności, rozliczalności i dostępności do informacji i danych, w tym danych osobowych.

3. Podczas identyfikacji stosowana jest kategoryzacja ryzyka.

4. Ustala się następujące kategorie (obszary) ryzyka:

1) ryzyko finansowe;
2) ryzyko dotyczące zasobów ludzkich;
3) ryzyko działalności;
4) ryzyko zewnętrzne.

Przykłady ryzyka występującego w ramach powyższych kategorii stanowi załącznik **załącznik nr 14 do Polityki.**

5. W ramach systemu bezpieczeństwa informacji i danych osobowych ustala się następujące kategorie (obszary) ryzyka;

1) ryzyko naruszenia bezpieczeństwa informacji;
2) ryzyko awarii technicznej;
3) ryzyko nieautoryzowanego działania;
4) ryzyko naruszenia bezpieczeństwa funkcji;
5) ryzyko utraty podstawowych usług;
6) ryzyko zniszczenia fizycznego;
7) ryzyko związane z wystąpieniem zjawiska naturalnego.

Przykłady ryzyka występującego w ramach powyższych kategorii (obszarów) stanowi **załącznik nr 15 do Polityki.**

§ 18. 1 Ocena ryzyka polega na określeniu wpływu i prawdopodobieństwa wystąpienia ryzyka, a następnie ustaleniu jego istotności według zasad określonych w § 17.

2. Określenie wpływu ryzyka polega na określeniu przewidywanych skutków jakie będzie miało, dla realizacji zadania lub osiągania celu w działaniu urzędu, wystąpienie zdarzenia objętego ryzykiem. Do określenia wpływu używany jest opis jakościowy przy zastosowaniu skali ocen: wysoki, średni, niski.

3. Określenie prawdopodobieństwa wystąpienia ryzyka polega na określeniu przewidywanej częstotliwości występowania zdarzenia objętego ryzykiem w trakcie roku. Do określenia prawdopodobieństwa stosowany jest opis jakościowy przy zastosowaniu skali ocen: wysokie, średnie, niskie.

4. Podczas określania wpływu i prawdopodobieństwa ziszczenia się ryzyka stosowane są zasady zawarte w **załączniku nr 16 do Polityki.**

§ 19. 1. W oparciu o dokonaną ocenę wpływu i prawdopodobieństwa wystąpienia ryzyka ustalany jest poziom istotności ryzyka wskazany w **załączniku nr 16 do Polityki.**

2. Ustala się następujące poziomy istotności ryzyka:

1) ryzyko poważne tj. ryzyko o wysokim wpływie oraz wysokim lub średnim prawdopodobieństwie oraz średnim wpływie i wysokim prawdopodobieństwie;
2) ryzyko umiarkowane tj. ryzyko o wysokim wpływie i niskim prawdopodobieństwie, ryzyko o średnim wpływie oraz średnim prawdopodobieństwie, a także ryzyko o niskim wpływie i wysokim prawdopodobieństwie;
3) ryzyko niskie tj. ryzyko o niskim wpływie oraz średnim lub niskim prawdopodobieństwie.

3. Ryzykiem akceptowanym jest ryzyko niskie oraz ryzyko umiarkowane. Ryzyko poważne przekracza akceptowany poziom ryzyka.

4. Ryzyko przekraczające akceptowany poziom ryzyka wymaga ustalenia i podjęcia działań ograniczających je do poziomu umiarkowanego lub niskiego poprzez zmniejszenie jego wpływu lub prawdopodobieństwa ziszczenia się (przeciwdziałanie ryzyku).

§ 20. 1. Metodami przeciwdziałania ryzyku są;

1) kontrolowanie ryzyka - podejmowanie działań zaradczych pozwalających na ograniczenie ryzyka do akceptowanego poziomu m. in. poprzez wzmocnienie mechanizmów kontroli wewnętrznej, w tym zwłaszcza procedury, instrukcje, upoważnienia, podział obowiązków, nadzór, szkolenia;
2) akceptacja - zaniechanie podejmowania działań zaradczych z uwagi na brak możliwości wskazania takich działań, które byłyby skuteczne lub w przypadku, gdy koszt podjętych działań zaradczych jest wyższy niż koszt poniesienia ryzyka;
3) przeniesienie ryzyka - przekazanie ryzyka podmiotowi zewnętrznemu np. w drodze ubezpieczenia, zlecenie wykonania usługi;
4) unikanie – zaprzestanie/zawieszenie działań rodzących zbyt duże ryzyko;

2. W celu określenia metody przeciwdziałania ryzyku należy przeanalizować:

1) przyczyny (źródła) ryzyka i możliwe scenariusze rozwoju wydarzeń;
2) istniejące mechanizmy kontroli stosowane w celu ograniczenia lub uniknięcia tego ryzyka;
3) skuteczność istniejących mechanizmów kontroli, tj. zakres w jakim przeciwdziałają ryzyku, a poprzez to ułatwiają lub utrudniają realizację ustalonych celów i zadań.

§ 21. 1. Naczelnicy wydziałów, dyrektorzy biur, osoby na samodzielnych stanowiskach dokonują identyfikacji ryzyka, oceny ryzyka oraz określenia metod przeciwdziałania ryzyku, na etapie opracowywania propozycji celów i zadań na dany rok budżetowy, wypełniając „Arkusze identyfikacji, oceny oraz określenia metody przeciwdziałaniu ryzyku", zwane dalej „Arkuszami", według wzoru zamieszczonego w **załączniku nr 17 do Polityki.**

2. W ramach systemu bezpieczeństwa informacji i danych osobowych, naczelnicy wydziałów, dyrektorzy biur, osoby na samodzielnych stanowiskach identyfikują aktywa organizacji do zagrożeń (utrata poufności, integralności, dostępności, rozliczalności), identyfikują ryzyka oraz wskazują stosowane w komórce organizacyjnej zabezpieczenia techniczne i organizacyjne, a następnie dokonuje szacowania ryzyka, według wzoru stanowiącego **załącznik nr 18 do Polityki.**

3. Arkusze przedkładane są do dnia 31 stycznia każdego roku, celem weryfikacji i akceptacji: - sekretarzowi urzędu w zakresie zidentyfikowanych ryzyk dotyczących realizacji zadań i celów przez urząd, - IOD w zakresie zidentyfikowanych ryzyk w bezpieczeństwie informacji i danych osobowych.

4. Sekretarz i IOD przekazują ADO informację o najistotniejszych ryzykach zagrażających realizacji celów i zadań urzędu w formie rejestru ryzyk, stanowiący załącznik **nr 19 i 20 do Polityki.**

§ 22. 1. Naczelnicy wydziałów, dyrektorzy biur, osoby na samodzielnych stanowiskach zapewniają stosowanie metod przeciwdziałania ryzyku ustalonych w Arkuszach.

2. Przynajmniej raz w roku należy dokonać przeglądu ryzyk wpisanych do w/w arkuszy.

3. W wyniku przeglądu mogą zostać usunięte z arkusza znajdujące się w nim ryzyka lub zostać wprowadzone nowe. Może również ulec zmianie istotność ryzyka oraz sposoby reakcji na nie.

4. Zidentyfikowane ryzyko oraz ustalone metody jego ograniczania do akceptowanego poziomu są na bieżąco oceniane (monitorowane) przez:

1) Naczelników wydziałów, dyrektorów biur, osoby na samodzielnych stanowiskach, którzy oceniają poziom zidentyfikowanego ryzyka oraz skuteczność stosowanych metod jego ograniczania;
2) IOD w zakresie bezpieczeństwa informacji, danych osobowych w ramach audytów ochrony danych osobowych i bezpieczeństwa informacji;
3) Wójta w ramach bieżącego zarządzania urzędem, w tym w szczególności w trakcie narad z naczelnikami wydziałów, dyrektorami biur, osobami na samodzielnych stanowiskach,

5. Efektywność zarządzania ryzykiem oraz system kontroli podlega niezależnej i obiektywnej ocenie przez audyt wewnętrzny oraz wewnętrzny audyt bezpieczeństwa informacji.

6. Wyniki oceny, o której mowa w ust. 4 i 5, wykorzystywane są do poprawy efektywności zarządzania ryzykiem oraz usprawnienia systemu zarządzania urzędem.

Rozdział 8.
Udostępnianie danych osobowych

§ 23. 1. ADO udostępnia dane osobowe przetwarzane we własnych zbiorach tylko osobom lub podmiotom uprawnionym do ich otrzymania na mocy przepisów prawa.

2. Dane osobowe mogą być udostępniane w następujących przypadkach:
   1) na podstawie wniosku od podmiotu uprawnionego do otrzymywania danych osobowych na podstawie przepisów;
   2) na podstawie umowy z innym podmiotem, w ramach której istnieje konieczność udostępnienia danych;
   3) na podstawie wniosku osoby, której dane dotyczą.

3. Wniosek o udostępnienie danych osobowych powinien zawierać informacje umożliwiające wyszukanie żądanych danych osobowych w zbiorze oraz wskazywać ich zakres i przeznaczenie.

4. Udostępniając dane osobowe należy zaznaczyć, że można je wykorzystać wyłącznie zgodnie z przeznaczeniem, dla którego zostały udostępnione.

5. W przypadku żądania udzielenia informacji na temat przetwarzanych danych osobowych na pisemny wniosek pochodzący od osoby, której dane dotyczą, odpowiedź na wniosek następuje w terminie 30 dni od daty jego otrzymania, chyba że przepisy stanowią inaczej.

6. Właściciel zasobów danych osobowych jest odpowiedzialny za przygotowanie danych osobowych do udostępnienia w zakresie wskazanym we wniosku.

7. Prawo dostępu przysługujące osobie, której dane dotyczą jest realizowane zgodnie z przepisami art. 15 RODO.

§ 24. Odmowa udostępnienia danych osobowych następuje wówczas, gdy spowodowałoby to istotne naruszenia dóbr osobistych osób, których dane dotyczą, lub innych osób oraz jeżeli dane osobowe nie mają istotnego związku ze wskazanymi we wniosku motywami działania wnioskodawcy.

Rozdział 9.

Postępowanie w przypadkach naruszenia bezpieczeństwa ochrony danych osobowych

§ 25. 1 Użytkownicy są zobowiązani do szczególnej staranności przy przetwarzaniu danych osobowych.

2. Użytkownicy każdorazowo przed przystąpieniem do pracy są zobowiązani do dokonania oceny i oględzin miejsca pracy pod kątem, czy nie dokonano jakichkolwiek nieuprawnionych działań związanych z ochroną danych osobowych przez osoby nieuprawnione.

3. Za naruszenie ochrony danych osobowych uważa się naruszenie bezpieczeństwa prowadzące do przypadkowego lub niezgodnego z prawem zniszczenia, utracenia, zmodyfikowania, nieuprawnionego ujawnienia lub nieuprawnionego dostępu dodanych osobowych przesyłanych, przechowywanych lub w inny sposób przetwarzanych, a w szczególności:

1) nieuprawniony dostęp lub próbę dostępu do systemu lub pomieszczeń, w których następuje proces przetwarzania danych (widoczne uszkodzenia bądź naruszenia zabezpieczeń);
2) naruszenie lub próbę naruszenia integralności zbioru danych lub integralności danych osobowych;
3) nieautoryzowane zniszczenie lub próbę zniszczenia danych zgromadzonych w zbiorach papierowych lub systemie;
4) zmianę lub utratę danych zapisanych na kopiach zapasowych lub archiwalnych dokonaną w sposób nieautoryzowany lub niezaplanowany;
5) nieuprawniony dostęp osoby nieuprawnionej (sygnał o nielegalnym logowaniu lub inny objaw wskazujący na próbę lub działanie związane z nielegalnym dostępem do systemu);
6) inny stan systemu lub pomieszczeń (wskazujący np. na włamanie) niż pozostawiony przez użytkownika po zakończeniu lub po przerwie w pracy z systemem;
7) podejrzenie o wycieku danych osobowych;

8) zagubienie, w szczególności zgubienie lub kradzież nośnika z danymi: np. pendrive, płyta CD, dysk, dokumenty lub nieautoryzowane / nieplanowane usunięcie danych osobowych;
9) podejrzenie, że do systemów lub pomieszczeń, gdzie są przetwarzane dane osobowe miały dostęp osoby nieuprawnione.

4. Naruszenia dotyczą zarówno danych osobowych przetwarzanych w formie elektronicznej, jak i papierowej.

5. Każdy pracownik jest zobowiązany do niezwłocznego poinformowania IOD, o każdym przypadku złamania zasad przetwarzania danych, a w szczególności o sytuacjach udostępnienia danych osobom nieuprawnionym.

6. IOD po identyfikacji problemu dokonuje klasyfikacji naruszenia. Naruszenie klasyfikowane jest jako:
1) nieskutkujące ryzykiem naruszenia praw lub wolności osób fizycznych;
2) skutkujące ryzykiem naruszenia praw lub wolności osób fizycznych.

7. Naruszenie kwalifikuje się jako naruszenie ochrony danych podlegające zgłoszeniu w ciągu 72h do Prezesa Urzędu Ochrony Danych Osobowych jeśli skutkuje ryzykiem naruszenia praw lub wolności osób fizycznych w szczególności, jeżeli konsekwencją naruszenia jest np. utrata kontroli nad danymi osobowymi lub ograniczenie praw osób, których dane dotyczą, dyskryminacja, kradzież lub sfałszowanie tożsamości, strata finansowa, nieuprawnione odwrócenie pseudonimizacji, naruszenie dobrego imienia, naruszenie poufności danych osobowych chronionych tajemnicą zawodową lub wszelkie inne znaczne szkody gospodarcze lub społeczne.

8. IOD prowadzi rejestr naruszeń ochrony danych osobowych stanowiący załącznik **nr 21 do Polityki.**

Rozdział 10.
Sprawozdanie roczne z funkcjonowania systemu ochrony danych osobowych

§ 26. 1. Corocznie do dnia 30 marca IOD przygotowuje sprawozdanie roczne z funkcjonowania systemu ochrony danych osobowych i przekazuje do ADO.

2. Sprawozdanie przygotowywane jest w formie pisemnej.

Rozdział 11.
Postanowienia końcowe

§ 27. 1. Niniejsza Polityka obowiązuje na wszystkich stanowiskach oraz obszarach, gdzie dochodzi do przetwarzania informacji podlegających ochronie.

2. Niniejsza Polityka podlega regularnym przeglądom i aktualizacjom dokonywanym przez IDO i ADO.

3. W sprawach nieuregulowanych w Polityce mają zastosowanie przepisy RODO i innych aktów prawnych dotyczących ochrony danych osobowych.

4. Integralną część Polityki stanowią następujące załączniki:

1) Załącznik nr 1 Upoważnienie do przetwarzania danych osobowych;
2) Załącznik nr 2 Oświadczenie o zapoznaniu się z Polityką Bezpieczeństwa Przetwarzania Danych Osobowych oraz odbyciu szkolenia z zakresu danych osobowych;
3) Załącznik nr 3 Ewidencja osób upoważnionych do przetwarzania danych osobowych;
4) Załącznik nr 4 Obszar i zakres przetwarzania danych osobowych;
5) Załącznik nr 5 Zgoda na przetwarzanie danych osobowych;
6) Załącznik nr 6 Wycofanie zgody na przetwarzanie danych osobowych;
7) Załącznik nr 7 Klauzula Informacyjna dotycząca przetwarzania danych osobowych;
8) Załącznik nr 8 Klauzula Informacyjna dotycząca monitoringu wizyjnego;
9) Załącznik nr 9 Rejestr kategorii czynności przetwarzania;
10) Załącznik nr 10 Książka ewidencji wydania kluczy;
11) Załącznik nr 11 Książka ewidencji wydania kluczy zapasowych;
12) Załącznik nr 12 Wzór umowy przetwarzania danych osobowych;
13) Załącznik nr 13 Ewidencja podmiotów przetwarzających;
14) Załącznik nr 14 Kategorie (obszary) ryzyka;
15) Załącznik nr 15 Kategorie (obszary) ryzyka;
16) Załącznik nr 16 Zasady oceny wpływu ryzyka;
17) Załącznik nr 17 Arkusz identyfikacji, oceny oraz określenia metody przeciwdziałaniu ryzyku;

18) Załącznik nr 18 Arkusz identyfikacji, oceny oraz określenia metody przeciwdziałaniu ryzyku w ramach systemu bezpieczeństwa informacji i danych osobowych;
19) Załącznik nr 19 Rejestr ryzyk;
20) Załącznik nr 20 Rejestr ryzyk w ramach systemu bezpieczeństwa informacji i danych osobowych;
21) Załącznik nr 21 Rejestr naruszeń ochrony danych osobowych.

WÓJT
Marcin Zawadka