Zarządzenie Nr 83/ 2018
Wójta Gminy Wiskitki
z dnia 20 lipca 2018 r.

w sprawie wdrożenia dokumentacji ochrony danych osobowych

Na podstawie art. 24 ust. 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/W (ogólne rozporządzenie o ochronie danych osobowych) zarządzam, co następuje:

§ 1. 1. W celu wykazania zgodności przetwarzania danych osobowych w Urzędzie Gminy Wiskitki wdrażam do stosowania:

1) Politykę Ochrony Danych Osobowych stanowiącą załącznik Nr 1 do niniejszego Zarządzenia oraz
2) Instrukcje zarządzania systemem informatycznym stanowiącą załącznik Nr 2 do niniejszego Zarządzenia

2. Powyższe dokumenty są dokumentami wewnętrznymi Urzędu Gminy dotyczącymi bezpieczeństwa danych osobowych i mogą być udostępnione wyłącznie właściwym organom.

§ 2. Zobowiązuję wszystkich pracowników do zapoznania się z dokumentami, o których mowa w § 1.

§ 3. Zarządzenie wchodzi w życie z dniem podpisania.

Łukasz Choiński
wyznaczony do pełnienia funkcji
Wójta Gminy Wiskitki

Załącznik Nr 2
do Zarządzenia Nr 83
Wójta Gminy Wiskitki
z dnia 20 lipca 2018 r.

Instrukcja zarządzania systemem informatycznym służącym do przetwarzania danych osobowych w URZĘDZIE GMINY WISKITKI

Lipiec 2018 rok

Instrukcja zarządzania systemem informatycznym służącym do przetwarzania danych osobowych, zwana dalej Instrukcją, przyjęta została w celu wykazania, że dane osobowe w Urzędzie Gminy Wiskitki w systemach informatycznych przetwarzane są w sposób zgodny z przepisami prawa mającymi zastosowanie do takiej czynności, zgodnie z zasadą art. 5 ust. 2 Rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z 27 kwietnia 2016 r. *w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE* (zwane dalej RODO). Instrukcja jest dokumentem powiązanym z Polityką ochrony danych osobowych w zakresie zarządzania system informatycznym służącym do przetwarzania danych osobowych.

§ 1
Definicje

1) **Administrator Danych Osobowych** – Urząd Gminy Wiskitki, w imieniu którego działa Wójt – Kierownik jednostki;
2) **dane osobowe** – oznaczają wszelkie informacje o zidentyfikowanej lub możliwej do zidentyfikowania osobie fizycznej (osobie, której dane dotyczą);
3) **system informatyczny administratora danych** – rozumie się przez to sprzęt komputerowy, oprogramowanie, dane eksploatowane w zespole współpracujących ze sobą urządzeń, programów, procedur przetwarzania informacji i narzędzi programowych. W systemie tym pracuje co najmniej jeden komputer centralny i system ten tworzy sieć teleinformatyczną administratora danych;
4) **użytkownik** – rozumie się osobę upoważnioną przez Administratora Danych Osobowych do przetwarzania danych osobowych w Urzędzie Gminy Wiskitki, której nadano identyfikator i przyznano hasło;
5) **sieć lokalna** - połączenie systemów informatycznych Administratora Danych wyłącznie dla własnych potrzeb przy wykorzystaniu urządzeń i sieci telekomunikacyjnych;
6) **zbiór danych** - każdy posiadający strukturę zestaw danych o charakterze osobowym, dostępny według określonych kryteriów, niezależnie od tego, czy zestaw ten jest rozproszony lub podzielony funkcjonalnie;
7) **przetwarzanie danych osobowych** – oznacza operację (czynność) lub zestaw operacji wykonywanych na danych osobowych lub zestawach danych osobowych w sposób zautomatyzowany lub niezautomatyzowany, taką jak zbieranie, utrwalanie, organizowanie, porządkowanie, przechowywanie, adaptowanie lub modyfikowanie, pobieranie, przeglądanie, wykorzystywanie, ujawnianie poprzez przesłanie, rozpowszechnianie lub innego rodzaju udostępnianie, dopasowywanie lub łączenie, ograniczanie, usuwanie lub niszczenie;
8) **zabezpieczenie danych w systemie Informatycznym** - wdrożenie i eksploatacja stosowanych środków technicznych i organizacyjnych zapewniających ochronę danych przed Ich nieuprawnionym przetwarzaniem;
9) **uwierzytelnienie** – rozumie się przez to działanie, którego celem jest weryfikacja deklarowanej tożsamości podmiotu;
10) **identyfikator użytkownika** – oznacza ciąg znaków literowych, cyfrowych lub innych jednoznacznie identyfikujący osobę upoważnioną do przetwarzania

danych osobowych w systemie informatycznym - Użytkownika w razie przetwarzania danych osobowych w systemie;

11) **hasło** – oznacza ciąg znaków alfanumerycznych (literowych, cyfrowych lub innych), znany jedynie osobie uprawnionej do pracy w systemie informatycznym - Użytkownikowi.

§ 2
Bezpieczeństwo teleinformatyczne

1. Przy ochronie zasobów kluczowe jest stosowanie podstawowej zasady bezpieczeństwa, że nie jest dozwolone wykorzystywanie zasobów w sposób inny niż jawnie dozwolony.
2. Do wykonywania obowiązków służbowych związanych z przetwarzaniem danych osobowych dozwolone jest używanie systemów, urządzeń i oprogramowania dopuszczonych do użytku zgodnie z wymogami ***Polityki ochrony danych osobowych*** oraz ***Instrukcji zarządzania systemem informatycznym służącym do przetwarzania danych osobowych***.
3. Pracownicy są uprawnieni do korzystania z zasobów teleinformatycznych niezbędnych do wykonywania przez nich obowiązków służbowych. Za określenie takich zasobów dla każdego pracownika i przyznanie dostępu odpowiedzialny jest Kierownik jednostki. Szczegółowe zasady przyznawania uprawnień opisano w § 3 Instrukcji.
4. Zakazane jest użytkowanie na terenie obszaru przetwarzania danych lub przy wykonywaniu obowiązków służbowych poza obszarem przetwarzania danych innych niż dopuszczone urządzeń, systemów i oprogramowania bez zgody Administratora Danych Osobowych i Informatyka.
5. Zakazane jest bez zgody Informatyka:
   a) użytkowanie urządzeń skutkujących połączeniem systemów Administratora Danych Osobowych z sieciami teleinformatycznymi innych podmiotów, w tym publicznymi sieciami teleinformatycznymi,
   b) użytkowanie urządzeń lub oprogramowania mających na celu zakłócenie działania innych systemów, urządzeń lub oprogramowania,
   c) użytkowanie urządzeń lub oprogramowania do testowania bezpieczeństwa lub wykrywania podatności,
   d) użytkowanie urządzeń lub oprogramowania mogących naruszyć bezpieczeństwo innych systemów lub urządzeń,
   e) wprowadzanie zmian konfiguracji urządzeń, systemów lub oprogramowania.
6. Zakazane jest bez zgody Administratora Danych Osobowych wykorzystywanie urządzeń do niejawnego przekazywania lub rejestracji danych dotyczących informacji chronionych, w tym głosu i obrazu, tj.: magnetofonów, dyktafonów, aparatów fotograficznych, kamer, telefonów komórkowych z opcją rejestrowania dźwięku i obrazu, rejestratorów ruchu sieciowego, rejestratorów pracy klawiatur itp.
7. Wykorzystanie należących do Administratora Danych Osobowych urządzeń, systemów i oprogramowania oraz innych zasobów do prywatnych celów pracowników jest dozwolone jedynie na uzasadniony wniosek pracownika i za zgodą Administratora Danych Osobowych w porozumieniu z Inspektorem Ochrony Danych i Informatykiem.
8. Zasoby Administratora Danych Osobowych powinny być przechowywane w taki sposób, aby zapobiec możliwości ich kradzieży lub uszkodzenia przez osoby

postronne oraz przypadkowe uszkodzenia przez osoby lub czynniki środowiskowe.

9. Wynoszenie aktywów (zasobów i informacji) poza obszar przetwarzania danych możliwe jest za zgodą Administratora Danych Osobowych.
10. Zakazane jest przesyłanie informacji podlegających ochronie na prywatne adresy poczty elektronicznej oraz prowadzenie korespondencji służbowej z wykorzystaniem prywatnego adresu e-mail użytkownika.
11. Zakazane jest używanie prywatnych nośników zewnętrznych (np. typu pendrive) i tworzenie nieautoryzowanych kopii baz danych.
12. Pracownicy są zobowiązani do ochrony zasobów będących własnością innych podmiotów, a powierzonych lub oddanych do dyspozycji Administratorowi Danych Osobowych lub udostępnionych pracownikom na czas wykonywania przez nich czynności służbowych w takim samym stopniu jak w przypadku zasobów będących własnością Administratora Danych Osobowych.

§ 3
Procedury nadawania uprawnień do przetwarzania danych i rejestrowania tych uprawnień w systemie informatycznym

1. Za bezpieczeństwo danych osobowych w systemie informatycznym odpowiedzialny jest Administrator Danych Osobowych.
2. Do obsługi systemu informatycznego oraz urządzeń wchodzących w jego skład, służących do przetwarzania danych, mogą być dopuszczone wyłącznie osoby posiadające pisemne upoważnienie wydane przez Administratora Danych Osobowych,
3. Po upoważnieniu osoby do dostępu do przetwarzania danych osobowych w systemie informatycznym zostaje jej nadany Identyfikator użytkownika. Z chwilą nadania identyfikatora osoba może uzyskać dostęp do systemów informatycznych w zakresie odpowiednim do danego upoważnienia.
4. Dla każdego użytkownika systemu informatycznego ustalony jest odrębny identyfikator i hasło.
5. Identyfikator użytkownika nie może być zmieniany, a po wyrejestrowaniu użytkownika z systemu informatycznego nie może być przydzielony innej osobie.
6. Identyfikator osoby, która utraciła uprawnienia do dostępu do danych osobowych, zostaje niezwłocznie wyrejestrowany z systemu informatycznego, w którym są przetwarzane, zaś hasło dostępu zostaje unieważnione oraz zostają podjęte inne działania niezbędne w celu zapobieżenia dalszemu dostępowi tej osoby do danych.
7. Przełożony, który jest odpowiedzialny za określenie zakresu obowiązków podległych pracowników, w sytuacji gdy przydziela pracownikowi zadania związane z przetwarzaniem danych osobowych, występuje za pośrednictwem stanowiska ds. kadr do Administratora Danych o udzielenie upoważnienia imiennego do przetwarzania danych.
8. W przypadku, gdy pracownik kończy zadanie związane z przetwarzaniem danych osobowych, przełożony pracownika występuje do Administratora Danych o cofnięcie uprawnień do przetwarzania danych osobowych.
9. W przypadku ustania stosunku pracy cofnięcie pracownikowi upoważnienia do przetwarzania danych osobowych przygotowuje osoba na stanowisku ds. kadr i jednocześnie niezwłocznie informuje Informatyka o tym fakcie. Informatyk bez zbędnej zwłoki dokonuje stosownych czynności w systemie informatycznym.

§ 4
Metody i środki uwierzytelnienia oraz procedury związane z ich zarządzaniem I użytkowaniem

1. W systemie informatycznym stosuje się uwierzytelnianie na poziomie dostępu do systemu operacyjnego. Do uwierzytelnienia użytkownika na poziomie dostępu do systemu operacyjnego stosuje się hasło oraz identyfikator użytkownika.
2. Hasła użytkowników umożliwiające dostęp do systemu informatycznego utrzymuje się *w* tajemnicy również po upływie ich ważności.
3. Minimalna długość hasła przydzielonego użytkownikowi wynosi 8 znaków alfanumerycznych, w skład którego wchodzi duża i mała litera, cyfra i znak specjalny. Historia haseł obliguje użytkownika do nadania hasła innego przez następne 12 miesięcy. Hasło nie może być identyczne jak identyfikator użytkownika ani jego imieniem i nazwiskiem.
4. Hasła powinny być często zmieniane nie rzadziej niż co 30 dni. Inspektor Ochrony Danych Osobowych lub Informatyk może, w uzasadnionych sytuacjach polecić dokonanie zmiany hasła przez użytkownika np. po każdym incydencie lub podejrzeniu naruszenia bezpieczeństwa danych osobowych.
5. Zabrania się użytkownikom systemu udostępniania swojego identyfikatora i hasła innym osobom oraz korzystania przez osoby upoważnione do przetwarzania danych osobowych z identyfikatora lub hasła innego użytkownika.
6. Dla każdej osoby, której dane osobowe są przetwarzane w systemie informatycznym, system zapewnia odnotowanie:
   a) daty pierwszego wprowadzenia danych do systemu,
   b) identyfikatora użytkownika wprowadzającego dane osobowe do systemu.
   c) informacji o odbiorcach, którym dane osobowe zostały udostępnione.
7. Hasła użytkowników uprzywilejowanych (tzw. użytkowników posiadających uprawnienia na poziomie administratorów systemów informatycznych) są zabezpieczone u Administratora Danych Osobowych na wypadek sytuacji awaryjnych, w szczególności w przypadku nieobecności administratora systemu informatycznego.

§ 5
Procedura rozpoczęcia, zawieszenia i zakończenia pracy przez użytkowników systemu

1. Pracownik po przyjściu do pracy uruchamia stację roboczą.
2. Przed uruchomieniem komputera należy sprawdzić, czy nie zostały do niego podłączone żadne niezidentyfikowane urządzenia.
3. Po uruchomieniu pracownik loguje się przy pomocy identyfikatora użytkownika oraz hasła do systemu informatycznego.
4. W trakcie pracy przy każdorazowym opuszczeniu stanowiska komputerowego należy dopilnować, aby na ekranie nie były wyświetlane dane osobowe.

5. Przy opuszczaniu stanowiska na dłuższy czas należy ustawić ręcznie blokadę klawiatury i wygaszacz ekranu (wygaszacz aktywujący się po 15 minutach braku aktywności).
6. Zmianę użytkownika stacji roboczej musi poprzedzać wylogowanie się poprzedniego użytkownik. Niedopuszczalne jest, aby dwóch lub większa liczba użytkowników wykorzystywała wspólne konto użytkownika.
7. Zakończenie pracy użytkownika w systemie informatycznym obejmuje wylogowanie się użytkownika z aplikacji.

§ 6
Tworzenie kopii zapasowych zbiorów danych

1. Dane osobowe, przetwarzane w systemie informatycznym, podlegają zabezpieczeniu poprzez tworzenie kopii zapasowych. Za proces tworzenia kopii zapasowych odpowiada Informatyk lub inna osoba wyznaczona przez Administratora Danych Osobowych.
2. Kopie zapasowe informacji przechowywanych w systemie informatycznym, przetwarzającym dane osobowe tworzone są za pomocą aplikacji DataProtector, a przechowywane są na macierzy dyskowej.
3. Wszystkie dane archiwizowane winny być identyfikowane, tj. zawierać takie informacje jak datę dokonania zapisu oraz identyfikator zapisanych w kopii danych.
4. Brak wykonywania kopii na stacjach roboczych użytkowników.

§ 7
Sposób, miejsce i okres przechowywania elektronicznych nośników informacji zawierających dane osobowe oraz kopii zapasowych

1. Nośniki danych zarówno w postaci elektronicznej, jak i papierowej powinny być zabezpieczone przed dostępem osób nieuprawnionych, nieautoryzowaną modyfikacją i zniszczeniem. Dane osobowe mogą być zapisywane na nośnikach przenośnych w przypadku tworzenia kopii zapasowych lub gdy istnieje konieczność przeniesienia tych danych w postaci elektronicznej, a wykorzystanie do tego celu sieci informatycznej jest nieuzasadnione lub zbyt niebezpieczne.
2. Nośników z danymi zarchiwizowanymi nie należy przechowywać w tych samych pomieszczeniach, w których przechowywane są zbiory danych osobowych używane na bieżąco.
3. Nośniki informacji, kopie zapasowe, które nie są przeznaczone do udostępnienia, przechowuje się w warunkach uniemożliwiających dostęp do nich osobom niepowołanym.
4. Kopie, które są już nieprzydatne, należy zniszczyć fizycznie lub stosując wymazywanie poprzez wielokrotny zapis nieistotnych informacji w obszarze zajmowanym przez dane kasowane.
5. Nośniki danych osobowych oraz wydruki powinny być przechowywane w zamkniętych szafach i nie powinny być bez uzasadnionej przyczyny wynoszone poza ten obszar. Przekazywanie nośników danych osobowych i wydruków poza miejscem pracy powinno się odbywać za wiedza i zgoda Administratora Danych Osobowych.

§ 8
Sposób zabezpieczenia systemu informatycznego przed działalnością wirusów komputerowych, nieuprawnionym dostępem oraz awariami zasilania

1.System informatyczny jest zabezpieczony przed działaniem oprogramowania, którego celem jest uzyskanie nieuprawionego dostępu oraz przed działaniami inicjowanymi z sieci zewnętrznej. Zabezpieczenie obejmuje:

Lp.	Obszar chroniony	Rodzaj ochrony	Typ
1.	Stacje robocze	System antywirusowy	Wpisać nazwę programu antywirusowego
2.		Firewall	Systemowy (windows)
3.		Szyfrowanie nośników danych	brak
4.	Sieć wewnętrzna	System antywirusowy	Brak skanowania
5.		Firewall	Pfsense (FreeBSD)
6.	Poczta e-mail	Szyfrowanie danych	Brak szyfrowania danych (jedynie obsługa połączeń SSL/TLS)
7.		System antywirusowy i antyspamowy	CLAMAV / SPAMASSASIN

2. Użytkowany system jest automatycznie skanowany w czasie rzeczywistym, a pełne skanowanie komputera odbywa się w interwale raz w tygodniu.
3. Aktualizacja bazy wirusów odbywa się poprzez automatyczne pobieranie bazy wirusów przez program antywirusowy co godzinę, bądź ręcznie na żądanie.
4. W przypadku wykrycia wirusa użytkownik powinien:
a) uruchomić program antywirusowy i skontrolować użytkowany system,
b) usunąć wirusa z systemu przy wykorzystaniu programu antywirusowego.
Jeżeli operacja usunięcia wirusa się nie powiedzie, użytkownik musi:
a) zakończyć pracę w systemie komputerowym,
b) odłączyć zainfekowany komputer od sieci,
c) powiadomić niezwłocznie o zaistniałej sytuacji Informatyka i Administratora Danych Osobowych.
6. Informatyk poddaje kwarantannie zainfekowany komputer i usuwa zagrożenie.
7. Urządzenia i nośniki zawierające dane osobowe przekazywane poza obszar, w którym są one przetwarzane, zabezpiecza się w sposób

zapewniający poufność i integralność danych.

§ 9
Poczta elektroniczna

1. Pracownicy mogą korzystać z poczty elektronicznej wyłącznie w celach służbowych.
2. Administrator Danych Osobowych może poznawać treść wiadomości elektronicznych wykorzystywanych przez pracowników znajdujących się we wszystkich systemach administratora.
3. Zabronione jest otwieranie wiadomości e-mail pochodzących od nieznanego nadawcy bądź z podejrzanym tytułem [tzw. *phishinge-mail].* W szczególności zabronione jest otwieranie linków bądź pobieranie plików zapisanych w komunikacji zewnętrznej od nieznanego nadawcy.

§ 10
Sposoby realizacji w systemach wymogów dotyczących przetwarzania danych osobowych

1. Informacje o odbiorcach danych zapisane są w systemie informatycznym, z którego nastąpiło udostępnienie.
2. Informacja o odbiorcy danych zapisana jest w systemie informatycznym przy uwzględnianiu daty i zakresu udostępnienia, a także dokładnego określenia odbiorcy danych.
3. Możliwe jest sporządzenie i wydrukowanie raportu zawierającego, w powszechnie zrozumiałej formie, powyższe informacje.

§ 11
Procedury wykonywania przeglądów i konserwacji systemów oraz nośników informacji służących do przetwarzania danych osobowych

1. Przeglądy kontrolne, serwis sprzętu i oprogramowania powinny być dokonywane przez firmy serwisowe, z którymi zostały zawarte umowy zawierające postanowienia zobowiązujące je do przestrzegania zasad poufności informacji uzyskanych w ramach wykonywanych zadań.
2. Przy dokonywaniu serwisu należy przestrzegać następujących zasad:

a) czynności serwisowe powinny być wykonywane - w obecności osoby upoważnionej do przetwarzania danych osobowych,
b) przed rozpoczęciem tych czynności dane i programy znajdujące się w systemie powinny zostać zabezpieczone przed ich zniszczeniem, skopiowaniem lub niewłaściwą zmianą,
c) prace serwisowe należy ewidencjonować protokołem zakończenia danych czynności.
d) w przypadku prac serwisowych dokonywanych przez podmiot zewnętrzny, wymagających dostępu do danych osobowych, z podmiotem takim powinny zostać zawarte stosowne umowy powierzenia danych osobowych.

Łukasz Choiński
wyznaczony do pełnienia
funkcji
Wójta Gminy Wiskitki

Załącznik Nr 1
do Zarządzenia Nr 83/2018
Wójta Gminy Wiskitki
z dnia 20 lipca 2018

POLITYKA OCHRONY DANYCH OSOBOWYCH W URZĘDZIE GMINY WISKITKI

Lipiec 2018 rok

Spis treści

Załączniki:

Nr 1 – Wykaz pomieszczeń, w których przetwarzane są dane osobowe
Nr 2 - Wykaz stosowanych programów i aplikacji
Nr 3 - Wzór upoważnienia
Nr 4 – Ewidencja osób upoważnionych
Nr 5 - Wykaz umów powierzeń
Nr 6 - Wzór rejestru czynności przetwarzania danych osobowych
Nr 7 – Wykaz komputerów
Nr 8 – Ewidencja urządzeń przenośnych
Nr 9 – Oświadczenie pracownika

WPROWADZENIE

Niniejsza Polityka ochrony danych osobowych w dalszej części zwana „Polityką" określa zasady, procedury przetwarzania i bezpieczeństwa danych osobowych stosowane w Urzędzie Gminy Wiskitki w celu spełnienia wymagań Rozporządzenia Parlamentu Europejskiego i Rady (UE) nr 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).
Niniejszy dokument jest jednym ze środków organizacyjnych wprowadzonych przez Administratora Danych Osobowych, którym potwierdza, że przetwarzanie danych osobowych odbywa się zgodnie z ww. Rozporządzeniem.
Kierownik jednostki deklaruje dołożenie wszelkich starań, aby zasady i procedury ujęte w niniejszej Polityce były przestrzegane przez pracowników.

Rozdział I

CEL POLITYKI

§ 1. Celem opracowania dokumentu Polityki ochrony danych osobowych jest zdefiniowanie ogólnych wymagań i zasad ochrony informacji, które będą fundamentem dla wszystkich dokumentów związanych z bezpieczeństwem danych osobowych, zarówno w wersji papierowej, jak i elektronicznej oraz dla tworzonego systemu zarządzania bezpieczeństwem danych osobowych w jednostce.

§ 2. Polityka niniejsza została opracowana dla:
1) zapewnienia maksymalnego poziomu bezpieczeństwa w procesie przetwarzania danych osobowych tj.: ochrony przed nieupoważnionym dostępem do danych i ich modyfikacją, utratą poufności przy zachowaniu integralności i rozliczalności danych poprzez właściwą organizację tego procesu oraz wprowadzenie odpowiednich działań przy wykorzystaniu odpowiednich środków technicznych, organizacyjnych i informatycznych,
2) podnoszenia świadomości pracowników poprzez szkolenia,
3) reagowania na wszelkiego rodzaju naruszenia bezpieczeństwa danych osobowych.

§ 3. Wdrożenie niniejszej Polityki jest ważne dla wskazania należytej dbałości o poufność, integralność i dostępność informacji podczas kontaktów ze stronami zewnętrznymi.

Rozdział II

DEFINICJE

1) **RODO** – Rozporządzenie Parlamentu Europejskiego i Rady (UE) Nr 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;

2) **ustawa** - Ustawa z dnia 10 maja 2018 r. o ochronie danych osobowych;

3) **Administrator Danych Osobowych (ADO)** – 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 Urzędzie Gminy Wiskitki jest nim Wójt.

4) **Inspektor Ochrony Danych (IOD)** – osoba, podmiot wyznaczony przez Administratora Danych Osobowych do informowania i doradzania w zakresie obowiązującego prawa dotyczącego ochrony danych osobowych, monitorowania przestrzegania zasad ochrony danych osobowych oraz działania jako punktu kontaktowego dla osób, których dane są przetwarzane, a także dla organu nadzorczego;

5) **Informatyk lub ASI** – osoba fizyczna lub prawna wyznaczona przez Administratora Danych Osobowych nadzorująca pracę systemu informatycznego oraz wykonująca w nim czynności wymagające specjalnych uprawnień;

6) **użytkownik systemu informatycznego** – pracownik Administratora Danych Osobowych posiadający upoważnienie do pracy w systemie informatycznym, zgodnie z zakresem obowiązków służbowych;

7) **dane osobowe** – oznaczają wszelkie informacje o zidentyfikowanej lub możliwej do zidentyfikowania osobie fizycznej (osobie, której dane dotyczą);

8) **dane osobowe sensytywne (wrażliwe)** – to szczególna kategoria danych osobowych ujawniająca: pochodzenie rasowe, etniczne, poglądy polityczne, przekonania religijne lub filozoficzne, dane genetyczne, dane biometryczne (wizerunek, źrenica oka, linie papilarne, głos), dane dotyczące zdrowia, niepełnosprawności, życia seksualnego lub orientacji seksualnej, środki zabezpieczenia społecznego, postępowania karne, sankcje karne;

9) **przetwarzanie danych osobowych** – oznacza operację (czynność) lub zestaw operacji wykonywanych na danych osobowych lub zestawach danych osobowych w sposób zautomatyzowany lub niezautomatyzowany, taką jak zbieranie, utrwalanie, organizowanie, porządkowanie, przechowywanie, adaptowanie lub modyfikowanie, pobieranie, przeglądanie, wykorzystywanie, ujawnianie poprzez przesłanie, rozpowszechnianie lub innego rodzaju

udostępnianie, dopasowywanie lub łączenie, ograniczanie, usuwanie lub niszczenie;

10) **podmiot przetwarzający (procesor)** – osoba fizyczna lub prawna, organ publiczny przetwarzający dane osobowe w imieniu Administratora Danych Osobowych;

11) **odbiorca danych osobowych** – osoba fizyczna lub prawna, organ publiczny lub inna jednostka, któremu ujawnia się (przekazuje) dane osobowe, niezależnie od tego czy jest stroną trzecią;

12) **profilowanie** – forma zautomatyzowanego przetwarzania danych osobowych, polegająca na wykorzystaniu danych osobowych do oceny niektórych czynników osobowych osoby fizycznej, w szczególności do analizy lub prognozy efektów jej pracy, sytuacji ekonomicznej, zdrowia, osobistych preferencji, zainteresowań, wiarygodności, zachowania, lokalizacji lub przemieszczania się;

13) **pseudonimizacja** – przetwarzanie danych osobowych w taki sposób, aby danych nie można było przypisać do określonego podmiotu danych bez użycia dodatkowych informacji np. lista nazwisk i numerów. Warunkiem jest przechowywanie tych dodatkowych informacji w odrębnym miejscu i zapewnienie, że dane osobowe nie są przypisane do zidentyfikowanej lub możliwej do zidentyfikowania osoby fizycznej;

14) **anonimizacja** – zmiana danych osobowych, w wyniku której dane tracą charakter danych osobowych;

15) **zgoda osoby, której dane dotyczą** – to dobrowolne, dowolnie określone, konkretne, świadome i jednoznaczne wyrażone za pomocą oświadczenia lub wyraźnego działania potwierdzającego wyrażającego zgodę na przetwarzanie jej danych osobowych. Zgoda musi być udokumentowana, aby ją udowodnić;

16) **ocena skutków** – proces przeprowadzany przez Administratora Danych Osobowych (może być z uczestnictwem Inspektora Ochrony Danych), gdy istnieje prawdopodobieństwo wysokiego ryzyka dla praw i wolności osób fizycznych, których dane osobowe są przetwarzane. Proces ten musi ocenić wpływ planowanych operacji przetwarzania danych na ochronę danych osobowych;

17) **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;

18) **organ nadzorczy** – oznacza niezależny organ publiczny ustanowiony przez państwo członkowskie, zgodnie z art. 51 RODO. W Polsce organem nadzorczym jest Prezes Urzędu Ochrony Danych Osobowych.

Rozdział III

ZASADY OGÓLNE

§ 4. Administrator Danych Osobowych zapewnia, że dane osobowe są przetwarzane zgodnie z niżej wymienionymi zasadami:

1) **legalności** – dane osobowe przetwarzane są zgodnie z prawem, na podstawie jednej z przesłanek wymienionych w art. 6 ust.1 lit. a do f RODO,

2) **celowości** – dane osobowe są przetwarzane w wyraźnym, konkretnym i prawnie uzasadnionym celu (konkretne cele przetwarzania danych osobowych powinny być wyraźne, uzasadnione i określone w momencie ich zbierania),

3) **adekwatności** – przetwarzane są tylko te dane, które są niezbędne ze względu na cel ich zbierania, wymaga to w szczególności zapewnienia ograniczenia okresu przechowywania danych do minimum,

4) **merytorycznej poprawności** – zbierane dane osobowe są poprawne i w razie potrzeby uaktualniane,

5) **ograniczenia przechowywania danych** – przechowywanie danych osobowych w formie umożliwiającej identyfikację osoby, której dane dotyczą przez okres nie dłuższy niż jest to niezbędne do celów, w którym dane te są przetwarzane,

6) **integralności i poufności danych** – forma przetwarzania danych osobowych jest zabezpieczona odpowiednimi środkami technicznymi i organizacyjnymi aby zapewnić adekwatne bezpieczeństwo danych, w tym ochronę przed niedozwolonym lub niezgodnym z prawem przetwarzaniem, jak również przed przypadkową utratą, zniszczeniem lub uszkodzeniem,

7) **rozliczalności** – wykazanie, że Administrator Danych Osobowych postępuje zgodnie z zasadami, dotyczącymi przetwarzania danych osobowych tzn.: wdrożenie odpowiednich i skutecznych środków oraz wykazanie, że te środki spełniają obowiązki nałożone przez RODO,

8) **przejrzystości** – informacje związane z przetwarzaniem danych są dla osoby, której dotyczą łatwo dostępne, zrozumiałe oraz sformułowane jasnym i prostym językiem,

9) **poufność** - dane osobowe powinny być przetwarzane w sposób zapewniający im odpowiednie bezpieczeństwo i odpowiednią poufność, w tym ochronę przed nieuprawnionym dostępem do nich i do sprzętu służącego ich przetwarzaniu oraz przed nieuprawnionym korzystaniem z tych danych i z tego sprzętu.

§ 5. Zabrania się przetwarzania danych osobowych ujawniających pochodzenie rasowe lub etniczne, poglądy polityczne, przekonania religijne lub światopoglądowe, przynależność do związków zawodowych oraz przetwarzania danych genetycznych, danych biometrycznych w celu jednoznacznego zidentyfikowania osoby fizycznej lub danych dotyczących zdrowia, seksualności lub orientacji seksualnej tej osoby. Powyższe nie dotyczy wówczas, gdy został zapewniony jeden z warunków zawartych w art. 9 ust. 2 RODO.

Rozdział IV

ZAKRES DZIAŁANIA JEDNOSTKI

§ 6. W ramach prowadzonej działalności Urząd Gminy Wiskitki jako jednostka organizacyjna realizuje zadania związane z realizacją zadań publicznych określonych przepisami prawa.

§ 7. Polityka ochrony danych osobowych odnosi się do:

1. Stanowisk pracy znajdujących się w strukturze organizacyjnej określonej w Regulaminie Organizacyjnym Urzędu Gminy Wiskitki.
2. Pomieszczeń, w których przetwarzane są informacje (dane osobowe) podlegające ochronie, zlokalizowanych w Urzędzie Gminy Wiskitki, przy ul. Kościuszk. Wykaz pomieszczeń, w których przetwarzane są dane osobowe stanowi ***załącznik Nr 1 do niniejszej Polityki***.
3. Zasobów informacyjnych (aktywów) zaangażowanych w realizację zadań publicznych, a w szczególności:
   1) potencjału ludzkiego, czyli wszystkich pracowników w rozumieniu przepisów Kodeksu Pracy, Karty Nauczyciela, konsultantów, praktykantów, stażystów oraz inne osoby i podmioty mające dostęp do informacji podlegającej ochronie,
   2) dokumentów papierowych i elektronicznych będących własnością Administratora Danych Osobowych lub stron zainteresowanych, o ile zostały przekazane zgodnie z przepisami RODO.
4. Zasobów informatycznych stosowanych do realizacji zadań. Wykaz stosowanych programów i aplikacji stanowi ***Załącznik Nr 2 do niniejszej Polityki.***
5. Technologii służących pozyskiwaniu, selekcjonowaniu, analizowaniu, przetwarzaniu, zarządzaniu i udostępnianiu informacji, do których zalicza się zarówno systemy papierowe, jak i elektroniczne wspomagające realizację zadań jednostki.

Rozdział V

ORGANIZACJA PRZETWARZANIA DANYCH OSOBOWYCH

§ 8. Administrator Danych Osobowych 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 organizacji oraz technik zabezpieczenia danych osobowych,
2) upoważnia poszczególne osoby do przetwarzania danych osobowych w określonym indywidualnie zakresie, odpowiadającym obowiązkom służbowym

na danym stanowisku pracy, wykonującym zadania na podstawie umowy zlecenia lub umowy o dzieło czy w ramach realizacji innych zadań przez np. stażystów, praktykantów czy wolontariuszy oraz cofa upoważnienia lub wyrejestrowuje użytkownika z systemu informatycznego,
3) wyznacza Inspektora Ochrony Danych Osobowych oraz zabezpiecza obsługę informatyczną poprzez zatrudnienie informatyka,
4) prowadzi ewidencję osób upoważnionych do przetwarzania danych osobowych,
5) prowadzi dokumentację z zakresu ochrony danych, w tym Rejestr czynności przetwarzania danych osobowych,
6) zapewnia użytkownikom właściwe stanowiska i warunki pracy, umożliwiające bezpieczne przetwarzanie danych osobowych,
7) podejmuje odpowiednie działania w przypadku naruszenia lub podejrzenia naruszenia ochrony danych osobowych,
8) zapewnia określone zasoby niezbędne do wykonywania zadań przez Inspektora Ochrony Danych.

§ 9. 1. Administrator Danych Osobowych oraz podmiot przetwarzający ma obowiązek właściwego i bezzwłocznego włączania Inspektora we wszystkie sprawy dotyczące ochrony danych osobowych (art. 38 ust. 1 RODO). Administrator Danych Osobowych lub podmiot przetwarzający powinien umożliwić Inspektorowi Ochrony Danych czynny udział we wszystkich sprawach dotyczących procesów przetwarzania danych osobowych oraz na bieżąco przekazywać mu wszystkie informacje związane z wykonywaniem jego zadań. Tym samym wiedza Inspektora ma obejmować informacje o każdej sprawie dotyczącej przetwarzania i ochrony danych osobowych w jednostce.
2. Inspektor Ochrony Danych, w związku z pełnieniem swojej funkcji, realizuje swoje zadania rzetelnie, a także charakteryzuje się wysokim poziomem etyki zawodowej.
3. Inspektor Ochrony Danych w zakresie swoich obowiązków podlega bezpośrednio Administratorowi Danych Osobowych, który wspiera Inspektora w wypełnianiu jego zadań, zapewniając jego udział we wszystkich sprawach związanych z ochroną danych osobowych.
4. Inspektor Ochrony Danych może zajmować stanowiska w sprawach dotyczących wprowadzenia rozwiązań w zakresie bezpieczeństwa danych osobowych

§ 10. **Do zadań Inspektora Ochrony Danych Osobowych należy:**

1) podejmowanie działań na rzecz zgodnego z przepisami prawa przetwarzania danych osobowych,
2) informowanie Administratora Danych Osobowych oraz pracowników, którzy przetwarzają dane osobowe, o obowiązkach spoczywających na nich na mocy rozporządzenia (RODO) oraz innych przepisów Unii lub państw członkowskich o ochronie danych osobowych i doradzanie im w tej sprawie,
3) monitorowanie przestrzegania przepisów krajowych, ogólnego rozporządzenia RODO, innych przepisów Unii lub państw członkowskich o ochronie danych oraz polityk administratora w dziedzinie ochrony danych osobowych,
4) podejmowanie działań zwiększających świadomość pracowników jednostki przetwarzających dane osobowe poprzez organizację szkoleń z zakresu ochrony danych osobowych,

5) prowadzenie okresowych przeglądów stanu zabezpieczenia danych osobowych, dokonywanie sprawdzeń lub audytów i przedstawianie ich wyników Administratorowi Danych Osobowych;
6) wydawanie na żądanie ADO zaleceń co do oceny skutków dla ochrony danych oraz monitorowanie jej wykonania,
7) współpraca z organem nadzorczym,
8) pełnienie funkcji punktu kontaktowego dla organu nadzorczego w kwestiach związanych z przetwarzaniem, w tym z uprzednimi konsultacjami oraz w stosownych przypadkach prowadzenie konsultacji we wszelkich innych sprawach,
9) w przypadku incydentu związanego z naruszeniem ochrony danych osobowych pełnienie roli punktu kontaktowego dla osób, których dane dotyczą, we wszystkich sprawach związanych z przetwarzaniem ich danych osobowych oraz z wykonywaniem praw przysługujących im na mocy ogólnego rozporządzenia RODO.

§ 11. **Informatyk**

Informatyk realizuje zadania w zakresie zarządzania i bieżącego nadzoru nad systemem informatycznym Administratora Danych Osobowych, w szczególności:

1) zarządza systemem informatycznym, w którym przetwarzane są dane osobowe, posługując się hasłem dostępu do wszystkich stacji roboczych z pozycji administratora,
2) przeciwdziała dostępowi osób nieupoważnionych do systemu informatycznego, w którym przetwarzane są dane osobowe,
3) na wniosek Kierownika jednostki przydziela każdemu pracownikowi identyfikator oraz hasło do systemu informatycznego oraz dokonuje modyfikacji uprawnień, a także usuwa konta użytkowników, zgodnie z zasadami określonymi w Instrukcji zarządzania systemem informatycznym służącym do przetwarzania danych osobowych,
4) nadzoruje działania mechanizmów uwierzytelniania użytkowników oraz kontroli dostępu do danych osobowych,
5) podejmuje działania w zakresie ustalenia i kontroli dostępu do danych osobowych,
6) na polecenie Administratora Danych Osobowych wyrejestrowuje użytkowników,
7) w sytuacji stwierdzenia naruszenia zabezpieczeń systemu informatycznego niezwłocznie informuje Inspektora Ochrony Danych o naruszeniu i współdziała z nim przy usuwaniu skutków naruszenia,
8) prowadzi szczegółową dokumentację naruszeń bezpieczeństwa danych osobowych w systemie informatycznym,
9) sprawuje nadzór nad wykonywaniem napraw, konserwacją oraz likwidacją urządzeń komputerowych, na których zapisane są dane osobowe, nad wykonaniem kopii zapasowych, ich przechowywaniem oraz okresowym sprawdzeniem pod kątem ich dalszej przydatności do odtwarzania danych w przypadku awarii systemu informatycznego,
10) 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.
11) współpracuje z Inspektorem Danych Osobowych m. in. przy opracowywaniu i aktualizacji dokumentacji dotyczącej ochrony danych osobowych.

§ 12. **Obowiązki osób upoważnionych do przetwarzania danych osobowych**

Osoba upoważniona do przetwarzania danych osobowych jest zobowiązana przestrzegać następujących zasad:
1) przetwarzania danych osobowych wyłącznie w zakresie ustalonym indywidualnie w upoważnieniu przez Administratora Danych Osobowych i tylko w celu wykonywania nałożonych obowiązków służbowych. Zakres dostępu do danych osobowych przypisany jest do niepowtarzalnego identyfikatora użytkownika, niezbędnego do rozpoczęcia pracy w systemie. Rozwiązanie stosunku pracy, odwołanie z pełnionej funkcji powoduje wygaśnięcie upoważnienia do przetwarzania danych osobowych,
2) zachowania tajemnicy danych osobowych oraz przestrzegania procedur ich bezpiecznego przetwarzania. Przestrzeganie tajemnicy danych osobowych obowiązuje przez cały okres zatrudnienia u Administratora Danych Osobowych, a także po ustaniu stosunku pracy lub odwołaniu z pełnionej funkcji,
3) zna, rozumie i stosuje w możliwie największym zakresie wszelkie dostępne środki ochrony danych osobowych oraz uniemożliwia osobom nieuprawnionym dostępu do swojej stacji roboczej,
4) przetwarza dane osobowe zgodnie z obowiązującymi przepisami prawa oraz przyjętymi regulacjami wewnętrznymi,
5) postępuje zgodnie z ustalonymi regulacjami wewnętrznymi dotyczącymi przetwarzania danych osobowych,
6) zachowuje w tajemnicy dane osobowe, do których uzyskał dostęp oraz informacje o sposobach ich zabezpieczenia,
7) chroni dane osobowe oraz środki użyte do ich przetwarzania przed nieuprawnionym dostępem, ujawnieniem, modyfikacją, zniszczeniem lub zniekształceniem,
8) informuje Administratora Danych Osobowych o wszelkich podejrzeniach naruszenia, zauważonych naruszeniach oraz słabościach systemu przetwarzającego dane osobowe,
9) zapoznała się z Polityką ochrony danych osobowych oraz Instrukcją zarządzania systemem informatycznym służącym do przetwarzania danych osobowych.

Rozdział VI

UPOWAŻNIENIA

§ 13. Każda osoba upoważniona musi przetwarzać dane osobowe wyłącznie na polecenie Administratora Danych Osobowych, chyba że wymaga tego prawo Unii lub prawo państwa członkowskiego.
§ 14. Administrator Danych Osobowych odpowiada za nadawanie i cofanie upoważnień do przetwarzania danych w zbiorach papierowych, systemach informatycznych. Wzór upoważnienia stanowi ***załącznik Nr 3 do niniejszej Polityki***.
§ 15. Upoważnienia mogą być nadawane w formie poleceń np.: upoważnienia do przeprowadzenia kontroli, audytów, wykonania innych czynności służbowych,

udokumentowanego polecenia ADO w postaci umowy powierzenia przetwarzania danych osobowych.
§ 16. Administrator Danych Osobowych lub osoba przez niego upoważniona prowadzi ewidencję osób upoważnionych w celu sprawowania kontroli nad prawidłowym dostępem do danych osób upoważnionych. Ewidencja ma charakter pomocniczy i nie jest wymagana przepisami RODO – wzór Ewidencji stanowi ***załącznik Nr 4 do niniejszej Polityki***.

Rozdział VII

PODMIOT PRZETWARZAJĄCY

§ 17. Jeżeli przetwarzanie ma być dokonywane w imieniu Administratora Danych Osobowych, korzysta on 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.

§ 18. Podmiot przetwarzający nie korzysta z usług innego podmiotu przetwarzającego bez uprzedniej szczegółowej lub ogólnej pisemnej zgody ADO. W przypadku ogólnej pisemnej zgody podmiot przetwarzający informuje ADO o wszelkich zamierzonych zmianach dotyczących dodania lub zastąpienia innych podmiotów przetwarzających, dając tym samym ADO możliwość wyrażenia sprzeciwu wobec takich zmian.

§ 19. Przetwarzanie przez podmiot przetwarzający odbywa się na podstawie umowy lub innego instrumentu prawnego, które podlegają prawu Unii lub prawu państwa członkowskiego i wiążą podmiot przetwarzający i administratora, określają przedmiot i czas trwania przetwarzania, charakter i cel przetwarzania, rodzaj danych osobowych oraz kategorie osób, których dane dotyczą, obowiązki i prawa administratora.

§ 20. 1. Podmiot przetwarzający zapewnia, by osoby upoważnione do przetwarzania danych osobowych zobowiązały się do zachowania tajemnicy lub by podlegały odpowiedniemu ustawowemu obowiązkowi zachowania tajemnicy.

2. Umowa powierzenia jest sporządzana na piśmie. Wykaz umów powierzenia danych osobowych prowadzony przez ADO stanowi ***załącznik Nr 5 do niniejszej Polityki***.

Rozdział VIII

REJESTR CZYNNOŚCI PRZETWARZANIA DANYCH OSOBOWYCH

§ 21. 1. Zgodnie z art. 30 RODO Administrator Danych Osobowych prowadzi rejestr czynności przetwarzana danych osobowych, w formie pisemnej, w tym elektronicznej.

2. Celem rejestru czynności przetwarzania danych osobowych jest możliwość pełnienia nadzoru i monitorowania procesów przetwarzania danych osobowych.

3. Rejestr czynności przetwarzania danych osobowych jest jednym z podstawowych narzędzi umożliwiających ADO rozliczanie większości obowiązków ochrony danych.

4. W rejestrze dla każdej czynności przetwarzania danych, którą Administrator Danych Osobowych uznał za odrębną dla potrzeb rejestru, jednostka odnotowuje co najmniej:
1) nazwę czynności lub procesu,
2) cel przetwarzania,
3) kategorie osób, których dane dotyczą,
4) opis kategorii danych,
5) podstawę prawną przetwarzania danych,
6) ogólny opis technicznych i organizacyjnych środków ochrony danych

§ 22. 1. Administrator Danych Osobowych ma obowiązek udostępnić rejestr na każde żądanie organu nadzorczego. Organ nadzorczy dokonuje kontroli tych rejestrów w celu monitorowania operacji przetwarzania.

2. Wzór rejestru czynności przetwarzania danych osobowych w jednostce stanowi ***załącznik Nr 6 do niniejszej Polityki***. Wzór rejestru zawiera także kolumny nieobowiązkowe, które ułatwiają zarządzanie zgodnością danych osobowych i rozliczanie się z niej.

Rozdział IX

OBOWIĄZEK INFORMACYJNY

§ 23. 1. Administrator Danych Osobowych dba, aby informacje dla osób, których dane przetwarza były sporządzone w formie zwięzłej, przejrzystej, zrozumiałej i łatwo dostępnej. Klauzulę informacyjną można opatrzyć standardowymi znakami graficznym, które w sposób widoczny, zrozumiały i czytelny przedstawią sens zamierzonego przetwarzania.

2. Obowiązek informacyjny realizowany jest w formie pisemnej lub inny sposób, w tym w stosownych przypadkach – elektronicznie, a także poprzez zamieszczenie na stronie internetowej, stronie BIP, umieszczenia na tablicach informacyjnych, przekazywanie informacji w trakcie spotkań z pracownikami. Spełnienie obowiązku informacyjnego w stosunku do osób jest wolne od opłat.

3. Administrator Danych Osobowych realizuje obowiązek informacyjny w sposób rzetelny i przejrzysty oraz zapewnia, że osoba, której dane dotyczą zostanie poinformowana o celach prowadzenia operacji przetwarzania. W przypadku profilowania ADO jest obowiązany do poinformowania osoby o tym fakcie oraz o konsekwencjach takiego profilowania. W przypadku zbierania danych od osoby, której dane dotyczą, należy wskazać, czy ma ona obowiązek je podać oraz o konsekwencjach ich niepodania.

4. Wobec osób, których dane osobowe przetwarza Administrator Danych Osobowych wykonano tzw. obowiązek informacyjny (art. 12, 13 i 14 RODO) wraz ze wskazaniem im praw (prawa dostępu do danych, przenoszenia, sprostowania, usunięcia, ograniczenia przetwarzania, sprzeciwu).

§ 24. W przypadku zbierania danych osobowych, od osoby której dane dotyczą, zgodnie z art. 13 ust. 1 i 2 RODO informujemy ją o:

1) swojej tożsamości i danych kontaktowych oraz tożsamość i danych kontaktowych swojego przedstawiciela,
2) danych kontaktowych inspektora ochrony danych,
3) celach przetwarzania, do których mają posłużyć dane osobowe,
4) podstawie prawnej przetwarzania,
5) prawnie uzasadnionym interesie realizowanym przez administratora lub przez stronę trzecią – jeżeli przetwarzanie odbywa się na podstawie prawnie usprawiedliwionego interesu administratora,
6) odbiorcach danych osobowych lub o kategoriach odbiorców, jeżeli istnieją,
7) transferze danych do państwa trzeciego, w tym o:
   a) przekazania danych osobowych do państwa trzeciego lub organizacji międzynarodowej,
   b) stwierdzeniu lub braku stwierdzenia przez Komisję odpowiedniego stopnia ochrony,
   c) lub wzmiankę o odpowiednich lub właściwych zabezpieczeniach oraz o możliwościach uzyskania kopii danych lub o miejscu udostępnienia danych w przypadku przekazania danych do państwa trzeciego,
8) okres, przez który dane osobowe będą przechowywane, a gdy nie jest to możliwe, kryteria ustalania tego okresu,
9) prawie do:
   a) żądania od administratora dostępu do danych osobowych dotyczących osoby, której dane dotyczą,
   b) ich sprostowania, usunięcia lub ograniczenia przetwarzania lub
   c) wniesienia sprzeciwu wobec przetwarzania, a także
   d) przenoszenia danych;
   e) prawie do cofnięcia zgody w dowolnym momencie bez wpływu na zgodność z prawem przetwarzania, którego dokonano na podstawie zgody przed jej cofnięciem jeżeli przetwarzanie odbywa się na podstawie zgody na przetwarzanie danych zwykłych lub szczególnej kategorii,
10) prawie wniesienia skargi do organu nadzorczego,
11) informacji, czy podanie danych osobowych jest wymogiem ustawowym, umownym lub warunkiem zawarcia umowy oraz czy osoba, której dane dotyczą jest zobowiązana do ich podania i jakie są ewentualne konsekwencje niepodania danych,
12) informacji o zautomatyzowanym podejmowaniu decyzji, w tym o profilowaniu oraz – przynajmniej w tych przypadkach – istotne informacje o zasadach ich podejmowania, a także o znaczeniu i przewidywanych konsekwencjach takiego przetwarzania dla osoby, której dane dotyczą.

§ 25. W przypadku zbierania danych osobowych z innego źródła niż dane osoby której dane dotyczą, zgodnie z art. 14 ust. 1 i 2 RODO informujemy ją o:
1) informacjach wymienionych w § 24,
2) kategoriach odnośnych danych osobowych,
3) źródle pochodzenia danych osobowych, a jeżeli ma to zastosowanie, o pochodzeniu ich ze źródeł powszechnie dostępnych.

Rozdział X

PRAWA OSÓB

§ 26. 1. Osoba, której dane dotyczą, jest uprawniona do uzyskania od Administratora Danych Osobowych informacji na temat przetwarzania jej danych osobowych, w szczególności:
1) celu przetwarzania,
2) kategorii danych osobowych,
3) informacje o odbiorcach lub kategoriach odbiorców, którym dane osobowe zostały lub zostaną ujawnione, w szczególności o odbiorcach w państwach trzecich lub organizacjach międzynarodowych,
4) w miarę możliwości planowany okres przechowywania danych osobowych, a gdy nie jest to możliwe, kryteria ustalania tego okresu,
5) informacje o prawie do żądania od administratora sprostowania, usunięcia lub ograniczenia przetwarzania danych osobowych dotyczącego osoby, której dane dotyczą, oraz do wniesienia sprzeciwu wobec takiego przetwarzania,
6) informacje o prawie wniesienia skargi do organu nadzorczego,
7) jeżeli dane osobowe nie zostały zebrane od osoby, której dane dotyczą – wszelkie dostępne informacje o ich źródle,
8) informacje o zautomatyzowanym podejmowaniu decyzji, w tym o profilowaniu oraz – przynajmniej w tych przypadkach – istotne informacje o zasadach ich podejmowania, a także o znaczeniu i przewidywanych konsekwencjach takiego przetwarzania dla osoby, której dane dotyczą,
9) jeżeli dane osobowe są przekazywane do państwa trzeciego lub organizacji międzynarodowej, osoba, której dane dotyczą, ma prawo zostać poinformowana o odpowiednich zabezpieczeniach związanych z przekazaniem.

2. Administrator Danych Osobowych ma obowiązek ułatwiania osobie, której dane dotyczą, wykonanie przysługujących jej praw:

1) **Prawo dostępu do swoich danych** – na żądanie osoby dotyczące dostępu do jej danych Administrator Danych Osobowych informuje osobę, czy przetwarza jej dane oraz informuje o szczegółach przetwarzania, zgodnie z art. 15 RODO (zakres odpowiada obowiązkowi informacyjnemu przy zbieraniu danych), a także udziela osobie dostępu do danych jej dotyczących. Dostęp do danych może być zrealizowany poprzez wydanie kopii danych.
2) **Prawo do sprostowania** – Administrator Danych Osobowych dokonuje sprostowania nieprawidłowych danych na żądanie osoby. ADO ma prawo odmówić sprostowania danych, chyba, że osoba w rozsądny sposób wykaże nieprawidłowości danych, których sprostowania się domaga. W przypadku sprostowania danych ADO informuje osobę o odbiorcach danych, na żądanie tej osoby.
3) **Prawo do usunięcia** – na żądanie osoby Administrator Danych Osobowych usuwa dane, gdy:
a) dane nie są niezbędne do celów, w których zostały zebrane, ani przetwarzane w innych zgodnych z prawem celach,
b) zgoda na ich przetwarzanie została cofnięta, a nie ma innej podstawy prawnej przetwarzania,
c) osoba wniosła skuteczny sprzeciw względem przetwarzania tych danych,
d) dane były przetwarzane niezgodnie z prawem,
e) konieczność usunięcia wynika z obowiązku prawnego,

f) żądanie dotyczy danych dziecka zebranych na podstawie zgody w celu świadczenia usług społeczeństwa informacyjnego oferowanych bezpośrednio dziecku np.: udział w konkursie na stronie internetowej.

4) **Prawo do ograniczenia** – Administrator Danych Osobowych dokonuje ograniczenia przetwarzania danych na żądanie osoby, gdy:

a) osoba kwestionuje prawidłowość danych – na okres pozwalający sprawdzić ich prawidłowość,

b) przetwarzanie jest niezgodne z prawem, a osoba której dane dotyczą sprzeciwia się ich usunięcia, żądając w zamian ograniczenia ich wykorzystywania,

c) nie potrzebuje danych osobowych, ale są one potrzebne osobie, której dane dotyczą do ustalenia, dochodzenia lub obrony roszczeń,

d) osoba wniosła sprzeciw względem przetwarzania z przyczyn związanych z jej szczególną sytuacją – do czasu stwierdzenia, czy po stronie Administratora Danych Osobowych zachodzą prawnie uzasadnione podstawy nadrzędne wobec podstaw sprzeciwu.

W trakcie ograniczenia przetwarzania Administrator Danych Osobowych przechowuje dane, natomiast nie przetwarza ich (nie wykorzystuje, nie przekazuje), bez zgody osoby, której dane dotyczą, chyba, że w celu ustalenia, dochodzenia lub obrony roszczeń, lub w celu ochrony praw innej osoby fizycznej lub prawnej, lub z uwagi na ważne względy interesu publicznego. ADO informuje osobę przed uchyleniem ograniczenia przetwarzania.

5) **Prawo do przenoszenia** – na żądanie osoby Administrator Danych Osobowych wydaje w ustrukturyzowanym, powszechnie używanym formacie nadającym się do odczytu maszynowego lub przekazuje innemu podmiotowi, jeśli jest to możliwe, dane dotyczące tej osoby, które dostarczyła ona Administratorowi Danych Osobowych, przetwarzane na podstawie zgody tej osoby lub w celu zawarcia lub wykonania umowy z nią zawartej w systemach informatycznych administratora.

6) **Prawo do sprzeciwu** – osoba, której dane dotyczą, ma prawo w dowolnym momencie wnieść sprzeciw – z przyczyn związanych z jej szczególną sytuacją – wobec przetwarzania dotyczących jej danych opartego na art. 6 ust. 1 lit. e) lub f), w tym profilowania na podstawie tych przepisów.

7) **Prawo do informacji o profilowaniu**.

§ 27. 1. Administrator Danych Osobowych dba o minimalizację przetwarzania danych pod kątem:

1) adekwatności danych do celów (ilości danych i zakresu przetwarzania),

2) dostępu do danych,

3) czasu przechowywania danych.

2. **Minimalizacja zakresu** – ADO dokonuje okresowego przeglądu ilości przetwarzanych danych i zakresu ich przetwarzania nie rzadziej niż raz na rok. ADO przeprowadza weryfikację zmian co do ilości i zakresu przetwarzania danych w ramach procedur zarządzania zmianą.

3. **Minimalizacja dostępu** – ADO stosuje ograniczenia dostępu do danych osobowych: prawne (zobowiązania do poufności, zakresy upoważnień), fizyczne (strefy dostępu, zamykanie pomieszczeń) i logiczne (ograniczenia uprawnień do systemów przetwarzających dane osobowe i zasobów sieciowych, w których rezydują dane osobowe). Stosuje kontrolę dostępu fizycznego oraz dokonuje aktualizacji uprawnień dostępowych przy zmianach w składzie personelu i zmianach

ról osób oraz zmianach podmiotów przetwarzających. ADO dokonuje okresowego przeglądu ustanowionych użytkowników systemów i aktualizuje ich nie rzadziej niż raz na rok.
4. **Minimalizacja czasu** – ADO wdraża mechanizmy kontroli cyklu życia danych osobowych, w tym weryfikacji dalszej przydatności danych względem terminów i punktów kontrolnych wskazanych w Rejestrze czynności przetwarzania danych osobowych. Dane, których zakres przydatności ulega ograniczeniu wraz z upływem czasu są usuwane z systemów informatycznych, jak też z akt podręcznych i głównych. Dane takie mogą być archiwizowane oraz znajdować się na kopiach zapasowych systemów i informacji przetwarzanych przez ADO. Procedury archiwizacji i korzystania z archiwów, tworzenia i wykorzystania kopii zapasowych uwzględniają wymagania kontroli nad cyklem życia danych, w tym wymogi usuwania danych.

§ 28. 1. Administrator Danych Osobowych udziela osobie, której dane dotyczą, informacji o działaniach podjętych w związku z jej żądaniem na podstawie art. 15 – 22 RODO w terminach:
1) **bez zbędnej zwłoki** – a w każdym razie w terminie miesiąca od otrzymania żądania,
2) **trzy miesiące** – w razie konieczności ww. termin jednego miesiąca można przedłużyć o kolejne dwa miesiące z uwagi na skomplikowany charakter żądania lub liczbę żądań, jednakże w terminie miesiąca od otrzymania żądania ADO informuje osobę, której dane dotyczą o takim przedłużeniu terminu, z podaniem przyczyn opóźnienia,
2. Jeśli osoba, której dane dotyczą, przekazała swoje żądanie elektronicznie, w miarę możliwości informacje także są przekazywane elektronicznie, chyba że osoba, której dane dotyczą, zażąda innej formy.

3. Jeżeli Administrator Danych Osobowych nie podejmuje działań w związku z żądaniem osoby, której dane dotyczą, to niezwłocznie – najpóźniej w terminie miesiąca od otrzymania żądania – informuje osobę, której dane dotyczą, o:
1) powodach niepodjęcia działań oraz
2) możliwości wniesienia skargi do organu nadzorczego oraz skorzystania ze środków ochrony prawnej przed sądem.

4. Prawo do kontroli jest wolne od opłat jednakże, jeżeli żądania osoby, której dane dotyczą, są ewidentnie nieuzasadnione lub nadmierne, w szczególności ze względu na swój ustawiczny charakter, administrator może:
1) pobrać rozsądną opłatę, uwzględniając administracyjne koszty udzielenia informacji, prowadzenia komunikacji lub podjęcia żądanych działań albo
2) odmówić podjęcia działań w związku z żądaniem.

5. Obowiązek wykazania, że żądanie ma ewidentnie nieuzasadniony lub nadmierny charakter, spoczywa na administratorze.

§ 29. 1. Jeżeli Administrator Danych Osobowych ma uzasadnione wątpliwości co do tożsamości osoby fizycznej składającej żądanie, może zażądać dodatkowych informacji niezbędnych do potwierdzenia tożsamości osoby, której dane dotyczą.

2. Administrator Danych Osobowych powinien skorzystać z wszelkich rozsądnych środków w celu zweryfikowania tożsamości żądającej dostępu osoby, której dane dotyczą, w szczególności w kontekście usług internetowych i identyfikatorów internetowych. Administrator Danych Osobowych nie powinien zatrzymywać danych osobowych wyłącznie w celu reagowania na ewentualne żądania.

3. Jeżeli Administrator Danych Osobowych przetwarza duże ilości informacji o osobie, której dane dotyczą, może zażądać przed podaniem informacji, by osoba, której dane dotyczą, sprecyzowała informacje lub czynności przetwarzania, których dotyczy jej żądanie.

Rozdział XI

BEZPIECZEŃSTWO DANYCH OSOBOWYCH

§ 30. 1. Administrator Danych Osobowych zapewnia stopień bezpieczeństwa odpowiadający ryzyku naruszenia praw i wolności osób fizycznych wskutek przetwarzania danych osobowych przez pracowników Urzędu Gminy Wiskitki.

2. Administrator Danych Osobowych w celu zapewnienia bezpieczeństwa informacji oraz ochrony danych osób, których dane dotyczą wspiera się:
1) Inspektorem Ochrony Danych
2) Informatykiem

3. Za bezpieczeństwo danych osobowych w Urzędzie odpowiedzialny jest każdy pracownik w związku z zajmowanym przez niego stanowiskiem pracy.

§ 31. Administrator Danych Osobowych przeprowadza i dokumentuje analizy adekwatności środków bezpieczeństwa danych osobowych. W tym celu:

1) zapewnia odpowiedni stan wiedzy o bezpieczeństwie informacji, cyberbezpieczeństwie i ciągłości działania – wewnętrznie lub ze wsparciem podmiotów wyspecjalizowanych;
2) kategoryzuje dane oraz czynności przetwarzania pod kątem ryzyka, które przedstawiają;
3) przeprowadza analizę ryzyka naruszenia praw lub wolności osób fizycznych dla czynności przetwarzania danych lub ich kategorii. Analizuje możliwe sytuacje i scenariusze naruszenia ochrony danych osobowych uwzględniając charakter, zakres, kontekst i cele przetwarzania, ryzyko naruszenia praw lub wolności osób fizycznych o różnym prawdopodobieństwie wystąpienia i wadze zagrożenia;
4) ustala możliwe do zastosowania organizacyjne i techniczne środki bezpieczeństwa i ocenia koszt ich wdrażania, w tym ustala przydatność i stosuje takie środki i podejście jak np.:
a) pseudonimizacja,
b) szyfrowanie danych osobowych,
c) inne środki cyberbezpieczeństwa składające się na zdolność do ciągłego zapewnienia poufności, integralności, dostępności, odporności systemów i usług przetwarzania,

d) środki zapewnienia ciągłości działania i zapobiegania skutkom katastrof, czyli zdolności do szybkiego przywrócenia dostępności danych osobowych i dostępu do nich w razie incydentu fizycznego lub technicznego.

§ 32. Administrator Danych Osobowych stosuje adekwatne środki bezpieczeństwa ustalone w ramach przeprowadzonej analizy ryzyka i oceny skutków dla ochrony danych. Środki bezpieczeństwa danych osobowych stanowią element środków bezpieczeństwa informacji i są określone w § 36.

§ 33. 1. Administrator Danych Osobowych ma obowiązek dokumentowania wszelkich naruszeń ochrony danych osobowych.

2. Zasady zgłaszania naruszenia ochrony danych organowi nadzorczemu określone są w artykule 33 RODO.

3. Administrator Danych Osobowych ma obowiązek zgłoszenia organowi nadzorczemu przypadek naruszenia ochrony danych osobowych w ciągu 72 godzin. Jeżeli zgłoszenie przekazane zostanie po tym terminie należy wówczas dołączyć wyjaśnienie przyczyn opóźnienia.

4. Zwolnienie z obowiązku zgłoszenia naruszenia, organowi nadzorczemu możliwe jest, jeżeli jest mało prawdopodobne, by naruszenie skutkowało ryzykiem naruszenia praw lub wolności osób fizycznych.

5. Jeżeli naruszenie dotyczy podmiotu przetwarzającego, to podmiot przetwarzający bez zbędnej zwłoki zgłasza je Administratorowi Danych Osobowych.

6. Jeżeli informacji nie możemy udzielić w tym samym czasie możemy je przekazywać organowi nadzorczemu sukcesywnie bez zbędnej zwłoki.

7. Administrator Danych Osobowych 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 na zweryfikowanie przestrzegania artykułu 33 RODO.

8. Procedura postępowania w przypadku naruszenia ochrony danych osobowych wprowadzona u Administratora Danych Osobowych stanowi odrębny dokument.

Zawiadamianie osoby, której dane dotyczą o naruszeniu ochrony danych osobowych

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

2. Zawiadomienie, jasnym i prostym językiem powinno opisywać charakter naruszenia ochrony danych osobowych oraz zawierać przynajmniej niżej wymienione informacje:

1) imię i nazwisko oraz dane kontaktowe Inspektora Ochrony Danych lub oznaczenie innego punktu kontaktowego, od którego można uzyskać więcej informacji,
2) opis możliwych konsekwencji naruszenia ochrony danych osobowych,
3) opis środków zastosowanych lub proponowanych przez ADO w celu zaradzenia naruszeniu ochrony danych osobowych, w tym w stosownych przypadkach środki w celu zminimalizowania jego ewentualnych negatywnych skutków.

§ 35. 1. Zawiadomienie nie jest wymagane w następujących przypadkach:

1) Administrator Danych Osobowych wdrożył odpowiednie techniczne i organizacyjne środki ochrony i środki te zostały zastosowane do danych osobowych, których dotyczy naruszenie, w szczególności takie jak: szyfrowanie, uniemożliwiające odczyt osobom nieuprawnionym do dostępu do tych danych osobowych.
2) Administrator Danych Osobowych zastosował środki eliminujące prawdopodobieństwo wysokiego ryzyka naruszenia praw lub wolności osoby, której dane dotyczą, o którym mowa w pkt 1.
3) 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.

2. Jeżeli Administrator Danych Osobowych nie zawiadomił jeszcze osoby, której dane dotyczą, o naruszeniu ochrony danych osobowych, organ nadzorczy – biorąc pod uwagę prawdopodobieństwo, że to naruszenie ochrony danych osobowych spowoduje wysokie ryzyko – może od niego tego zażądać lub może stwierdzić, że spełniony został jeden z warunków, wymienionych wyżej.

Środki organizacyjne zabezpieczające przed naruszeniem ochrony danych osobowych

§ 36. 1. Dla zapewnienia ochrony danych osobowych i bezpieczeństwa informacji zastosowano następujące środki organizacyjne:

1) dostęp do danych osobowych mają tylko pracownicy posiadający pisemne, imienne upoważnienia nadane przez Administratora Danych Osobowych,
2) każdy z pracowników zobowiązał się zachować szczególną ostrożność przy przetwarzaniu danych osobowych,
3) dane osobowe chronione są przed dostępem osób nieupoważnionych,
4) pomieszczenia, w których są przetwarzane dane osobowe są zamykane na klucz,
5) dostęp do kluczy posiadają tylko upoważnieni pracownicy,
6) dostęp do pomieszczeń możliwy jest tylko i wyłącznie w godzinach pracy. W przypadku gdy dostęp jest wymagany poza godzinami pracy – możliwy jest tylko za pozwoleniem Administratora Danych Osobowych,
7) dostęp do pomieszczeń, w których są przetwarzane dane osobowe mogą mieć tylko upoważnieni pracownicy,
8) w przypadku pomieszczeń, do których dostęp mają również osoby nieupoważnione, mogą one w nich przebywać tylko w obecności osób upoważnionych i tylko w czasie wymaganym na wykonanie niezbędnych czynności,
9) szafy, w których przechowywane są dane powinny być zamykane na klucz,
10) klucze do szaf posiadają tylko upoważnieni pracownicy,

11) szafy z danymi mogą być otwarte tylko na czas potrzebny na dostęp do danych a następnie powinny być zamykane,
12) pracownicy zobowiązani są stosować zasadę czystego biurka - wszystkie dokumenty i materiały powinny być po zakończeniu pracy chowane w przeznaczonych do tego szafkach, szufladach itp. W przypadku braku dostatecznej ilości dostępnego miejsca dokumenty i materiały powinny być pozostawiane na biurku uporządkowane.

2. Dla zapewnienia ochrony danych osobowych i bezpieczeństwa informacji zastosowano następujące środki techniczne:
1) dostęp do komputerów, na których są przetwarzane dane mają tylko upoważnieni pracownicy,
2) monitory komputerów, na których przetwarzane są dane są tak ustawione aby osoby nieupoważnione nie miały wglądu w dane,
3) po zakończeniu pracy komputery przenośne zawierające dane osobowe powinny być zabezpieczone w zamykanych na klucz szafach,
4) w razie potrzeby wyniesienia komputera przenośnego zawierającego dane osobowe, lub inne informacje chronione, komputer taki musi być odpowiednio dodatkowo zabezpieczony, a dane zaszyfrowane. Pracownik, któremu powierzono komputer przenośny musi zapoznać się z zasadami postępowania z komputerami przenośnymi, których stosowanie potwierdza podpisem. Regulamin postępowania z komputerami przenośnymi stanowi odrębny dokument.
5) nie należy udostępniać komputerów osobom nieupoważnionym,
6) w przypadku potrzeby przeniesienia danych osobowych pomiędzy komputerami należy dokonać tego z zachowaniem szczególnej ostrożności, a nośniki użyte do tego należy wyczyścić (skasować nieodwracalnie), aby nie zostały na nich dane osobowe.
W wypadku niemożliwości skasowania danych z nośnika (płyta CD-ROM) należy taką płytę zniszczyć fizycznie.
7) w przypadku wykorzystania do przenoszenia dysków, dane należy kasować z tych dysków,
8) niezabezpieczonych danych osobowych nie należy przesyłać drogą elektroniczną,
9) sieć komputerowa powinna być zabezpieczona przed wszelkim dostępem z zewnątrz,
10) błędne i nieaktualne wydruki oraz wydruki papierowe zawierające dane osobowe lub inne informacje chronione niszczone są za pomocą niszczarki lub w inny mechaniczny sposób uniemożliwiający powtórne ich odtworzenie.

3. W jednostce prowadzony i aktualizowany jest wykaz komputerów, którego wzór stanowi ***załącznik nr 7 do niniejszej Polityki***.

4. W jednostce prowadzona i aktualizowana jest ewidencja urządzeń przenośnych. Wzór ewidencji stanowi ***załącznik Nr 8 do niniejszej Polityki***.

Rozdział XII

ZARZĄDZANIE RYZYKIEM

§ 37. 1. Celem zarządzania ryzykiem jest wdrożenie odpowiednich środków technicznych i organizacyjnych w taki sposób, aby przetwarzanie danych odbywało się zgodnie z ogólnym rozporządzeniem o ochronie danych (RODO).

2. Zarządzanie ryzykiem powinno prowadzić do eliminacji lub ograniczenia – do akceptowanego poziomu – prawdopodobieństwa i następstw wystąpienia zdarzeń negatywnych. Zarządzanie ryzykiem w kontekście ochrony danych osobowych jest procesem ciągłym.

3. Proces analizy ryzyka i zagrożeń ma charakter subiektywnej oceny dokonywanej przez osoby uprawnione do analizy ryzyka.
4. Dla poszczególnych rodzajów zidentyfikowanego i oszacowanego ryzyka wskazuje się rozwiązania (w tym obowiązujące przepisy prawa oraz przyjęte w organizacji procedury, instrukcje i faktycznie podejmowane działania), które mają na celu ograniczenie prawdopodobieństwa lub następstw wystąpienia ryzyka.

5. Przeprowadzona w jednostce analiza ryzyka stanowi odrębny dokument.

Rozdział XIII

OCENA SKUTKÓW DLA OCHRONY DANYCH OSOBOWYCH

§ 38. 1. Administrator Danych Osobowych dokonuje oceny skutków planowanych operacji przetwarzania dla ochrony danych osobowych tam, gdzie zgodnie z analizą ryzyka ryzyko naruszenia praw i wolności osób jest wysokie.

2. Ocena skutków dla ochrony danych to nowy mechanizm wprowadzony przepisami unijnego rozporządzenia o ochronie danych. Obowiązek jej przeprowadzenia nie ma charakteru powszechnego, gdyż zgodnie z art. 35 ust. 1 RODO, dotyczy administratorów, u których przetwarzanie danych może powodować wysokie ryzyko naruszenia praw lub wolności osób fizycznych. Ocena skutków powinna odnosić się do planowanych operacji przetwarzania dla ochrony danych osobowych.

3. Prawodawca unijny wskazał przykładowe przypadki, w których należy przeprowadzić ocenę skutków dla ochrony danych, nałożył na organy nadzorcze obowiązek określenia i podania do publicznej wiadomości wykazu rodzajów operacji, w odniesieniu do których przeprowadzenie oceny jest obligatoryjne, jak również przewidział możliwość wskazania wykazu operacji niepodlegających wymogowi dokonania oceny skutków dla ochrony danych. Ponadto prawodawca unijny określił w art. 35 ust. 7 RODO minimalne wymogi co do zawartości oceny skutków dla ochrony danych.

4. Obowiązek przeprowadzenia oceny został wyłączony w przypadku, gdy przetwarzanie jest niezbędne do wypełnienia obowiązku prawnego ciążącego na administratorze lub do wykonania zadania realizowanego w interesie publicznym

lub w ramach sprawowania władzy publicznej powierzonej administratorowi, a oceny skutków dokonano na etapie prac legislacyjnych.

Rozdział XIV

POSTANOWIENIA KOŃCOWE

§ 39. Każdy pracownik Administratora Danych Osobowych podpisuje Oświadczenie o zapoznaniu się z treścią niniejszej Polityki oraz zobowiązuje się do przestrzegania zawartych w niej zasad. **Wzór Oświadczenia stanowi *załącznik Nr 9 do niniejszej Polityki.***

Łukasz Choiński
wyznaczony do pełnienia funkcji
Wójta Gminy Wiskitki

Załącznik Nr 1 do Polityki

Wzór wykazu budynków, pomieszczeń lub części pomieszczeń tworzących obszar, w którym są przetwarzane dane osobowe

w.....

Administrator Danych Osobowych określa poniżej obszary przetwarzania danych osobowych w ....., które obejmują następujące lokalizacje i pomieszczenia:

Lp.	Lokalizacja	Adres	Pomieszczenia

Pomieszczenia, w których ma miejsce przetwarzanie danych osobowych, są zamykane na czas nieobecności w nich osób uprawnionych, w sposób uniemożliwiający dostęp osób trzecich.

Załącznik Nr 2 do Polityki

Wykaz stosowanych programów i aplikacji

w.....

Lp.	Nazwa programu lub aplikacji	Data zakupu	Opis	Miejsce instalacji (nr pokoju, piętro)	Imię i nazwisko użytkownika

Załącznik Nr 3 do Polityki

....., dnia ..... r.

UPOWAŻNIENIE

do przetwarzania danych osobowych

Na podstawie art. 29 w związku z art. 5 i art. 6 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 osobowych)

UPOWAŻNIAM

.....
(imię i nazwisko pracownika)

zatrudnionego w .....ma stanowisku.....
(nazwa stanowiska służbowego)

do przetwarzania w imieniu Administratora Danych Osobowych – danych osobowych.....
(podać kategorie osób, których dane dotyczą)

w ramach wykonywania obowiązków służbowych związanych z realizacją zadań.....

Upoważnienie dotyczy następujących operacji przetwarzania danych osobowych: wgląd, zbieranie, przeglądanie, rejestrowanie, przechowywanie, opracowywanie, zmienianie, wyszukiwanie, wykorzystanie, ujawnienie poprzez transmisję, rozpowszechnianie, udostępnianie i usunięcie.

Upoważnienie jest ważne do czasu ustaniu stosunku pracy lub cofnięcia upoważnienia przez Administratora Danych Osobowych.

.....
(podpis ADO)

Zobowiązanie osoby upoważnionej

Zobowiązuję się do zachowania szczególnej staranności i ostrożności w zakresie określonym w niniejszym upoważnieniu.

Przyjęłam do wiadomości i stosowania

.....
(data i czytelny podpis)

Załącznik Nr 4 do Polityki

EWIDENCJA OSÓB UPOWAŻNIONYCH DO PRZETWARZANIA DANYCH OSOBOWYCH

W .....

Lp.	Imię i nazwisko	Data nadania upoważnienia	Data ustania upoważnienia	Zakres upoważnienia		Login/Identyfikator w systemie informatycznym	Uwagi
				Zakres kategorii danych osobowych	Zakres dopuszczalnych operacji		
1.							
2.							
3.							
4.							

EWIDENCJA OSÓB UPOWAŻNIONYCH DO PRZETWARZANIA DANYCH OSOBOWYCH – UMOWY ZLECENIA I INNE

W .....

Lp.	Imię i nazwisko	Data nadania upoważnienia	Data ustania upoważnienia	Zakres upoważnienia		Login/Identyfikator w systemie informatycznym	Uwagi
				Zakres kategorii danych osobowych	Zakres dopuszczalnych operacji		
1.							
2.							
3.							
4.							

Załącznik Nr 5 do Polityki

Wykaz umów powierzenia przetwarzania danych osobowych w .....

Lp.	Numer umowy	Data zawarcia umowy	Czas zakończenia obowiązywania umowy	Nazwa procesora (podmiotu przetwarzającego)	Kategorie przetwarzanych przez procesora danych osobowych
1.					
2.					
3.					
4.					
5.					

Załącznik Nr 6 do Polityki

Rejestr czynności przetwarzania danych osobowych prowadzony w	
Dane Administratora Danych Osobowych (imię, nazwisko/ nazwa, dane kontaktowe): (art. 30 ust. 1 lit. a)	
Dane inspektora ochrony danych lub osoby odpowiedzialnej za ochronę danych osobowych u administratora, jeżeli została wyznaczona (imię, nazwisko, dane kontaktowe):	
Osoba odpowiedzialna za aktualizację rejestru:	
Data wpisu / modyfikacja wpisu	
Data wykreślenia z rejestru	

Nazwa procesu (czynność przetwarzania):		**Numer wpisu:**
Cel przetwarzania danych (art. 30 ust.1 lit. b)		
Charakter przetwarzania danych		
Podstawa przetwarzania		
Kategorie osób, których dane dotyczą (art. 30 ust.1 lit. c)		
Zakres przetwarzanych danych według kategorii danych (art. 30 ust.1 lit. c)	Dane osobowe zwykłe	
	Dane osobowe sensytywne (wrażliwe)	
Kontekst przetwarzanych danych		
Kategorie odbiorców / Odbiorcy danych (art. 30 ust. 1 lit. d)		
Transfery danych (art. 30 ust.1 lit. e)		
Termin usunięcia danych (retencja danych) (art. 30 ust.1 lit. f)		
Opis środków technicznych i organizacyjnych (art. 30 ust.1 lit. g)		
Informacje dodatkowe np. proces uprzednich konsultacji, zastosowanie kodeksu dobrych praktyk, certyfikacja		
Miejsce przechowywania danych osobowych (budynek, piętro, nr pokoju)		
Nazwa i dane kontaktowe podmiotu przetwarzającego (art. 30 ust.1 lit. d)		
Dane współadministratora (jeśli dotyczy) (art. 30 ust.1 lit. a)		
Czy wymagane jest przeprowadzenie oceny skutków dla ochrony danych osobowych (DPIA)?		

Załącznik Nr 7 do Polityki

WYKAZ KOMPUTERÓW

w.....

Lp.	Nr seryjny/ ewidencyjny	Klasyfikacja (laptop/stacj.)	Data zakupu	System operacyjny	Zastosow. zabezp.	Czy na stacji rob. przetw. są dane osob.	Zainstal. oprogr. użytkowe	Użytkownik	Uwagi (elementy zestawu)

Załącznik Nr 8 do Polityki

EWIDENCJA URZĄDZEŃ PRZENOŚNYCH

w.....

Lp.	Oznaczenie nośnika	Data wpisu do ewidencji	Opis nośnika (no. pendrive)	Miejsce przechowywania nośnika	Podpis użytkownika

Załącznik Nr 9 do Polityki

.....
(imię i nazwisko pracownika)

.....
(stanowisko)

OŚWIADCZENIE

Oświadczam, że zapoznałem/zapoznałam się z treścią Polityki ochrony danych osobowych i Instrukcją zarządzania systemem służącym do przetwarzania danych osobowych – dokumentami obowiązującymi w Urzędzie Gminy Wiskitki.

Jednocześnie oświadczam, że zobowiązuję się przestrzegać zasad określonych w niniejszej Polityce i Instrukcji podczas wykonywania obowiązków służbowych.

.....
(data i podpis osoby składającej oświadczenie)