Załącznik Nr 1 do
Zarządzenia Nr 16.2021
Wójta Gminy Kozielice
z dnia 8 marca 2021 r.

POLITYKA BEZPIECZEŃSTWA INFORMACJI

w Urzędzie Gminy w Kozielicach

1. Postanowienia ogólne.

1) Polityka Bezpieczeństwa Informacji zwana dalej „polityką" jest **dokumentem wewnętrznym i nadrzędnym dla innych procedur oraz regulaminów z zakresu ochrony danych osobowych przyjętych w Urzędzie Gminy w Kozielicach.**
2) Celem niniejszego dokumentu jest wprowadzenie spójnych zasad zachowania bezpieczeństwa danych osobowych w Urzędzie Gminy w Kozielicach, zwanym dalej urzędem, zgodnie z Rozporządzeniem Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE, zwanym w dalszej części polityki „RODO".
3) Zarządzanie bezpieczeństwem informacji jest pojęciem obejmującym zasady zarządzania system chroniącym dane oraz sposoby reagowania na zagrożenia. Zapewnienie odpowiedniej wiedzy zarządzających urzędem oraz siecią informatyczną w zakresie pojawiających się nowych zagrożeń oraz metod ochrony jest kolejnym elementem zapewnienia bezpieczeństwa. Osoby obsługujące systemy przetwarzające dane osobowe są ogniwem zabezpieczeń, na którego skuteczność wpływa również zapewnienie rzetelnej informacji w zakresie sposobu bezpiecznego użytkowania oprogramowania i sprzętu.
4) Zastosowanie niniejszej polityki powinno zapewnić zabezpieczenia adekwatne i proporcjonalne do wyników szacowania ryzyka występującego dla przetwarzanych i przechowywanych danych oraz w systemach informatycznych urzędu.
5) Polityka Bezpieczeństwa Informacji jest jednocześnie dokumentem określającym zadania osób funkcyjnych, pracowników oraz pracowników i współpracowników podmiotów trzecich, które na mocy zawartych umów mają dostęp do informacji chronionych. Ma ona pomóc w zapewnieniu poufności, integralności, dostępności oraz rozliczalności przetwarzanych danych osobowych i innych zidentyfikowanych aktywów informacyjnych.
6) Polityka dotyczy wszystkich danych przetwarzanych w Urzędzie Gminy w Kozielicach, niezależnie od formy przetwarzania danych oraz od tego, czy dane są lub mogą być przetwarzane w zbiorach danych. Polityka reguluje w szczególności przetwarzanie danych w zbiorach ewidencyjnych prowadzonych w formie papierowej oraz systemach informatycznych.
7) Polityka jest przechowywana w wersji elektronicznej oraz w wersji papierowej w siedzibie administratora.

2. Definicje.

Terminom używanym w niniejszej Polityce bezpieczeństwa danych osobowych nadaje się następujące znaczenia:

1) **RODO** - Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (Dz. Urz. UE. L 119/1 z dnia 4 maja 2016 r.).
2) **Administrator danych osobowych /ADO/** – Gmina Kozielice, Urząd Gminy w Kozielicach lub Wójt Gminy Kozielice w zależności od przepisów prawa mających zastosowanie w konkretnej sytuacji, które określają zadania i kompetencje tych podmiotów i organów.
3) **Inspektor Ochrony Danych Osobowych /IODO/** - osoba, wyznaczona przez ADO lub podmiot przetwarzający, posiadająca odpowiednie kwalifikacje zawodowe, wiedzę fachową na temat prawa i praktyk w dziedzinie ochrony danych osobowych oraz umiejętności wymagane do wypełniania zadań związanych z ochroną tych danych.
4) **Administrator Systemu Teleinformatycznego /AST/** - pracownik lub podmiot zewnętrzny odpowiedzialny za prawidłową pracę systemów teleinformatycznych, w tym utrzymanie ciągłości działania oraz bezpieczeństwa w infrastrukturze informatycznej, inwentaryzowanie, okresowe sprawdzanie stanu urządzeń oraz sprzętu pozwalającego na obsługę czynności przetwarzania danych osobowych w systemach informatycznych.
5) **Dane osobowe** - informacje o zidentyfikowanej lub możliwej do zidentyfikowania osobie fizycznej („osobie, której dane dotyczą"). Możliwa do zidentyfikowania osoba fizyczna to osoba, którą można bezpośrednio lub pośrednio zidentyfikować, w szczególności na podstawie identyfikatora takiego jak imię i nazwisko, numer identyfikacyjny, dane o lokalizacji, identyfikator internetowy lub jeden bądź kilka szczególnych czynników określających fizyczną, fizjologiczną, genetyczną, psychiczną, ekonomiczną, kulturową lub społeczną tożsamość osoby fizycznej.
6) **Zbiór danych** – każdy uporządkowany zestaw danych osobowych, dostępny według określonych kryteriów, niezależnie od tego, czy zestaw ten jest scentralizowany, zdecentralizowany czy rozproszony funkcjonalnie lub geograficznie.
7) **Przetwarzanie danych** – jakiekolwiek operacje wykonywane na danych osobowych lub zestawach danych osobowych w sposób zautomatyzowany lub niezautomatyzowany, takie jak: zbieranie, utrwalanie, organizowanie, porządkowanie, przechowywanie, adaptowanie lub modyfikowanie, pobieranie, przeglądanie, wykorzystywanie, ujawnianie poprzez przesłanie, rozpowszechnienie lub innego rodzaju udostępnianie, dopasowywanie lub łączenie, ograniczanie, usuwanie lub niszczenie.
8) **Ograniczenie przetwarzania** - oznaczenie przechowywanych danych osobowych w celu ograniczenia ich przyszłego przetwarzania.
9) **Odbiorca** - osoba fizyczna lub prawna, organ publiczny, jednostka lub inny podmiot, któremu ujawnia się dane osobowe, niezależnie od tego, czy jest stroną trzecią. Organy publiczne, które mogą otrzymywać dane osobowe w ramach konkretnego postępowania zgodnie z prawem Unii lub prawem państwa członkowskiego, nie są jednak uznawane za odbiorców; przetwarzanie tych danych przez te organy publiczne musi być zgodne z przepisami o ochronie danych mającymi zastosowanie stosownie do celów przetwarzania.

10) **Podmiot przetwarzający** - osoba fizyczna lub prawna, organ publiczny, jednostka lub inny podmiot, który przetwarza dane osobowe w imieniu administratora, na podstawie umowy powierzenia przetwarzania danych osobowych.
11) **Pseudonimizacja** - odwracalne przetworzenie danych osobowych w taki sposób, by nie można ich było już przypisać konkretnej osobie, której dane dotyczą, bez użycia dodatkowych informacji, pod warunkiem, że takie dodatkowe informacje są przechowywane osobno i są objęte środkami technicznymi i organizacyjnymi uniemożliwiającymi ich przypisanie zidentyfikowanej lub możliwej do zidentyfikowania osobie fizycznej;
12) **Anonimizacja –** oznacza trwałe, nieodwracalne przekształcenie danych osobowych powodujące brak możliwości przyporządkowania informacji konkretnej osobie fizycznej.
13) **Zgoda na przetwarzanie danych osobowych** – dobrowolne, konkretne, świadome i jednoznaczne oświadczenie woli osoby, której dane są przetwarzane przyzwalające na przetwarzanie dotyczących jej danych osobowych.
14) **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.
15) **Osoba upoważniona do przetwarzania danych osobowych** – osoba, która złożyła ADO oświadczenie o zachowaniu w tajemnicy przetwarzanych danych i stosowanych sposobach zabezpieczenia tych danych, posiadająca imienne upoważnienie wydane przez ADO, określające imię i nazwisko osoby upoważnionej, datę nadania i ustania oraz zakres upoważnienia do przetwarzania danych osobowych oraz identyfikator jeżeli dane są przetwarzane w systemie informatycznym.
16) **System informatyczny** – zespół współpracujących ze sobą urządzeń, programów oraz narzędzi programowych zastosowanych w celu przetwarzania danych.
17) **Sieć lokalna** – połączenie systemów informatycznych administratora wyłącznie dla jego własnych potrzeb przy wykorzystaniu urządzeń i sieci telekomunikacyjnych.
18) **Użytkownik** – każda osoba upoważniona przez ADO do przetwarzania danych, a w szczególności osoba fizyczna świadcząca na rzecz administratora pracę lub usługi w oparciu o jakikolwiek stosunek prawny, jeżeli to świadczenie pracy lub usług wiąże się z przetwarzaniem danych.
19) **Zabezpieczenie danych** – zabezpieczenie danych poprzez wdrożenie i eksploatację środków technicznych i organizacyjnych zapewniających ochronę danych przed ich nieuprawnionym przetwarzaniem.
20) **Identyfikator (login)** – ciąg znaków literowych, cyfrowych lub innych jednoznacznie identyfikujący użytkownika upoważnionego do przetwarzania danych w systemie informatycznym.
21) **Hasło** – ciąg znaków literowych, cyfrowych lub innych, znany jedynie administratorowi oraz użytkownikowi upoważnionemu do przetwarzania danych w systemie informatycznym.
22) **Uwierzytelnianie** – proces, którego celem jest weryfikacja tożsamości deklarowanej przez użytkownika.

3. Podmioty w systemie ochrony danych osobowych.

Podmiotami lub organami odpowiedzialnymi za ochronę i przetwarzanie danych osobowych w Urzędzie Gminy w Kozielicach są:

1). Administrator Danych Osobowych (ADO), do którego zadań należą:
a. podejmowanie decyzji o celach i środkach przetwarzania danych osobowych;
b. wdrażanie odpowiednich środków technicznych i organizacyjnych, mających na celu zabezpieczanie przetwarzanych danych oraz zapewnianie poufności, integralności i dostępności danych;
c. wyznaczenie Inspektora Ochrony Danych Osobowych;
d. wyznaczenie Administratora Systemów Teleinformatycznych oraz określenie zakresu jego zadań i czynności w zakresie ochrony danych osobowych;
e. podejmowanie odpowiednich działań w przypadku naruszenia lub podejrzenia naruszenia przetwarzanych danych zgodnie z procedurami określonymi w niniejszej polityce;
f. upoważnienie poszczególnych osób do przetwarzania danych osobowych w określonym indywidualnie zakresie;
g. podejmowanie decyzji dotyczących przeprowadzenia oceny skutków planowanych operacji przetwarzania danych po konsultacji z IODO;
h. wdrożenie Polityki Bezpieczeństwa Informacji;
i. wdrożenie rejestru czynności przetwarzania danych osobowych, rejestru upoważnień, rejestru umów powierzenia przetwarzania danych osobowych, rejestru naruszeń i innych rejestrów oraz procedur wynikających z niniejszej polityki;
j. kontrola przestrzegania procedur przetwarzania danych osobowych w urzędzie.

2). Inspektor Ochrony Danych Osobowych (IODO), do którego zadań należą:
a. informowanie ADO oraz użytkowników, którzy przetwarzają dane osobowe, o obowiązkach spoczywających na nich na mocy obowiązujących przepisów, kodeksów postępowania i zatwierdzonych mechanizmów certyfikacji;
b. nadzorowanie i monitorowanie przestrzegania przepisów prawa o ochronie danych osobowych oraz wewnętrznych procedur w dziedzinie ochrony danych osobowych;
c. prowadzenie szkoleń z zakresu ochrony danych osobowych;
d. aktualizacje i sprawowanie nadzoru nad dokumentacją z zakresu ochrony danych osobowych;
e. prowadzenie i aktualizacja rejestru czynności przetwarzania danych (RCPD);
f. prowadzenie rejestru upoważnień do przetwarzania danych;
g. prowadzenie i aktualizacja rejestru umów powierzenia przetwarzania danych osobowych;
h. prowadzenie i aktualizacja rejestru naruszeń zasad ochrony danych osobowych;,
i. informowanie ADO o wystąpieniu incydentu,
j. współpraca z ADO w zakresie oceny skutków planowanych operacji przetwarzania danych;
k. pełnienie funkcji punktu kontaktowego dla Prezesa Urzędu Ochrony Danych Osobowych w kwestiach związanych z przetwarzaniem danych osobowych;
l. weryfikacja zgodności przetwarzania danych osobowych z przepisami o ochronie danych osobowych oraz opracowanie w tym zakresie minimum raz w roku sprawozdania dla ADO;

m. nadzorowanie i monitorowanie realizacji obowiązku informacyjnego zgodnie z wymogami RODO;
n. wykonania szacowania ryzyka i oceny skutków przed wprowadzeniem nowej technologii (np. nowego systemu informatycznego, w którym przetwarzane będą dane osobowe) wraz z administratorem systemu i właścicielem zasobu.

3). Administrator Systemów Teleinformatycznych (ASI) – zadania określone zakresem czynności zawarte w załączniku Nr 1 do Zarządzenia Nr 94.2020 Wójta Gminy Kozielice z dnia 23 listopada 2020 r.

4). Osoby upoważnione do przetwarzania danych osobowych – to osoby dopuszczone do przetwarzania danych osobowych, na podstawie upoważnienia przez ADO, do zadań tych osób należą m.in:

a. przestrzeganie przepisów prawa powszechnie obowiązującego i regulacji dotyczących ochrony danych osobowych;
b. przetwarzanie danych zgodnie z zakresem udzielonego upoważnienia;
c. zachowanie w tajemnicy danych osobowych oraz sposobów ich zabezpieczenia;
d. niezwłoczne zgłaszanie incydentów dot. bezpieczeństwa danych osobowych.

4. Podstawy przetwarzania danych osobowych.

1) Przetwarzanie danych osobowych jest dopuszczalne tylko wtedy, **gdy zostanie spełniona jedna z przesłanek wynikających z art. 6 RODO** w przypadku przetwarzania danych zwykłych.
2) Dane osobowe w jednostce przetwarzane są gdy:
   a. osoba, której dane dotyczą **wyraziła zgodę** na przetwarzanie swoich danych osobowych w jednym lub większej liczbie określonych celów;
   b. przetwarzanie jest **niezbędne do wykonania umowy**, której stroną jest osoba, której dane dotyczą, lub do podjęcia działań na żądanie osoby, której dane dotyczą, przed zawarciem umowy;
   c. przetwarzanie jest **niezbędne do wypełnienia obowiązku prawnego** ciążącego na administratorze;
   d. przetwarzanie jest **niezbędne do ochrony żywotnych interesów** osoby, której dane dotyczą, lub innej osoby fizycznej;
   e. przetwarzanie jest **niezbędne do wykonania zadania realizowanego w interesie publicznym lub w ramach sprawowania władzy publicznej** powierzonej administratorowi.
3) W przypadku przetwarzania danych na podstawie zgody osoby, której dane dotyczą, należy stosować **oświadczenie o wyrażeniu zgody na przetwarzanie danych osobowych,** którego wzór stanowi załącznik nr 1 do niniejszej polityki, natomiast załącznik nr 2 stanowi wzór **oświadczenia o odwołaniu zgody na przetwarzanie danych osobowych.**

5. Obowiązki osób przetwarzających dane osobowe.

1) Każda osoba przetwarzająca dane osobowe na potrzeby urzędu jest zobowiązana zapoznać się z treścią niniejszej Polityki Bezpieczeństwa Informacji oraz bezwzględnie stosować się do jej zapisów.
2) Do przetwarzania danych osobowych mogą być dopuszczone **tylko osoby posiadające pisemne upoważnienia do przetwarzania danych osobowych,** wydane przez ADO, **wraz z pisemnym oświadczeniem o zobowiązaniu się do zachowania poufności**

i w tajemnicy danych osobowych. Wzór upoważnienia do przetwarzania danych osobowych wraz z oświadczeniem o zachowaniu poufności określa załącznik nr 3 do niniejszej polityki.

3) Wydane upoważnienia podlegają ewidencji w „**Rejestrze upoważnień do przetwarzania danych osobowych",** prowadzonego przez IODO, wg wzoru określonego w załączniku nr 4 do niniejszej polityki.
4) Wszystkie osoby zatrudnione w Urzędzie Gminy w Kozielicach są zobowiązane do zachowania tajemnicy i poufności danych osobowych oraz sposobów ich zabezpieczenia. W tym celu podpisują pisemne oświadczenie o zobowiązaniu się do zachowania poufności i w tajemnicy danych osobowych.
5) Egzemplarz oryginalnego upoważnienia do przetwarzania danych osobowych, podpisany własnoręcznie przez pracownika, przechowuje się w aktach osobowych pracownika.
6) Rozwiązanie stosunku pracy lub odwołanie z pełnionej funkcji powoduje **wygaśnięcie upoważnienia do przetwarzania danych osobowych.**
7) Upoważnienia do przetwarzania danych osobowych udzielane są również wolontariuszom, praktykantom, stażystom. Zakończenie stażu, praktyki, wolontariatu powoduje wygaśnięcie upoważnienia.
8) W przypadku zmiany stanowiska, zakresu obowiązków lub w sytuacji, która wpływa bezpośrednio na rodzaj i zakres przetwarzanych danych osobowych, **pracownik ds. kadr jest zobowiązany do niezwłocznego zgłoszenia ADO konieczności zmiany upoważnienia lub jego aktualizacji.**
9) Przed rozpoczęciem przetwarzania należy złożyć **oświadczenie o zapoznaniu się z dokumentacją ochrony danych osobowych,** w tym z Polityką Bezpieczeństwa Informacji.
10) Dane osobowe można przetwarzać wyłącznie w zakresie ustalonym przez ADO, **zawartym w upoważnieniu i tylko w celu wykonywania obowiązków służbowych.**
11) **Przestrzeganie tajemnicy danych osobowych obowiązuje przez cały okres zatrudnienia, a także po ustaniu stosunku pracy lub odwołania z pełnionej funkcji.**
12) Przetwarzane dane osobowe muszą być zabezpieczone przed udostępnieniem osobom nieupoważnionym.
13) Pracownicy są zobowiązani do przestrzegania przepisów prawa powszechnie obowiązującego i regulacji dotyczących ochrony danych osobowych. W tym celu zobowiązani są do:
    a. pisemnego zgłaszania nowych zbiorów danych osobowych do IODO.
    b. bieżącej oceny funkcjonowania mechanizmów zabezpieczeń i ochrony;
    c. występowania z wnioskami w sprawie wprowadzenia niezbędnych zmian w zakresie ochrony danych osobowych.
14) Pracownicy przetwarzający dane osobowe obowiązani są:

    a. dołożyć należytej staranności w celu ochrony interesu osób, których dane są gromadzone i przetwarzane.
    b. przestrzegać i realizować prawa osób, których dane są przetwarzane, określone w RODO i pkt 8 niniejszej polityki.
    c. powiadomić o sprostowaniu lub usunięciu danych osobowych lub o ograniczeniu przetwarzanie, chyba, że okaże się to niemożliwe lub będzie wymagać niewspółmiernie dużego wysiłku.
15) Naruszenie postanowień Polityki Bezpieczeństwa Informacji może skutkować zablokowaniem dostępu pracownika do informacji chronionych i systemów. **W przypadku ciężkich naruszeń takie działanie może prowadzić do wszczęcia**

postępowania dyscyplinarnego oraz do rozwiązania bądź wypowiedzenia umowy o pracę. W przypadku poniesienia strat w wyniku naruszenia, Wójt Gminy Kozielice może dochodzić roszczeń odszkodowawczych na drodze sądowej.

16) **Każde naruszenie bezpieczeństwa informacji powinno być niezwłocznie zgłaszane ADO i IODO lub w przypadku naruszeń bezpieczeństwa systemów teleinformatycznych AST.**
17) W razie wykrycia naruszenia ochrony danych osobowych każdy pracownik ma obowiązek postępować zgodnie z procedurami zawartymi w niniejszej polityce.

6. Zbieranie danych osobowych.

1) Dane osobowe przetwarzane w urzędzie mogą być pozyskiwane bezpośrednio od osób, których te dane dotyczą. Administrator podczas pozyskiwania tych danych podaje informacje wynikające z obowiązku informacyjnego, o którym mowa w pkt 7 polityki.
2) W przypadku zbierania danych osobowych nie od osoby, której te dane dotyczą, należy zapewnić, że istnieje podstawa prawna przetwarzania danych i również wypełnić obowiązek informacyjny określony w pkt 7 polityki.
3) Przetwarzanie, w tym przechowywanie danych osobowych powinno się odbywać w postaci umożliwiającej identyfikację osób, których dotyczą.
4) Przetwarzanie, w tym przechowywanie danych osobowych powinno się odbywać nie dłużej niż jest to niezbędne do realizacji celu przetwarzania.
5) Dane osobowe, które są zbierane powinny być merytorycznie poprawne.
6) Zakres danych osobowych, które są zbierane powinien być adekwatny w stosunku do celu, w jakim dane zostały zebrane.
7) Zebrane dane po ich wykorzystaniu mogą być przechowywane w przypadku, gdy odpowiedni przepis prawa wymaga ich archiwizacji przez określony czas.
8) **Przetwarzanie danych osobowych kandydata do pracy** jest możliwe podczas procesu rekrutacji **wyłącznie po uzyskaniu jego pisemnego oświadczenia o wyrażeniu zgody na przetwarzanie danych osobowych w celu przeprowadzenia procesu rekrutacyjnego lub przyszłych procesów rekrutacyjnych**. W przypadku wymagań wynikających z zapisów odpowiednich przepisów prawa, po zakończeniu rekrutacji dokumenty zawierające dane osobowe kandydatów do pracy są archiwizowane zgodnie z zapisami tych przepisów. W przypadku wycofania zgody kandydata bądź żądania usunięcia danych (prawo do bycia zapomnianym) dane osobowe są skutecznie usuwane ale pod warunkiem poinformowania osoby, której dane dotyczą o braku możliwości wnoszenia roszczeń i odwołań w stosunku do procesu rekrutacyjnego, do którego dane zostały przekazane.

7. Obowiązek informacyjny przy przetwarzaniu danych.

1) **Obowiązek informacyjny** spoczywający na administratorze w myśl art. 13 i 14 RODO jest realizowany poprzez **przekazanie osobie, której dane są przetwarzane informacji dotyczących pozyskiwania danych osobowych**, a także ich dalszego przetwarzania.
2) Obowiązek informacyjny jest realizowany zarówno w przypadku zbierania danych od osoby, której dane dotyczą, jak również z innych źródeł.
3) Administrator realizuje obowiązek informacyjny poprzez wykorzystanie odpowiednich środków, które umożliwią w zwięzłej, przejrzystej i łatwo dostępnej formie udzielenie osobie, której dane dotyczą wszelkich informacji, o których mowa w art. 13 i 14 RODO.

4) Jedną z form spełniania obowiązku informacyjnego jest udostępnienie osobom, których dane osobowe są przetwarzane **klauzul informacyjnych. Klauzule informacyjne winny być każdorazowo dostosowane do celu przetwarzania, podstawy prawnej i okresu przechowywania danych**.
5) Zwolnienie z realizacji obowiązku informacyjnego znajduje zastosowanie w sytuacji, gdy dane pozyskiwane są od osoby, której te dane dotyczą, a podmiot ten dysponuje już informacjami, o których mowa w art. 13 RODO oraz w zakresie uregulowanym przez przepisy krajowe, w szczególności przez ustawę o ochronie danych osobowych.
6) Obowiązek informacyjny należy spełnić w momencie zbierania danych.

8. Prawa osób, których dane dotyczą.

1) Każdej osobie przysługuje prawo do kontroli przetwarzania danych, które jej dotyczą, zawartych w zbiorach danych osobowych przetwarzanych i przechowywanych w urzędzie, a zwłaszcza prawo do uzyskania wyczerpującej informacji o przetwarzanych danych osobowych, które jej dotyczą.
2) Zgodnie z RODO, osobom, których dane osobowe są przetwarzane przysługują następujące prawa:
a. prawo dostępu do danych,
b. prawo do sprostowania danych,
c. prawo do usunięcia danych („prawo do bycia zapomnianym"),
d. prawo do ograniczenia przetwarzania,
e. prawo do przenoszenia danych,
f. prawo wniesienia sprzeciwu,
g. prawo do cofnięcia zgody w dowolnym momencie bez wpływu na zgodność z prawem przetwarzania, którego dokonano na podstawie zgody przed jej cofnięciem.
h. prawo do wniesienia skargi do Urzędu Ochrony Danych Osobowych**,** w przypadku przetwarzania danych osobowych z naruszeniem przepisów RODO.
3) Na wniosek osoby, której dane dotyczą, zgodnie z pkt 8 ppkt. 1) i 2), ADO jest zobowiązany do udzielenia informacji. Informacja powinna być udzielona w formie pisemnej oraz powszechnie zrozumiałej.
4) W razie wniesienia żądania oraz wykazania przez osobę, które dane dotyczą, że jej dane osobowe są niekompletne, nieaktualne, nieprawdziwe lub zostały zebrane z naruszeniem przepisów albo są zbędne do realizacji celu dla którego zostały zebrane, ADO bez zbędnej zwłoki dokonuje uzupełnienia, uaktualnienia, sprostowania danych, czasowego lub stałego wstrzymania przetwarzania kwestionowanych danych lub ich usunięcia ze zbioru, chyba, że dotyczy to danych osobowych, w odniesieniu do których tryb ich uzupełnienia, uaktualnienia lub sprostowania określają odrębne przepisy.

9. Obszary przetwarzania danych osobowych, zbiory danych osobowych, rejestr czynności przetwarzania danych osobowych.

1) Obszar, w którym przetwarzane są dane osobowe obejmuje:
a. urząd,
b. komputery przenośne oraz inne nośniki danych wykorzystywane przez użytkowników, a znajdujące się poza obszarem wskazanym w lit. a.
2) W Urzędzie Gminy w Kozielicach dane osobowe przetwarzane są w ramach zbiorów danych osobowych. Wykaz obszarów podlega aktualizacji w zależności od potrzeb i zatwierdzeniu przez ADO.

3) Osoby upoważnione do przetwarzania danych osobowych mogą przetwarzać dane tylko w wyznaczonych do tego miejscach z zachowaniem dedykowanego do tej czynności sprzętu informatycznego oraz innych urządzeń.

4). Wynoszenie zbiorów danych osobowych poza obszar przetwarzania możliwy jest za wyłączną zgodą ADO.

5). Administrator prowadzi **Rejestr Czynności Przetwarzania Danych Osobowych (RCPD).** Wzór rejestru czynności przetwarzania stanowi załącznik nr 5 do polityki. Rejestr prowadzony i na bieżąco aktualizowany jest przez Inspektora Ochrony Danych Osobowych. Każda aktualizacja rejestru podlega zatwierdzeniu przez ADO.

10. Powierzenie przetwarzania danych osobowych.

1) Administrator Danych Osobowych (ADO):

a. przekazuje dane do podmiotów trzecich zgodnie z przepisami prawa powszechnie obowiązującego np. do Zakładu Ubezpieczeń Społecznych, Urzędu Skarbowego, Państwowej Inspekcji Pracy, sądów powszechnych, Policji i Prokuratury.

b. **powierza przetwarzanie danych innemu podmiotowi w drodze umowy powierzenia przetwarzania danych osobowych**, zawartej w formie pisemnej, zgodnie z wymogami wskazanymi dla takich umów w art. 28 RODO.

2) Podmiot, któremu powierzono przetwarzanie danych osobowych, może przetwarzać dane wyłącznie w zakresie i celu przewidzianym w umowie oraz zgodnie z zasadami przetwarzania i zabezpieczeniami określonymi w umowie.

3) Podmiot, któremu powierzono przetwarzanie danych osobowych jest obowiązany zastosować środki techniczne i organizacyjne zapewniające ochronę przetwarzanych danych osobowych a w szczególności powinien stosować techniczne i organizacyjne środki bezpieczeństwa, o których mowa w art. 32 ust. 1 RODO.

4) Umowy powierzenia przetwarzania danych osobowych podlegają ewidencji w **Rejestrze Umów Powierzenia Przetwarzania Danych Osobowych**, określonym w załączniku nr 6 do polityki. Rejestr prowadzony jest przez Inspektora Ochrony Danych Osobowych.

11. Przekazywanie danych do państwa trzeciego.

Administrator nie będzie przekazywał danych do państwa trzeciego, poza sytuacjami w których następuje to na wniosek podmiotów takich jak sądy, urzędy, organy ścigania lub osoby, której dane dotyczą.

12. Określenie środków fizycznych, technicznych i organizacyjnych niezbędnych dla zapewnienia integralności, poufności oraz rozliczalności przetwarzania danych osobowych.

1) Administrator danych osobowych zapewnia zastosowanie środków technicznych i organizacyjnych niezbędnych dla zapewnienia integralności, poufności oraz rozliczalności przetwarzanych danych. **Wykaz stosowanych przez administratora środków fizycznych, technicznych i organizacyjnych** stanowi załącznik nr 7 do polityki.

2) Zastosowane środki ochrony powinny być adekwatne do stwierdzonego poziomu ryzyka dla poszczególnych rodzajów zbiorów danych i kategorii danych oraz systemów informatycznych.

13. Dodatkowe obowiązki po stronie użytkowników.

Ze względów bezpieczeństwa przetwarzanych danych użytkowników zobowiązuje się do:

1) **Zachowania w poufności wszelkich informacji w tym w szczególności przetwarzanych danych osobowych**.
2) **Stosowania zasady „czystego biurka”** - w trakcie pracy użytkownik powinien mieć na biurku tylko te materiały, które są niezbędne do wykonywania obowiązków służbowych. W przypadku opuszczenia stanowiska pracy materiały zawierające dane, wymagające szczególnej ochrony, powinny być zabezpieczone przed dostępem osób nieuprawnionych. Po zakończeniu dnia pracy każdy użytkownik zobowiązany jest do zabezpieczenia wszelkich dokumentów i nośników zawierających istotne dane, w celu uniemożliwienia dostępu do nich osób nieupoważnionych, przechowywania dokumentacji papierowej w szafach zamykanych na klucz.
3) **Stosowania zasady „czystego ekranu”** - w przypadku chwilowego opuszczenia stanowiska pracy użytkownik zobowiązany jest do wylogowania się z systemu bądź zablokowania dostępu do pulpitu stacji roboczej w celu uniemożliwienia dostępu do systemu operacyjnego lub aplikacji przez osoby niepowołane. Ponadto w trakcie pracy użytkownik powinien mieć otwarte tylko te aplikacje, które są niezbędne do wykonywania obowiązków służbowych.
4) **Stosowania zasady „czystego kosza”** oznaczającej ochronę niepotrzebnych dokumentów papierowych i miękkich nośników zawierających dane osobowe w sposób uniemożliwiający ich ponowne odczytanie poprzez bieżące korzystanie z niszczarek i innego sprzętu pozwalającego na ich fizyczne zniszczenie
5) **Stosowania zasady „czystej drukarki”** mającej na celu uniemożliwienie osobom trzecim zabrania wydruków z drukarek (szczególnie ogólnodostępnych). Drukowane informacje powinny być zabierane z drukarek niezwłocznie po wydrukowaniu. W przypadku nieudanej próby wydrukowania należy skontaktować się z osobą odpowiedzialną za eksploatację urządzenia, jeżeli zachodzi podejrzenie, iż wydruk zostanie wydrukowany bez nadzoru.
6) **Niepozostawiania osób postronnych w pomieszczeniu**, **w którym przetwarzane są dane osobowe**, bez obecności osoby upoważnionej.
7) **Stosowania się do pozostałych instrukcji i zarządzeń wewnętrznych związanych z bezpieczeństwem informacji,** w tym m.in. „Instrukcji postępowania z kluczami oraz zabezpieczenia pomieszczeń i obiektu Urzędu Gminy w Kozielicach”, „Instrukcji zarządzania system informatycznym”.
8) Użytkownicy - osoby przetwarzające dane osobowe mogą korzystać **wyłącznie z elektronicznych nośników** (w szczególności pendriv-y, dysków zewnętrznych, CD-R, DVD) oraz komputerów przenośnych **przeznaczonych do użytku służbowego.**
9) Szczegółowe zasady bezpieczeństwa systemów informatycznych określa „**Instrukcja zarządzania system informatycznym”** stanowiąca załącznik nr 8 do niniejszej polityki.

14. Naruszenia zasad ochrony danych osobowych.

1) W przypadku stwierdzenia naruszenia zabezpieczeń lub zaistnienia sytuacji, które mogą wskazywać na naruszenie zabezpieczenia danych osobowych, każdy pracownik/użytkownik przetwarzający dane osobowe **zobowiązany jest przerwać czynności i niezwłocznie zgłosić ten fakt bezpośredniemu przełożonemu**, a następnie postępować stosownie do podjętej przez niego decyzji.
2) **Zgłoszenie powinno zawierać**:
   a. imię i nazwisko zgłaszającego,
   b. określenie sytuacji i czasu w jakim stwierdzono naruszenie zabezpieczeń danych osobowych;
   c. określenie wszelkich istotnych informacji mogących wskazywać na przyczynę naruszenia;
   d. określenie znanych zgłaszającemu sposobów zabezpieczenia systemu oraz wszelkich kroków podjętych po ujawnieniu zdarzenia.
3). **Osoba zgłaszająca naruszenie w miarę możliwości powinna zabezpieczyć materiał dowodowy** np.: zrobić zdjęcie ekranu komputera, co do którego zaistniało podejrzenie, że jego działanie odbiega od normy. Osobą odpowiedzialną za przyjmowanie zgłoszeń naruszeń w urzędzie gminy jest Inspektor Ochrony Danych Osobowych (IODO).
4). W przypadku stwierdzenia naruszenia zasad ochrony danych ADO **dokonuje oceny, czy zaistniałe naruszenie mogło powodować ryzyko naruszenia praw lub wolności osób fizycznych** i dokonuje kwalifikacji naruszenia jako naruszenie niskie lub wysokie.
5). W przypadku kwalifikacji naruszenia jako niskie należy dokonać wpisu do **rejestru naruszeń**, którego wzór stanowi załącznik nr 9 do polityki.
6). **Naruszenia zakwalifikowane jako wysokie, podlegają zgłoszeniu do organu nadzorczego „niezwłocznie", jednak nie później niż po upływie 72 godzin po stwierdzeniu naruszenia.**
7) Jeżeli ryzyko naruszenia praw i wolności jest wysokie, ADO zawiadamia o incydencie także osobę, której dane dotyczą.

15. Przeprowadzanie okresowych analiz ryzyka w zakresie bezpieczeństwa informacji.

1) W celu zapewnienia bezpieczeństwa informacji w Urzędzie Gminy w Kozielicach minimum raz w roku przeprowadzana jest „**Analiza Ryzyka"** zgodnie z art. 5 ust. 2 oraz Motywem 76 Preambuły „RODO".
2) Głównym celem analizy ryzyka bezpieczeństwa informacji jest wyznaczenie właściwych kierunków działania kierownictwa oraz określenie priorytetów dla zarządzania ryzykami i zabezpieczeniami. Wyniki analizy ryzyka prowadzą do opracowania planu postępowania z ryzykiem obejmującego wprowadzenie rozwiązań umożliwiających odpowiednio: unikanie tych ryzyk, ograniczanie ich do akceptowanego poziomu, przeniesienie lub świadomą ich akceptację.
3) Zaleca się, by zarządzanie ryzykiem w bezpieczeństwie informacji zapewniało:
   a. zidentyfikowanie ryzyka,
   b. oszacowanie ryzyka z punktu widzenia następstw dla działalności oraz prawdopodobieństwa wystąpienia,
   c. informowanie o prawdopodobieństwie i następstwach ryzyka oraz zrozumienie tych informacji,
   d. ustanowienie priorytetów postępowania z ryzykiem,
   e. określenie priorytetów dla działań podjętych w celu zredukowania ryzyka,

f. regularne monitorowanie i przegląd różnych typów ryzyka oraz procesu zarządzania ryzykiem,
g. zbieranie informacji w celu doskonalenia podejścia do zarządzania ryzykiem,
h. szkolenie kierownictwa w zakresie ryzyka oraz działań podejmowanych w celu postępowania z ryzykiem.

16. Postanowienia końcowe.

1. Niniejsza Polityka Bezpieczeństwa Informacji obowiązuje na wszystkich stanowiskach oraz obszarach, gdzie dochodzi do przetwarzania informacji podlegających ochronie.
2. Niniejsza polityka podlega regularnym przeglądom i aktualizacjom dokonywanym przez IODO i ADO.
3. Integralną część polityki stanowią następujące załączniki:

Załącznik nr 1 „Wzór Oświadczenia o wyrażeniu zgody na przetwarzanie danych osobowych”;

Załącznik nr 2 „Wzór Oświadczenia o odwołaniu zgody na przetwarzanie danych osobowych”;

Załącznik nr 3 „Wzór upoważnienia do przetwarzania danych osobowych wraz z oświadczeniem o zachowaniu poufności i tajemnicy przetwarzanych danych osobowych”;

Załącznik nr 4 „Wzór Rejestru Upoważnień do przetwarzania danych osobowych”;

Załącznik nr 5 „Wzór Rejestru Czynności Przetwarzania Danych Osobowych”;

Załącznik nr 6 „Rejestr Umów Powierzenia Przetwarzania Danych Osobowych”;

Załącznik nr 7 „Wykaz środków fizycznych, technicznych i organizacyjnych stosowanych w celu zabezpieczenia danych oraz informacji”;

Załącznik nr 8 „Instrukcja zarządzania system informatycznym”;

Załącznik nr 9 „Wzór rejestru naruszeń zasad ochrony danych osobowych”.