

Zarządzenie Nr 38.2022
Wójta Gminy Przytyk
z dnia 8 lipca 2022 roku

w sprawie zmiany Zarządzenia nr 23a.2020 Wójta Gminy Przytyk z dnia 10 czerwca 2020r. w sprawie wprowadzenia Polityki Ochrony Danych Osobowych w Urzędzie Gminy w Przytyku

Na podstawie art. 24 ust. 1 i 2 Rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016r. 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) zarządzam, co następuje:

§ 1

Zmianie ulega treść załącznika do Zarządzenia Nr 23a.2020 Wójta Gminy Przytyk z dnia 10 czerwca 2020r. w sprawie wprowadzenia Polityki Ochrony Danych Osobowych w Urzędzie Gminy w Przytyku poprzez dodanie jako części integralnej następujących elementów:

1. Procedury do Polityki ochrony danych osobowych.
2. Instrukcja Zarządzania Systemem Informatycznym służącym do przetwarzania danych osobowych wraz z procedurami dotyczącymi cyberbezpieczeństwa i bezpieczeństwa informacji

§ 2

Pozostałe zapisy zarządzenia nie ulegają zmianie.

§ 3

Zarządzenie wchodzi w życie z dniem podjęcia.


Z up. WÓJTA
mgr Magdalena Kowalczyk
ZASTĘPCA WÓJTY
Zastępca Wójta Gminy Przytyk

POLITYKA OCHRONY DANYCH OSOBOWYCH

Urząd Gminy w Przytyku
ul. Zachęta 57, 26-650 Przytyk

POLITYKA OCHRONY DANYCH OSOBOWYCH

Urząd Gminy w Przytyku
ul. Zachęta 57, 26-650 Przytyk

POLITYKA OCHRONY DANYCH OSOBOWYCH

Urząd Gminy w Przytyku
ul. Zachęta 57, 26-650 Przytyk

SPIS TREŚCI

A. POSTANOWNIENIA OGÓLNE	4
1. Cel i podstawa prawna Polityki ochrony danych osobowych	4
2. Słowniczek pojęć użytych w polityce	4
3. Zakres informacji objętych Polityką ochrony danych osobowych oraz zakres zastosowania	6
B. PODMIOTY ODPOWIEDZIALNE ZA OCHRONĘ DANYCH OSOBOWYCH	7
1. Struktura organizacji ochrony danych osobowych	7
1.1 Administrator Danych	7
2.1 Administrator Systemów Informatycznych	9
3.1 Inspektor Ochrony Danych	10
4.1 Osoby upoważnione do przetwarzania danych osobowych	12
C. ZASADY PRZETWARZANIA DANYCH OSOBOWYCH	13
1. Ogólne zasady przetwarzania danych osobowych	13
2. Zakres przetwarzanych danych osobowych	13
3. Dopuszczenie osób do przetwarzania danych osobowych	15
4. Powierzenie przetwarzania danych osobowych	15
5. Udostępnianie danych osobowych	17
6. Przekazywanie danych osobowych do Państw Trzecich	17
7. Współadministrowanie danymi osobowymi	19
8. Audyty zgodności przetwarzania danych osobowych	19
9. Realizacja praw osób, których dane dotyczą	20
10. Ochrona danych osobowych w fazie projektowania oraz domyślna ochrona danych osobowych	21
11. Ocena skutków dla ochrony danych osobowych (privacy impact assessment)	22
12. Incydenty ochrony danych osobowych	22
13. Ogólne zasady bezpieczeństwa ochrony danych osobowych	22
14. Przeglądy i aktualizacja Polityki ochrony danych osobowych	24
15. Procedura szkoleń w zakresie udzielania upoważnień do przetwarzania danych osobowych	25
D. ZAŁĄCZNIKI	26

POLITYKA OCHRONY DANYCH OSOBOWYCH

Urząd Gminy w Przytyku

ul. Zachęta 57, 26-650 Przytyk

Załącznik nr 1 Wykaz procesów przetwarzania danych osobowych Wraz z osobami zarządzającymi procesami przetwarzania danych.....	27
Załącznik nr 2 – Zasady retencji danych osobowych.....	32
Załącznik nr 3 –Upoważnienia do przetwarzania danych osobowych	40
Załącznik nr 4 – Wzór ewidencji osób upoważnionych do przetwarzania danych osobowych	45
Załącznik nr 5 – Wzory wyznaczenia oraz odwołania Inspektora Ochrony Danych	46
Załącznik nr 6 – Wzory wyznaczenia oraz odwołania Administratora Systemów Informatycznych.....	48
Załącznik nr 7 Oświadczenie pracownika o zapoznaniu się z dokumentacją.....	50
Załącznik nr 8 Rejestr kategorii czynności przetwarzania podmiotu przetwarzającego.....	51
Załącznik nr 9 Rejestr czynności przetwarzania administratora	52

POLITYKA OCHRONY DANYCH OSOBOWYCH

Urząd Gminy w Przytyku

ul. Zachęta 57, 26-650 Przytyk

A. POSTANOWNIENIA OGÓLNE

1. CEL I PODSTAWA PRAWNA POLITYKI OCHRONY DANYCH OSOBOWYCH

Polityka ochrony danych osobowych została opracowana i wdrożona w strukturze Administratora Danych w celu zapewnienia zgodności przetwarzania danych osobowych z wymogami obowiązujących w tym zakresie polskich i europejskich aktów prawnych, w szczególności:

1. 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),
2. Ustawy z dnia 10 maja 2018 r. o ochronie danych osobowych tj. Dz. U. z 2019r. poz. 730

Politykę stosuje się do danych osobowych przetwarzanych przez Administratora danych osobowych w systemie informatycznym, danych osobowych zapisanych na zewnętrznych nośnikach informacji, zbiorów przetwarzanych metodą tradycyjną oraz informacji dotyczących bezpieczeństwa przetwarzania danych osobowych, w szczególności dotyczących wdrożonych zabezpieczeń technicznych i organizacyjnych.

Polityka ochrony danych osobowych ma zastosowanie do wszystkich pracowników Administratora Danych, którzy w zakresie swoich obowiązków służbowych przetwarzają dane osobowe, jak również innych osób, które z upoważnienia Administratora Danych uzyskały dostęp do danych osobowych. Każda z tych osób została zapoznana z najważniejszymi procedurami bezpieczeństwa danych opisanymi w Polityce ochrony danych osobowych i zobowiązana do ich przestrzegania w zakresie wynikającym z przydzielonych zadań. Osoby, o których mowa złożyły oświadczenie o zapoznaniu się z procedurami bezpieczeństwa danych oraz zobowiązały się do ich stosowania.

Wszelkie wątpliwości dotyczące sposobu interpretacji zapisów Polityki ochrony danych osobowych, powinny być rozstrzygane na korzyść zapewnienia możliwie najwyższego poziomu ochrony danych osobowych oraz realizacji praw osób, których dane dotyczą.

2. SŁOWNICZEK POJĘĆ UŻYTYCH W POLITYCE

1. **Administrator Danych (ADO)** – Urząd Gminy w Przytyku, ul. Zachęta 57, 26-650 Przytyk

Urząd Gminy w Przytyku

ul. Zachęta 57, 26-650 Przytyk

2. **Administrator Systemów Informatycznych (ASI)** – osoba wyznaczona przez Administratora Danych, koordynująca działania związane z zapewnieniem bezpieczeństwa systemów informatycznych, w tym również odpowiadająca za nadzór nad zabezpieczeniem danych osobowych przetwarzanych w systemach informatycznych wykorzystywanych przez Administratora Danych,
3. **Inspektor Ochrony Danych (IOD)** – osoba wyznaczona przez Administratora Danych, koordynująca procesy związane z przestrzeganiem zasad ochrony danych osobowych w ramach procesów przetwarzania danych osobowych zachodzących w strukturze Administratora Danych,
4. **Polityka** – niniejsza Polityka ochrony danych osobowych,
5. **przetwarzanie** – operacja 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,
6. **dane osobowe** – informacje o zidentyfikowanej lub możliwej do zidentyfikowania osobie fizycznej („osobie, której dane dotyczą”), gdzie poprzez możliwą do zidentyfikowania osobę fizyczną rozumie się osobę, 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,
7. **pracownik** – osoba współpracująca z Administratorem Danych na podstawie umowy o pracę lub umowy cywilnoprawnej,
8. **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 (ogólne rozporządzenie o ochronie danych),
9. **Ustawa** -Ustawa z dnia 10 maja 2018 r. o ochronie danych osobowych, tj. Dz. U. z 2019r. poz. 730
10. **państwo trzecie** – państwo nienależące do Europejskiego Obszaru Gospodarczego.

3. ZAKRES INFORMACJI OBJĘTYCH POLITYKĄ OCHRONY DANYCH OSOBOWYCH ORAZ ZAKRES ZASTOSOWANIA

Polityka ochrony danych osobowych opisuje zasady i procedury przetwarzania danych osobowych. Jest to zestaw praw, reguł i praktycznych doświadczeń dotyczących sposobu zarządzania, ochrony i dystrybucji danych osobowych wewnątrz Administratora Danych. Polityka odnosi się całościowo do problemu zabezpieczenia danych osobowych, tj. zarówno do zabezpieczenia danych przetwarzanych tradycyjnie, jak i danych przetwarzanych w systemach informatycznych.

Politykę ochrony danych osobowych stosuje się do wszelkich czynności, stanowiących w myśl RODO, przetwarzanie danych osobowych. Bez względu na źródło pochodzenia danych osobowych, ich zakres, cel zebrania, sposób przetwarzania lub czas przetwarzania, stosowane są zasady ujęte w Polityce.

Rygorowi Polityki podlegają także dane powierzone Administratorowi Danych do przetwarzania na podstawie umowy powierzenia przetwarzania danych osobowych lub innego instrumentu prawnego oraz dane osobowe, które zostały Administratorowi Danych udostępnione.

Urząd Gminy w Przytyku

ul. Zachęta 57, 26-650 Przytyk

**B. PODMIOTY ODPOWIEDZIALNE ZA OCHRONĘ DANYCH
OSOBOWYCH**

1. STRUKTURA ORGANIZACJI OCHRONY DANYCH OSOBOWYCH

Za przetwarzanie danych osobowych oraz ich ochronę zgodnie z postanowieniami RODO, Ustawy, Polityki oraz procedur wewnętrznych z zakresu ochrony danych osobowych wdrożonych w strukturze Administratora Danych, odpowiadają:

1. Administrator Danych,
2. Administrator Systemów Informatycznych,
3. Inspektor Ochrony Danych,
4. Osoby upoważnione do przetwarzania danych osobowych.

1.1 ADMINISTRATOR DANYCH

1. Administrator Danych wyznacza:
 - 1.1. IOD,
 - 1.2. Administratora Systemów Informatycznych.
2. Administrator Danych jest odpowiedzialny za:
 - 2.1. podjęcie odpowiednich środków organizacyjnych i technicznych w celu zapewnienia i wykazania przetwarzania danych osobowych zgodnie z określonymi w RODO zasadami przetwarzania danych osobowych,
 - 2.2. wdrożenie odpowiednich procedur ochrony danych osobowych,
 - 2.3. stosowanie zatwierdzonych kodeksów postępowania lub zatwierdzonych mechanizmów certyfikacji, jeżeli byłoby to niezbędne, jako element dla stwierdzenia przestrzegania przez Administratora Danych ciążących na nim obowiązków,
 - 2.4. zapewnienie realizacji praw osób, których dane dotyczą,
 - 2.5. prowadzenie rejestru czynności przetwarzania danych osobowych,
 - 2.6. prowadzenie rejestru kategorii przetwarzania dokonywanych w imieniu innego administratora,

POLITYKA OCHRONY DANYCH OSOBOWYCH

Urząd Gminy w Przytyku

ul. Zachęta 57, 26-650 Przytyk

- 2.7. współpracę z organem nadzorczym w ramach wykonywania przez niego swoich zadań,
- 2.8. wdrożenie odpowiednich środków organizacyjnych i technicznych, aby zapewnić stopień bezpieczeństwa odpowiadający istniejącemu ryzyku naruszenia praw lub wolności osób, których dane dotyczą,
- 2.9. zgłaszanie naruszenia ochrony danych osobowych właściwemu organowi nadzorczemu, a w przypadku, gdy znajdą ku temu odpowiednie przesłanki, również osobie, której dane dotyczą,
- 2.10. dokumentowanie wszelkich naruszeń ochrony danych osobowych, w tym okoliczności naruszenia, jego skutków oraz podjętych działań zaradczych,
- 2.11. dokonanie oceny skutków planowanych operacji przetwarzania dla ochrony danych osobowych w sytuacji, jeżeli dany rodzaj przetwarzania może powodować wysokie ryzyko naruszenia praw lub wolności osób fizycznych, w tym, jeżeli znajdą ku temu odpowiednie przesłanki, konsultację z organem nadzorczym,
- 2.12. nadawanie upoważnień do przetwarzania danych osobowych oraz prowadzenie ewidencji osób upoważnionych do przetwarzania danych osobowych,
- 2.13. zapewnienie legalności przekazywania danych osobowych do podmiotów trzecich,
- 2.14. w stosunku do IOD:
 - 2.14.1. zapewnienie, że jest on właściwie i niezwłocznie włączany we wszystkie sprawy dotyczące ochrony danych osobowych,
 - 2.14.2. wspieranie IOD w wypełnianiu przez niego zadań, zapewniając mu zasoby niezbędne do wykonania tych zadań oraz dostęp do danych osobowych i operacji przetwarzania, a także zasoby niezbędne do utrzymania jego wiedzy fachowej,
 - 2.14.3. zapewnienie by IOD nie otrzymywał instrukcji dotyczących wykonywania swoich zadań,
 - 2.14.4. publikację danych kontaktowych IOD oraz zawiadomienie o nich organu nadzorczego.
3. Administrator Danych nadzoruje działania IOD oraz ASI oraz wydaje im zalecenia, co do sposobu wykonywania obowiązków wynikających z Polityki.

Urząd Gminy w Przytyku

ul. Zachęta 57, 26-650 Przytyk

4. Administrator Danych każdorazowo wyraża zgodę oraz ostateczną akceptację na wszystkie działania IOD oraz ASI, w które zaangażowane są podmioty trzecie. Do zaakceptowania tych działań, wystarczająca jest zgoda wyrażona w formie wiadomości e-mail.

2.1 ADMINISTRATOR SYSTEMÓW INFORMATYCZNYCH

1. Funkcję ASI pełni osoba wyznaczona przez Administratora Danych.
2. Wzory dokumentów wyznaczenia oraz odwołania ASI znajdują się w Załączniku nr 6 do Polityki.
1. Do zadań ASI należy:
 - 1.1. nadawanie uprawnień do systemów informatycznych,
 - 1.2. prowadzenie rejestru nadanych uprawnień do systemów informatycznych,
 - 1.3. nadzór nad stosowaniem środków zapewniających bezpieczeństwo przetwarzania danych osobowych w systemach informatycznych, a w szczególności przeciwdziałających dostępowi osób niepowołanych do tych systemów,
 - 1.4. podejmowanie odpowiednich działań w przypadku wykrycia naruszeń w systemie zabezpieczeń,
 - 1.5. identyfikacja i analiza zagrożeń oraz ocena ryzyka, na które może być narażone przetwarzanie danych osobowych w systemach informatycznych,
 - 1.6. sprawowanie nadzoru nad kopiami zapasowymi;
 - 1.7. inicjowanie i nadzór nad wdrażaniem nowych narzędzi, procedur organizacyjnych oraz sposobów zarządzania systemami informatycznymi, które mają doprowadzić do wzmocnienia bezpieczeństwa przy przetwarzaniu danych osobowych,
 - 1.8. podejmowanie innych czynności w zakresie zabezpieczenia przetwarzania danych w systemach informatycznych,
 - 1.9. dokonywanie cyklicznych przeglądów aktualności i stosowania procedur z zakresu przetwarzania danych w systemach informatycznych, na podstawie opracowanego planu przeglądów.

ścisła współpraca z IOD w zakresie bezpieczeństwa i zasad przetwarzania danych osobowych w systemach informatycznych.

POLITYKA OCHRONY DANYCH OSOBOWYCH

Urząd Gminy w Przytyku

ul. Zachęta 57, 26-650 Przytyk

3.1 INSPEKTOR OCHRONY DANYCH

1. Funkcję IDO pełni osoba wyznaczona przez Administratora Danych.
2. Wzory dokumentów wyznaczenia oraz odwołania IOD znajdują się w Załączniku nr 5 do Polityki.
3. IOD jest wyznaczany przez Administratora Danych na podstawie kwalifikacji zawodowych, a w szczególności wiedzy fachowej na temat prawa i praktyk w dziedzinie ochrony danych oraz umiejętności wypełnienia swoich zadań.
4. Do zadań IOD należy:
 - 4.1. informowanie o obowiązkach wynikających z RODO oraz innych właściwych przepisów Unii lub państw członkowskich o ochronie danych osobowych oraz doradzanie w tym zakresie,
 - 4.2. monitorowanie przestrzegania RODO oraz innych właściwych przepisów Unii lub państw członkowskich o ochronie danych osobowych,
 - 4.3. monitorowanie przestrzegania wdrożonych procedur ochrony danych osobowych,
 - 4.4. doradztwo w zakresie podziału obowiązków (np. między współadministratorami, Administratorem Danych a podmiotem przetwarzającym lub pomiędzy pracownikami Administratora Danych),
 - 4.5. działania zwiększające świadomość pracowników Administratora Danych w zakresie obowiązków wynikających z RODO lub przyjętych procedur,
 - 4.6. szkolenia dla pracowników Administratora Danych uczestniczących w operacjach przetwarzania danych,
 - 4.7. przeprowadzanie audytów w zakresie przestrzegania RODO i wdrożonych procedur ochrony danych osobowych,
 - 4.8. udzielanie na żądanie zaleceń, co do oceny skutków dla ochrony danych osobowych oraz monitorowanie jej wykonania / koordynowanie procesu oceny skutków dla ochrony danych osobowych,
 - 4.9. współpraca z organem nadzorczym oraz pełnienie funkcji punktu kontaktowego dla organu nadzorczego w kwestiach związanych z przetwarzaniem danych,

Urząd Gminy w Przytyku

ul. Zachęta 57, 26-650 Przytyk

- 4.10. pełnienie funkcji punktu kontaktowego dla osób, których dane dotyczą, we wszystkich sprawach związanych z przetwarzaniem ich danych osobowych oraz z wykonywaniem praw przysługujących im na mocy RODO,
- 4.11. opracowywanie i aktualizacja Polityki,
- 4.12. administrowanie oraz kontrola upoważnień do przetwarzania danych osobowych,
- 4.13. udział w procesach związanych z naruszeniami ochrony danych osobowych, tj.:
 - 4.13.1. prowadzenie rejestru naruszeń,
 - 4.13.2. koordynowanie postępowania w sytuacji wykrycia naruszenia (dokumentacja naruszenia, postępowania naprawcze),
 - 4.13.3. koordynowanie zgłoszenia naruszenia organowi nadzorczemu oraz osobom, których dane dotyczą,
- 4.14. opracowywanie unikalnych treści klauzul informacyjnych, klauzul zgód na przetwarzanie danych osobowych, umów powierzenia przetwarzania danych osobowych oraz innych klauzul / postanowień związanych z przetwarzaniem danych osobowych (np. postanowień w zakresie współadministrowania),
- 4.15. prowadzenie rejestru czynności przetwarzania danych osobowych,
- 4.16. prowadzenie rejestru kategorii czynności przetwarzania dokonywanych w imieniu innego administratora,
- 4.17. udział w procesie realizacji praw osób, których dane dotyczą (tj. udzielanie odpowiedzi na zapytania, prowadzenie korespondencji, spotkania z osobami realizującymi swoje prawa),
- 4.18. reagowanie na skargi osób, których dane dotyczą (tj. korespondencja z organem nadzorczym, korespondencja ze skarżącym),
- 4.19. udział w postępowaniach administracyjnych oraz sądowych prowadzonych w związku ze skargami osób, których dane dotyczą,
- 4.20. udział w procesach certyfikacji oraz przystępowania do funkcjonujących kodeksów postępowania,
- 4.21. kontrola podmiotów przetwarzających.

Urząd Gminy w Przytyku

ul. Zachęta 57, 26-650 Przytyk

4.1 OSOBY UPOWAŻNIONE DO PRZETWARZANIA DANYCH OSOBOWYCH

1. Każda osoba, która uzyskała upoważnienie do przetwarzania danych, zobowiązana jest do ich ochrony w sposób zgodny z przepisami RODO, Ustawy oraz postanowieniami Polityki.
2. Osoba upoważniona zobowiązana jest do zachowania w tajemnicy danych osobowych oraz sposobów ich zabezpieczenia. Obowiązek ten istnieje także po ustaniu zatrudnienia. Stosowny zapis o przyjęciu zobowiązania do zachowania w tajemnicy przetwarzanych danych osobowych zawiera upoważnienie, którego wzór znajduje się w Załączniku nr 3 do Polityki.
3. Naruszenie obowiązku ochrony danych osobowych, a w szczególności obowiązku zachowania danych osobowych w tajemnicy skutkuje poniesieniem odpowiedzialności karnej na podstawie przepisów Ustawy oraz stanowi ciężkie naruszenie obowiązków pracowniczych i może być podstawą rozwiązania stosunku pracy w trybie art. 52 Ustawy z dnia 26 czerwca 1974 r. Kodeks Pracy (t.j. Dz. U. z 2019 r. poz. 1495) .bądź rozwiązania stosunku cywilnoprawnego.

Urząd Gminy w Przytyku

ul. Zachęta 57, 26-650 Przytyk

C. ZASADY PRZETWARZANIA DANYCH OSOBOWYCH

1. OGÓLNE ZASADY PRZETWARZANIA DANYCH OSOBOWYCH

1. Przetwarzanie danych osobowych w strukturze Administratora Danych odbywa się zgodnie z ogólnymi zasadami przetwarzania danych osobowych określonymi w art. 5 RODO. Oznacza to, że dane osobowe przetwarza się:
 - 1.1 zgodnie z prawem, w oparciu o co najmniej jedną przesłankę legalności przetwarzania danych osobowych wskazaną w art. 6 lub 9 RODO (*zasada legalności*),
 - 1.2 w sposób przejrzysty dla osób, których dane dotyczą (*zasada przejrzystości*),
 - 1.3 w sposób rzetelny przy uwzględnieniu interesów i rozsądnych oczekiwań osób, których dane dotyczą (*zasada rzetelności*),
 - 1.4 w konkretnych, wyraźnych i prawnie uzasadnionych celach (*zasada ograniczenia celu*),
 - 1.5 przy uwzględnieniu ich prawidłowości i ewentualnego uaktualniania (*zasada prawidłowości*),
 - 1.6 przez okres nie dłuższy, niż jest to niezbędne dla celów, w których są przetwarzane (*zasada ograniczenia przechowywania*),
 - 1.7 w zakresie adekwatnym, stosownym oraz niezbędnym dla celów, w których są przetwarzane (*zasada minimalizacji danych*),
 - 1.8 w sposób zapewniający odpowiednie bezpieczeństwo (*integralność i poufność*).
2. Administrator Danych gwarantuje, że określone decyzje odnoszące się do procesów przetwarzania danych osobowych zostały przeanalizowane z punktu widzenia zgodności z ogólnymi zasadami przetwarzania danych, a przede wszystkim, że są z nimi zgodne.

2. ZAKRES PRZETWARZANYCH DANYCH OSOBOWYCH

1. Polityka ma zastosowanie w stosunku do wszystkich danych osobowych przetwarzanych przez Administratora Danych, niezależnie od formy ich przetwarzania (elektroniczna lub papierowa) oraz tego, czy są to dane przetwarzane w zbiorach danych, w zestawach czy stanowią one pojedyncze informacje osobowe.

Urząd Gminy w Przytyku
ul. Zachęta 57, 26-650 Przytyk

2. Wykaz budynków, pomieszczeń lub części pomieszczeń, tworzących obszar, w którym przetwarzane są dane osobowe stanowi Załącznik nr 1 do Polityki.
3. Administrator Danych prowadzi:
 - 3.1. rejestr czynności przetwarzania danych osobowych, których jest administratorem,
 - 3.2. rejestr kategorii czynności przetwarzania dokonywanych w imieniu administratorów, którzy powierzyli mu przetwarzanie danych.
4. Rejestr, o którym mowa w pkt 3.1. zawiera co najmniej następujące informacje:
 - 4.1. nazwę oraz dane kontaktowe Administratora Danych oraz wszelkich współadministratorów,
 - 4.2. gdy ma to zastosowanie imię, nazwisko lub nazwę oraz dane kontaktowe swojego przedstawiciela,
 - 4.3. imię i nazwisko oraz dane kontaktowe IOD,
 - 4.4. cele przetwarzania,
 - 4.5. opis kategorii osób, których dane dotyczą,
 - 4.6. opis kategorii danych osobowych,
 - 4.7. kategorie odbiorców, którym dane osobowe zostały lub zostaną ujawnione, w tym odbiorców w państwach trzecich lub w organizacjach międzynarodowych,
 - 4.8. gdy ma to zastosowanie, przekazania danych osobowych do państwa trzeciego lub organizacji międzynarodowej, w tym nazwa tego państwa trzeciego lub organizacji międzynarodowej, a w przypadku przekazania, o których mowa w art. 49 ust. 1 akapit drugi RODO, dokumentacja odpowiednich zabezpieczeń,
 - 4.9. jeżeli jest to możliwe, planowane terminy usunięcia poszczególnych kategorii danych,
 - 4.10. ogólny opis technicznych i organizacyjnych środków bezpieczeństwa.
5. Rejestr, o którym mowa w pkt 3.2. zawiera co najmniej następujące informacje:
 - 5.1. nazwę oraz dane kontaktowe Administratora Danych,
 - 5.2. imię i nazwisko lub nazwę oraz dane kontaktowe każdego administratora, w imieniu którego działa Administrator Danych,

POLITYKA OCHRONY DANYCH OSOBOWYCH

Urząd Gminy w Przytyku

ul. Zachęta 57, 26-650 Przytyk

- 5.3. gdy ma to zastosowanie, imię, nazwisko lub nazwę oraz dane kontaktowe przedstawiciela każdego administratora, w imieniu którego działa Administrator Danych,
 - 5.4. gdy ma to zastosowanie, imię i nazwisko oraz dane kontaktowe IOD każdego administratora, w imieniu którego działa Administrator Danych,
 - 5.5. kategorie przetwarzania dokonywanych w imieniu każdego z administratorów,
 - 5.6. gdy ma to zastosowanie, przekazania danych osobowych do państwa trzeciego lub organizacji międzynarodowej, w tym nazwa tego państwa trzeciego lub organizacji międzynarodowej, a w przypadku przekazania, o których mowa w art. 49 ust. 1 akapit drugi RODO, dokumentacja odpowiednich zabezpieczeń,
 - 5.7. ogólny opis technicznych i organizacyjnych środków bezpieczeństwa.
6. Administrator Danych prowadzi rejestry, o których mowa w pkt 3 w formie papierowej.
 7. W przypadku zgłoszenia przez organ nadzoru żądania w tym zakresie, Administrator Danych udostępnia mu prowadzone przez siebie rejestry.

3. DOPUSZCZENIE OSÓB DO PRZETWARZANIA DANYCH OSOBOWYCH

1. Administrator Danych realizując Politykę, w zakresie udostępniania danych osobowych w ramach własnej (wewnętrznej) struktury, zezwala na ich przetwarzanie w systemie informatycznym lub w wersji papierowej wyłącznie osobom, które uzyskały uprzednie, stosowne upoważnienie do przetwarzania danych osobowych.
2. Upoważnienie do przetwarzania danych osobowych nadawane jest po przeprowadzeniu szkolenia lub zaznajomieniu w innej formie, osoby upoważnianej z zasadami ochrony danych osobowych obowiązującymi w strukturze Administratora Danych.
3. Upoważnienie do przetwarzania danych osobowych, nadawane jest indywidualnie, z wyraźnym wskazaniem, jakie zbiory danych obejmuje swoim zakresem.
4. Administrator Danych prowadzi ewidencję osób upoważnionych do przetwarzania danych osobowych, której wzór stanowi Załącznik nr 4 do Polityki.
5. Szczegółowa Procedura nadawania upoważnień do przetwarzania danych osobowych stanowi Załącznik nr 3 do Polityki.

4. POWIERZENIE PRZETWARZANIA DANYCH OSOBOWYCH

Urząd Gminy w Przytyku

ul. Zachęta 57, 26-650 Przytyk

1. Administrator Danych realizując Politykę dopuszcza, by dane osobowe, których jest administratorem były przetwarzane poza własnymi strukturami organizacyjnymi. Może się to odbywać wyłącznie na drodze powierzenia danych, w określonym celu i zakresie, podmiotowi przetwarzającemu na mocy umowy powierzenia przetwarzania danych osobowych lub innego instrumentu prawnego.
2. Podstawowym warunkiem dopuszczalności powierzenia przetwarzania danych w imieniu administratora jest poddanie planowanego outsourcingu analizie, która powinna zapewnić, że wybór podmiotu przetwarzającego został uzależniony od zapewnienia wystarczających gwarancji ochrony danych.
3. Zawierana przez Administratora Danych umowa powierzenia przetwarzania danych osobowych musi być zgodna z postanowieniami art. 28 RODO, tj. w szczególności określać:
 - 3.1. przedmiot powierzenia,
 - 3.2. czas trwania powierzenia,
 - 3.3. charakter i cel przetwarzania,
 - 3.4. rodzaj powierzanych danych osobowych,
 - 3.5. kategorie osób, których dane dotyczą,
 - 3.6. warunki podpowierzenia przetwarzania danych
 - 3.7. obowiązki i prawa Administratora Danych,
 - 3.8. obowiązki podmiotu przetwarzającego.
4. Umowa powierzenia może zostać zawarta w formie pisemnej lub papierowej.
5. W przypadku, gdy elementy powierzenia przetwarzania danych wskazane w pkt 3 znajdują się już w zawartej z danym podmiotem umowie, nie ma konieczności sporządzania dodatkowej umowy powierzenia przetwarzania danych osobowych.
6. Za zawieranie umów powierzenia przetwarzania danych osobowych odpowiada ADO
7. ADO przed planowanym rozpoczęciem współpracy z podmiotem przetwarzającym, jest zobowiązany poinformować o tym IOD oraz skonsultować z nim postanowienia zawieranej umowy w zakresie powierzenia przetwarzania danych osobowych. Powierzenie przetwarzania danych może odbyć się wyłącznie na podstawie postanowień zaakceptowanych przez IOD.

Urząd Gminy w Przytyku
ul. Zachęta 57, 26-650 Przytyk

8. Umowa powierzenia przetwarzania danych osobowych podpisywana jest zgodnie z zasadami reprezentacji Administratora Danych lub udzielonymi pełnomocnictwami.
9. Każdorazowe dokonanie powierzenia danych osobowych musi zostać obligatoryjnie odnotowane w rejestrze czynności przetwarzania danych osobowych.
10. Administrator Danych w zakresie prowadzonej przez siebie działalności może przetwarzać również dane osobowe powierzone przez podmioty, na rzecz których świadczy usługi. Przyjęcie danych w powierzenie przez Administratora Danych musi zostać obligatoryjnie odnotowane w rejestrze kategorii czynności przetwarzania danych osobowych.

5. UDOSTĘPNIANIE DANYCH OSOBOWYCH

1. Administrator Danych realizując Politykę dopuszcza, by dane osobowe, których jest administratorem były przekazywane innym administratorom w formie udostępnienia danych.
2. Udostępnienie danych osobowych może nastąpić tylko w oparciu o co najmniej jedną przesłankę spośród wskazanych w art. 6 RODO i / lub art. 9 RODO.
3. Podmioty lub kategorie podmiotów, którym udostępnia się dane osobowe muszą zostać obligatoryjnie wskazane w rejestrze czynności przetwarzania danych osobowych.

6. PRZEKAZYWANIE DANYCH OSOBOWYCH DO PAŃSTW TRZECICH

1. Przekazywanie danych, których administratorem jest Administrator Danych do państw trzecich i organizacji międzynarodowych, może się odbywać wyłącznie po spełnieniu warunków przewidzianych w Rozdziale V RODO.
2. Przekazywanie danych do państw trzecich może mieć formę zarówno powierzenia przetwarzania danych osobowych oraz udostępnienia danych osobowych, co oznacza, że w zależności od rodzaju przekazania, należy wziąć również pod uwagę postanowienia podrozdziałów 4 i 5 Polityki.
3. Przekazanie danych osobowych, których administratorem jest Administrator Danych do państwa trzeciego może nastąpić w sytuacji, jeżeli Komisja Europejska wydała decyzję, że dane państwo trzecie, terytorium lub określony sektor lub określone sektory w tym państwie trzecim lub dana organizacja międzynarodowa zapewniają odpowiedni stopień ochrony. Takie przekazanie nie wymaga specjalnego zezwolenia.

Urząd Gminy w Przytyku

ul. Zachęta 57, 26-650 Przytyk

4. W przypadkach braku decyzji Komisji Europejskiej, o której mowa w pkt 3, dokonanie transferu danych do państwa trzeciego jest możliwe, gdy Administrator Danych samodzielnie zapewni odpowiednie zabezpieczenia i pod warunkiem, że będą obowiązywały egzekwowalne prawa osób, których dane dotyczą i skuteczne środki ochrony prawnej za pomocą:
 - 4.1. wiążących reguł korporacyjnych (*Binding Corporate Rules*) zatwierdzonych przez organ nadzorczy, mających zastosowanie do każdego z członków grupy przedsiębiorstw lub grupy przedsiębiorców prowadzących wspólną działalność gospodarczą,
 - 4.2. standardowych klauzul ochrony danych (*Standard Contractual Clauses*) przyjętych lub zatwierdzonych przez Komisję Europejską,
 - 4.3. zatwierdzonego kodeksu postępowania lub
 - 4.4. zatwierdzonego mechanizmu certyfikacji.
5. W szczególnych przypadkach, dopuszcza się przekazanie danych osobowych przez Administratora Danych do państwa trzeciego pomimo braku decyzji Komisji Europejskiej, o której mowa w pkt 3 oraz zapewnienia odpowiednich zabezpieczeń, o których mowa w pkt 4. Do tych szczególnych przypadków zalicza się przekazanie danych pod warunkiem, że:
 - 5.1. osoba, której dane dotyczą, poinformowana jest o ewentualnym ryzyku, z którymi może się dla niej wiązać proponowane przekazanie, wyrazi na nie wyraźną zgodę,
 - 5.2. przekazanie jest niezbędne do wykonania umowy zawartej z osobą, której dane dotyczą,
 - 5.3. przekazanie jest niezbędne do zawarcia lub wykonania umowy zawartej w interesie osoby, której dane dotyczą,
 - 5.4. przekazanie jest niezbędne ze względu na ważne względy interesu publicznego,
 - 5.5. przekazanie jest niezbędne ze względu na posiadane roszczenia,
 - 5.6. przekazanie jest niezbędne do ochrony żywotnych interesów osoby, których dane dotyczą lub
 - 5.7. przekazanie nastąpi z publicznego rejestru.
6. ADO przed planowanym przekazaniem danych do państwa trzeciego, jest zobowiązany poinformować o tym IOD oraz skonsultować z nim warunki przekazania tych danych. Przekazanie danych może odbyć się wyłącznie na podstawie warunków i postanowień zaakceptowanych przez IOD.

Urząd Gminy w Przytyku

ul. Zachęta 57, 26-650 Przytyk

7. WSPÓŁADMINISTROWANIE DANYMI OSOBOWYMI

1. Administrator Danych w zakresie przetwarzanych przez siebie danych osobowych dopuszcza możliwość przyjęcia modelu współadministrowania danymi osobowymi zgodnie z art. 26 RODO.
2. Współadministrowanie danymi może zachodzić wówczas, jeżeli Administrator Danych oraz co najmniej jeden inny podmiot, wspólnie ustalają cele i sposoby przetwarzania danych osobowych. Oznacza to, że w danym procesie przetwarzania danych osobowych muszą zostać spełnione równocześnie trzy warunki, tj. Administrator Danych oraz co najmniej jeden inny podmiot muszą:
 - 2.1. być administratorami w rozumieniu art. 4 pkt 7 RODO,
 - 2.2. muszą wspólnie ustalić cele przetwarzania danych,
 - 2.3. muszą wspólnie ustalić sposoby (techniczne i organizacyjne) przetwarzania danych osobowych.
3. W przypadku spełnienia warunków, o których mowa w pkt 2 Administrator Danych oraz co najmniej jeden inny podmiot stają się współadministratorami danych w zakresie danego procesu przetwarzania danych osobowych.
4. W przypadku przyjęcia modelu współadministrowania danymi, współadministratorzy danych w drodze wspólnych uzgodnień, w przejrzysty sposób określają odpowiednie zakresy swojej odpowiedzialności dotyczącej wypełniania obowiązków wynikających z RODO.
5. W sytuacji, kiedy w zakresie zachodzących w strukturze Administratora Danych procesów przetwarzania danych osobowych pojawią się procesy wobec których istnieje prawdopodobieństwo zachodzenia współadministrowania danymi, ADO informuje o tym fakcie IOD.
6. IOD dokonuje oceny, czy dany proces przetwarzania spełnia warunki współadministrowania danymi.
7. W przypadku, kiedy wynik oceny, o której mowa w pkt 6 wskazuje na współadministrowanie danymi osobowymi, IOD, przy współudziale pozostałych współadministratorów, opracowuje wspólne uzgodnienia, o których mowa w pkt 4.

8. AUDYTY ZGODNOŚCI PRZETWARZANIA DANYCH OSOBOWYCH

Urząd Gminy w Przytyku

ul. Zachęta 57, 26-650 Przytyk

1. Audyty zgodności przetwarzania danych osobowych z przepisami o ochronie danych osobowych oraz procedurami wdrożonymi w strukturze Administratora Danych przeprowadzane są przez IOD.
2. IOD przeprowadza audyt według opracowanego planu audytów.
2. IOD przygotowuje plan audytów na okres nie krótszy niż kwartał i nie dłuższy niż rok z zaznaczeniem, że plan musi obejmować co najmniej jeden audyt.
3. Plan audytów IOD przygotowuje w formie papierowej bądź elektronicznej i przedstawia Administratorowi Danych nie później niż na dwa tygodnie przed dniem rozpoczęcia okresu objętego planem.
4. W planie audytów IOD uwzględnia, w szczególności:
 - 4.1. przedmiot, zakres oraz termin przeprowadzenia poszczególnych audytów oraz sposób i zakres ich dokumentowania,
 - 4.2. procesy przetwarzania danych osobowych objęte audytem,
 - 4.3. konieczność weryfikacji zgodności przetwarzania danych osobowych z:
 - 4.3.1. zasadami przetwarzania danych osobowych,
 - 4.3.2. zasadami dotyczącymi zabezpieczenia danych osobowych,
 - 4.3.3. zasadami przekazywania danych osobowych.
5. W toku audytu IOD dokonuje i dokumentuje czynności, w zakresie niezbędnym do oceny zgodności przetwarzania danych osobowych z przepisami o ochronie danych osobowych oraz do opracowania sprawozdania.
6. Po zakończeniu audytu, IOD przygotowuje dla Administratora Danych, sprawozdanie w tym zakresie. Sprawozdanie sporządzane jest w postaci elektronicznej albo w postaci papierowej.
7. IOD przekazuje Administratorowi Danych sprawozdanie nie później niż w terminie 30 dni od zakończenia audytu.

9. REALIZACJA PRAW OSÓB, KTÓRYCH DANE DOTYCZĄ

Urząd Gminy w Przytyku
ul. Zachęta 57, 26-650 Przytyk

3. Administrator Danych uwzględnia w zachodzących w jego strukturze procesach przetwarzania danych osobowych, procedury i zasady ułatwiające osobie, której dane dotyczą, wykonywanie praw przysługujących jej na mocy przepisów RODO, w tym, w szczególności:

- 1.1. prawo do wycofania wyrażonej zgody (art. 7 ust. 3 RODO),
- 1.2. prawo dostępu przysługujące osobie, której dane dotyczą (art. 15 RODO),
- 1.3. prawo do sprostowania danych (art. 16 RODO),
- 1.4. prawo do usunięcia danych (*prawo do bycia zapomnianym*) (art. 17 RODO);,
- 1.5. prawo do ograniczenia przetwarzania (art. 18 RODO),
- 1.6. prawo do przenoszenia danych (art. 20 RODO),
- 1.7. prawo sprzeciwu (art. 21 RODO),
- 1.8. prawo do niepodlegania decyzjom opartym na zautomatyzowanym przetwarzaniu (art. 22 RODO).

**10. OCHRONA DANYCH OSOBOWYCH W FAZIE PROJEKTOWANIA ORAZ
DOMYŚLNA OCHRONA DANYCH OSOBOWYCH**

1. Administrator Danych wdraża odpowiednie środki techniczne i organizacyjne, zaprojektowane w celu skutecznej realizacji zasad ochrony danych, nadania przetwarzaniu danych niezbędnych zabezpieczeń oraz zapewnieniu ochrony praw osób, których dane dotyczą.
2. Wdrażając odpowiednie środki techniczne i organizacyjne Administrator Danych uwzględnia:
 - 2.1. stan wiedzy technicznej,
 - 2.2. koszt wdrażania,
 - 2.3. charakter, zakres, kontekst i cele przetwarzania danych,
 - 2.4. ryzyko naruszenia praw lub wolności osób fizycznych o różnym prawdopodobieństwie wystąpienia i wadze zagrożenia wynikające z przetwarzania.
3. Administrator Danych wdraża takie środki techniczne i organizacyjne, aby domyślnie przetwarzane były wyłącznie te dane osobowe, które są niezbędne dla osiągnięcia określonego celu przetwarzania, biorąc pod uwagę: ilość zbieranych danych osobowych, ich zakres, okres ich przechowywania oraz ich dostępność dla innych osób.

POLITYKA OCHRONY DANYCH OSOBOWYCH

Urząd Gminy w Przytyku

ul. Zachęta 57, 26-650 Przytyk

4. W szczególności stosowane środki techniczne i organizacje muszą zapewnić, by domyślnie dane osobowe nie były udostępniane nieokreślonej liczbie osób.
5. W pierwszej kolejności, Administrator Danych rozważa, czy cel jakiemu ma służyć projektowane rozwiązanie jest możliwy do osiągnięcia bez konieczności przetwarzania danych osobowych. Jeśli tak, należy wybrać takie rozwiązanie.
6. Administrator Danych zapewnia, aby spełnienie warunków wskazanych w pkt 1-5 (tzw. zasady *privacy by design* i *privacy by default*) było odpowiednio udokumentowane np. w formie notatki, maila, raportu z przeprowadzonych testów systemu informatycznego, wydruku z ekranu systemu.

11. OCENA SKUTKÓW DLA OCHRONY DANYCH OSOBOWYCH (PRIVACY IMPACT ASSESSMENT)

1. Administrator Danych dokonuje oceny skutków dla ochrony danych w celu opisanego przetwarzania danych osobowych oraz oceny jego konieczności i proporcjonalności, a także w celu wspomagania zarządzania ryzykiem naruszenia praw i wolności osób fizycznych wynikającym z przetwarzania ich danych osobowych.
2. W strukturze Administratora Danych ocena skutków dla ochrony danych osobowych stanowi narzędzie rozliczalności ułatwiające przestrzeganie wymogów określonych w RODO, a także wykazanie, że podjęto odpowiednie środki w celu zapewnienia przestrzegania przepisów RODO.

12. INCYDENTY OCHRONY DANYCH OSOBOWYCH

1. Osobami odpowiedzialnymi za bezpieczeństwo danych osobowych, w tym w szczególności za przeciwdziałanie dostępowi osób niepowołanych do pomieszczeń oraz systemów, w których przetwarzane są dane osobowe oraz za podejmowanie odpowiednich działań w przypadku wykrycia incydentów ochrony danych osobowych, jest: Administrator Danych, IOD oraz ASI (w odniesieniu do danych przetwarzanych w systemach informatycznych).

13. OGÓLNE ZASADY BEZPIECZEŃSTWA OCHRONY DANYCH OSOBOWYCH

Urząd Gminy w Przytyku
ul. Zachęta 57, 26-650 Przytyk

1. Dostęp do danych osobowych mogą mieć tylko pracownicy posiadający upoważnienie do ich przetwarzania.
2. Przebywanie osób nieuprawnionych do przetwarzania danych w pomieszczeniu, w którym przetwarzane są dane osobowe jest dopuszczalne tylko w obecności osoby upoważnionej do ich przetwarzania, chyba, że dane te są w odpowiedni sposób zabezpieczone przed dostępem.
3. Pracownicy mający dostęp do danych osobowych nie mogą ich ujawniać zarówno w miejscu pracy, jak i poza nim, w sposób wykraczający poza czynności związane z ich przetwarzaniem, w zakresie obowiązków służbowych, w ramach udzielonego upoważnienia do przetwarzania danych.
4. Pracownicy przechowujący dane osobowe zobowiązani są do zabezpieczenia materiałów zawierających dane w sposób uniemożliwiający dostęp do nich osobom nieuprawnionym.
5. Niedopuszczalnym jest wynoszenie materiałów zawierających dane osobowe poza obszar ich przetwarzania bez związku z wykonywaniem czynności służbowych. Za bezpieczeństwo i zwrot materiałów zawierających dane osobowe odpowiada w tym przypadku osoba dokonująca ich wyniesienia oraz jej bezpośredni przełożony.
6. Nikomu nie należy udostępniać indywidualnych haseł i identyfikatorów do systemów informatycznych.
7. Wysyłanie seryjnych wiadomości e-mail wymaga zastosowania opcji *kopia ukryta*.
8. Nie można udzielać informacji dotyczących danych osobowych innym podmiotom na podstawie prośby o takie dane skierowanej w formie zapytania telefonicznego.
9. W miejscu przetwarzania danych osobowych utrwalonych w formie papierowej pracownicy zobowiązani są do stosowania zasady tzw. *czystego biurka*, która oznacza nie pozostawianie materiałów zawierających dane osobowe w miejscu umożliwiającym fizyczny dostęp do nich osobom nieuprawnionym. Za realizację powyższej zasady odpowiedzialny jest na swym stanowisku każdy z pracowników. Nie należy pozostawiać danych osobowych w miejscach ogólnodostępnych takich jak np. biurka, blaty, parapety.
10. Niszczenie brudnopisów, błędnych lub zbędnych kopii materiałów zawierających dane osobowe odbywać się musi w sposób uniemożliwiający odczytanie zawartej w nich treści, np. z wykorzystaniem niszczarek.
11. Za bezpieczeństwo przetwarzania danych osobowych w określonym zbiorze indywidualną odpowiedzialność ponosi przede wszystkim każdy pracownik mający dostęp do danych.

POLITYKA OCHRONY DANYCH OSOBOWYCH

Urząd Gminy w Przytyku

ul. Zachęta 57, 26-650 Przytyk

12. W czasie chwilowej nieobecności pracowników w pomieszczeniach, w godzinach pracy jak i po zakończeniu pracy, są oni zobowiązani do zamykania na klucz pomieszczeń lub budynków wchodzących w skład obszarów, w których przetwarzane są dane osobowe.
13. Klucze do pomieszczeń, w których przetwarzane są dane osobowe nie mogą być pozostawione w zamku w drzwiach. Pracownicy zobowiązani są do dołożenia należytej staranności w celu zabezpieczenia kluczy przed udostępnieniem ich osobom nieupoważnionym.
14. Przed wyjściem z pomieszczenia, w którym przechowywane są dane osobowe należy upewnić się, że zostało ono odpowiednio zabezpieczone (zamknięte okna, drzwi).
15. Po zakończeniu pracy w systemie informatycznym, w którym przechowywane są dane osobowe, należy wylogować się z systemu.
16. Osoba użytkująca komputer przenośny zawierający dane osobowe zobowiązana jest do zachowania szczególnej ostrożności podczas jego transportu, przechowywania i użytkowania poza obszarem, w którym przetwarzane są dane osobowe.
17. Na pracowniku pracującym zdalnie spoczywa obowiązek odpowiedniego zabezpieczenia danych tak, aby osoby trzecie nie miały dostępu do danych osobowych.
18. Dane osobowe przesyłane elektronicznie powinny być zabezpieczone hasłem. Hasło to powinno być wysyłane oddzielnym kanałem telekomunikacyjnym.

14. PRZEGLĄDY I AKTUALIZACJA POLITYKI OCHRONY DANYCH OSOBOWYCH

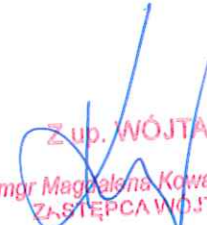
1. Polityka podlega okresowemu przeglądowi pod kątem jej adekwatności, nie rzadziej niż raz do roku.
2. Przeglądu Polityki dokonuje IOD. Dokonanie przeglądu Polityki może nastąpić, w szczególności w ramach przeprowadzanego przez IOD audytu zgodności przetwarzania danych osobowych.
3. Przegląd powinien obejmować, w szczególności ocenę adekwatności Polityki do:
 - 3.1. procesów funkcjonujących w strukturach Administratora Danych,
 - 3.2. obowiązujących przepisów prawa odnoszących się do ochrony danych osobowych, którym podlega Administrator Danych.

Urząd Gminy w Przytyku
ul. Zachęta 57, 26-650 Przytyk

4. W każdym przypadku, gdy zmianie ulegają przepisy prawa będące źródłem wskazanych w Polityce obowiązków lub zaistnieją istotne zmiany faktyczne w ramach struktury Administratora Danych przegląd Polityki wykonywany jest niezwłocznie.
5. Jeżeli w wyniku przeglądu Polityki stwierdzona zostanie konieczność aktualizacji jej zapisów, IOD dokonuje aktualizacji Polityki w wymaganym zakresie.

15. PROCEDURA SZKOLEŃ W ZAKRESIE UDZIELANIA UPOWAŻNIEŃ DO PRZETWARZANIA DANYCH OSOBOWYCH

1. IOD przed nadaniem pracownikowi upoważnienia, organizuje dla niego krótkie szkolenie, podczas którego informuje go o podstawowych aspektach prawnych związanych z ochroną danych osobowych (najważniejsze definicje, odpowiedzialność prawna, obowiązek właściwego zabezpieczenia danych przetwarzanych w formie papierowej oraz w systemach informatycznych).
2. Szkolenie jest przeprowadzone w formie tradycyjnej w siedzibie Administratora Danych lub miejscu przez niego wskazanym.
3. W przypadku szkolenia w formie tradycyjnej:
 - 3.1. IOD na podstawie otrzymanego wniosku sporządza listę osób uczestniczących w szkoleniu tradycyjnym,
 - 3.2. IOD przeprowadza szkolenie w siedzibie Administratora Danych lub miejscu wskazanym przez Administratora Danych,
 - 3.3. IOD odbiera od osób uczestniczących w szkoleniu podpisy poświadczające ich obecność na szkoleniu.
4. Osobie, która ukończyła szkolenie nadawane jest upoważnienie do przetwarzania danych osobowych.


Z up. WÓJTA
mgr Magdalena Kowalczyk
ZASTĘPCA WÓJTY

POLITYKA OCHRONY DANYCH OSOBOWYCH

Urząd Gminy w Przytyku
ul. Zachęta 57, 26-650 Przytyk

D. ZAŁĄCZNIKI

Załącznik nr 1	Wykaz procesów przetwarzania danych osobowych wraz osobami zarządzającymi procesami przetwarzania danych
Załącznik nr 2	Zasady retencji danych osobowych
Załącznik nr 3	Upoważnienia do przetwarzania danych osobowych
Załącznik nr 4	Wzór ewidencji osób upoważnionych do przetwarzania danych osobowych
Załącznik nr 5	Wzory wyznaczenia oraz odwołania Inspektora Ochrony Danych
Załącznik nr 6	Wzory wyznaczenia oraz odwołania Administratora Systemów Informatycznych
Załącznik nr 7	Oświadczenie pracownika o zapoznaniu się z dokumentacją
Załącznik nr 8	Rejestr kategorii czynności przetwarzania podmiotu przetwarzającego
Załącznik nr 9	Rejestr czynności przetwarzania administratora

Częścią integralną Polityki ochrony danych osobowych są:

- 1. Procedury do Polityki ochrony danych osobowych**
- 2. Instrukcja Zarządzania Systemem Informatycznym służącym do przetwarzania danych osobowych wraz z procedurami dotyczącymi cyberbezpieczeństwa i bezpieczeństwa informacji**

Data: 01/06/2020 r. Aktualizacja 09/06/2021 r. Miejsce: Radom	Pełen podpis Administratora Danych:	Pieczęć
	Urząd Gminy w Przytyku . Zachęta 57, 26-650 Przytyk	

**ZAŁĄCZNIK NR 1 WYKAZ PROCESÓW PRZETWARZANIA DANYCH
OSOBOWYCH WRAZ Z OSOBAMI ZARZĄDZAJĄCYMI PROCESAMI
PRZETWARZANIA DANYCH**

Lp.	Proces przetwarzania danych osobowych	Osoba zarządzająca procesami przetwarzania danych osobowych (imię, nazwisko, stanowisko, dane kontaktowe)
1.	Prowadzenie akt osobowych	
2.	Wypłata wynagrodzeń	
3.	Prowadzenie dokumentacji BHP	
4.	Rekrutacja kandydatów do pracy	
5.	Rejestr podatków i opłat lokalnych	
6.	Kontokwincje zobowiązania pieniężnego - rejestr podatników i dłużników gminy	
7.	Rejestr opłat za zagospodarowanie odpadów komunalnych	
8.	Ewidencja skarg i wniosków oraz petycji	
9.	Rejestr cudzoziemców	
10.	Rejestr wydawanych decyzji o warunkach zabudowy i zagospodarowania terenu	

Urząd Gminy w Przytyku
ul. Zachęta 57, 26-650 Przytyk

11.	Ewidencja działalności gospodarczej	
12.	Rejestr wyborców i rejestr pełnomocnictw	
13.	Urząd Stanu Cywilnego	
14.	Rejestr dowodów osobistych	
15.	Oświadczenia o stanie majątkowym osób sprawujących funkcje publiczne	
16.	Rejestr Płatników od środków transportowych	
17.	Rejestr aktów własności ziemi	
18.	System Informacji Oświatowej	
19.	Wykonywanie orzeczeń sądowych w zakresie nieodpłatnej pracy na cele społeczne	
20.	Spełnienie obowiązku nauki	
21.	Wykaz decyzji zezwalających na usuwanie drzew i krzewów	
22.	Numeracja porządkowa nieruchomości	
23.	Świadczenia osobiste i rzeczowe	
24.	Regulowanie własności działek o nieuregulowanym stanie prawnym	
25.	Decyzje w sprawie zmiany nazwisk i imion	

Urząd Gminy w Przytyku
ul. Zachęta 57, 26-650 Przytyk

26.	Podziały, rozgraniczenia oraz wznowienie granic na nieruchomościach	
27.	Kandydaci na ławników	
28.	Zbiór informacji o rodzaju i miejscach występowania azbestu lub wyrobów zawierających azbest	
29.	Decyzje o środowiskowych uwarunkowaniach zgody na realizację przedsięwzięcia	
30.	Ewidencja bezodpływowych zbiorników na nieczystości ciekłe	
31.	Rejestr zezwoleń na sprzedaż napojów alkoholowych	
32.	Ewidencja najemców lokali komunalnych	
33.	Ewidencja decyzji dotyczących świadczeń na rzecz obrony	
34.	Kurierzy akcji kurierskiej	
35.	Wnioski nauczycieli o podjęcie postępowania egzaminacyjnego na stopień nauczyciela mianowanego	
36.	Decyzje w sprawie zajęcia pasa drogowego	
37.	Zbiór wydanych decyzji administracyjnych dotyczących spraw meldunkowych	
38.	Archiwum zakładowe UG	
39.	Rejestr Korespondencji	

Urząd Gminy w Przytyku
ul. Zachęta 57, 26-650 Przytyk

40.	Medale za długoletnie pożycie małżeńskie	
41.	Zamówienia publiczne	
42.	Rozliczanie dotacji pomiędzy gminami na dzieci uczęszczające do przedszkoli publicznych	
43.	Ewidencja Soltysów	
44.	Dane adresowe radnych oraz członków komisji rady gminy	
45.	Wnioski o udostępnienie informacji publicznej	
46.	Rolnicy poszkodowani w wyniku klęsk żywiołowych	
47.	Dowóz uczniów do szkół w tym uczniów niepełnosprawnych	
48.	Wyprawka szkolna	
49.	Dofinansowanie pracodawcom kosztów kształcenia zawodowego	
50.	Ewidencja użytkowników przydomowych oczyszczalni ścieków	
51.	Rejestr mieszkańców	
52.	Zwrot podatku akcyzowego dla rolników	
53.	Księgowość i finanse	
54.	Zakładowy Fundusz Świadczeń Socjalnych	
55.	Komisja ds. świadczeń socjalnych	

Urząd Gminy w Przytyku
ul. Zachęta 57, 26-650 Przytyk

56.	Zaświadczenia o braku zaległości w podatkach	
57.	Windykacja należności z tytułu podatków i opłat	
58.	Gospodarka wodna	
59.	Plany urządzania lasów niestanowiących własności Skarbu Państwa	
60.	Monitoring wizyjny	
61.	Ewidencja gruntów i budynków	
62.	Promocja gminy	
63.	Spis rolny	
64.	Rejestr wniosków i miejscowych planów zagospodarowania przestrzennego oraz studium uwarunkowań i kierunków zagospodarowania przestrzennego	
65.	Zapytania ofertowe	
66.	Program " Czyste powietrze"	
67.	Dodatek osłonowy	
68.	Konkursy na stanowiska w jednostkach podległych	

Z up. WÓJTA
mgr Małgorzata Kowalczyk
ZASTĘPCA WÓJTA

Urząd Gminy w Przytyku
ul. Zachęta 57, 26-650 Przytyk

ZAŁĄCZNIK NR 2 – ZASADY RETENCJI DANYCH OSOBOWYCH

RODO nakłada na Administratora Danych obowiązek przechowywania danych w postaci umożliwiającej identyfikację osób, których dotyczą, nie dłużej niż jest to niezbędne do osiągnięcia celu przetwarzania. Po osiągnięciu celu dane osobowe powinny zostać usunięte lub poddane anonimizacji. W tym celu, Administrator Danych jest zobowiązany do stałego nadzorowania zawartości administrowanych zbiorów danych oraz występujących w ich ramach procesów przetwarzania, pod kątem konieczności usuwania danych zbędnych, albo do których przetwarzania przestał być upoważniony.

W związku z powyższym, dla danych osobowych przetwarzanych przez Urząd Gminy w Przytyku, ul. Zachęta 57, 26-650 Przytyk, jako ich administratora w rozumieniu art. 4 pkt 7 RODO, ustala się następujące terminy retencji.

Lp.	Proces przetwarzania danych osobowych	Retencja danych
1.	Prowadzenie akt osobowych	Art. 6 ust. 1 lit c RODO Zgodnie z obowiązującymi przepisami prawa
2.	Wypłata wynagrodzeń	Art. 6 ust. 1 lit c RODO Zgodnie z obowiązującymi przepisami prawa
3.	Prowadzenie dokumentacji BHP	Art. 6 ust. 1 lit c RODO 5 lat
4.	Rekrutacja kandydatów do pracy	Art. 6 ust. 1 lit a i c RODO Na czas trwania procesu
5.	Rejestr podatków i opłat lokalnych	Art. 6 ust. 1 lit c RODO Zgodnie z obowiązującymi przepisami prawa
6.	Kontokwinariusze zobowiązania pieniężnego -rejestr podatników i dłużników gminy	Art. 6 ust. 1 lit c RODO Zgodnie z obowiązującymi przepisami prawa
7.	Rejestr opłat za zagospodarowanie odpadów komunalnych	Art. 6 ust. 1 lit c RODO Zgodnie z obowiązującymi przepisami prawa

Urząd Gminy w Przytyku
ul. Zachęta 57, 26-650 Przytyk

8.	Ewidencja skarg i wniosków oraz petycji	Art. 6 ust. 1 lit c RODO Zgodnie z obowiązującymi przepisami prawa
9.	Rejestr cudzoziemców	Art. 6 ust. 1 lit c RODO Zgodnie z obowiązującymi przepisami prawa
10.	Rejestr wydawanych decyzji o warunkach zabudowy i zagospodarowania terenu	Art. 6 ust. 1 lit c RODO Zgodnie z obowiązującymi przepisami prawa
11.	Ewidencja działalności gospodarczej	Art. 6 ust. 1 lit c RODO Zgodnie z obowiązującymi przepisami prawa
12.	Rejestr wyborców i rejestr pełnomocnictw	Art. 6 ust. 1 lit c RODO Zgodnie z obowiązującymi przepisami prawa
13.	Urząd Stanu Cywilnego	Art. 6 ust. 1 lit c RODO Zgodnie z obowiązującymi przepisami prawa
14.	Rejestr dowodów osobistych	Art. 6 ust. 1 lit c RODO Zgodnie z obowiązującymi przepisami prawa
15.	Oświadczenia o stanie majątkowym osób sprawujących funkcje publiczne	Art. 6 ust. 1 lit c RODO Zgodnie z obowiązującymi przepisami prawa
16.	Rejestr Płatników od środków transportowych	Art. 6 ust. 1 lit c RODO Zgodnie z obowiązującymi przepisami prawa
17.	Rejestr aktów własności ziemi	Art. 6 ust. 1 lit c RODO Zgodnie z obowiązującymi przepisami prawa
18.	System Informacji Oświatowej	Art. 6 ust. 1 lit c RODO

Urząd Gminy w Przytyku
ul. Zachęta 57, 26-650 Przytyk

		Zgodnie z obowiązującymi przepisami prawa
19.	Wykonywanie orzeczeń sądowych w zakresie nieodpłatnej pracy na cele społeczne	Art. 6 ust. 1 lit c RODO Zgodnie z obowiązującymi przepisami prawa
20.	Spełnienie obowiązku nauki	Art. 6 ust. 1 lit c RODO Zgodnie z obowiązującymi przepisami prawa
21.	Wykaz decyzji zezwalających na usuwanie drzew i krzewów	Art. 6 ust. 1 lit c RODO Zgodnie z obowiązującymi przepisami prawa
22.	Numeracja porządkowa nieruchomości	Art. 6 ust. 1 lit c RODO Zgodnie z obowiązującymi przepisami prawa
23.	Świadczenia osobiste i rzeczowe	Art. 6 ust. 1 lit c RODO Zgodnie z obowiązującymi przepisami prawa
24.	Regulowanie własności działek o nieuregulowanym stanie prawnym	Art. 6 ust. 1 lit c RODO Zgodnie z obowiązującymi przepisami prawa
25.	Decyzje w sprawie zmiany nazwisk i imion	Art. 6 ust. 1 lit c RODO Zgodnie z obowiązującymi przepisami prawa
26.	Podziały, rozgraniczenia oraz wznowienie granic na nieruchomościach	Art. 6 ust. 1 lit c RODO Zgodnie z obowiązującymi przepisami prawa
27.	Kandydaci na ławników	Art. 6 ust. 1 lit c RODO Zgodnie z obowiązującymi przepisami prawa

Urząd Gminy w Przytyku
ul. Zachęta 57, 26-650 Przytyk

28.	Zbiór informacji o rodzaju i miejscach występowania azbestu lub wyrobów zawierających azbest	Art. 6 ust. 1 lit c RODO Zgodnie z obowiązującymi przepisami prawa
29.	Decyzje o środowiskowych uwarunkowaniach zgody na realizację przedsięwzięcia	Art. 6 ust. 1 lit c RODO Zgodnie z obowiązującymi przepisami prawa
30.	Ewidencja bezodpływowych zbiorników na nieczystości ciekłe	Art. 6 ust. 1 lit c RODO Zgodnie z obowiązującymi przepisami prawa
31.	Rejestr zezwoleń na sprzedaż napojów alkoholowych	Art. 6 ust. 1 lit c RODO Zgodnie z obowiązującymi przepisami prawa
32.	Ewidencja najemców lokali komunalnych	Art. 6 ust. 1 lit c RODO Zgodnie z obowiązującymi przepisami prawa
33.	Ewidencja decyzji dotyczących świadczeń na rzecz obrony	Art. 6 ust. 1 lit c RODO Zgodnie z obowiązującymi przepisami prawa
34.	Kurierzy akcji kurierskiej	Art. 6 ust. 1 lit c RODO Zgodnie z obowiązującymi przepisami prawa
35.	Wnioski nauczycieli o podjęcie postępowania egzaminacyjnego na stopień nauczyciela mianowanego	Art. 6 ust. 1 lit c RODO Zgodnie z obowiązującymi przepisami prawa
36.	Decyzje w sprawie zajęcia pasa drogowego	Art. 6 ust. 1 lit c RODO Zgodnie z obowiązującymi przepisami prawa
37.	Zbiór wydanych decyzji administracyjnych dotyczących spraw meldunkowych	Art. 6 ust. 1 lit c RODO Zgodnie z obowiązującymi przepisami prawa
38.	Archiwum zakładowe UG	Art. 6 ust. 1 lit c RODO

POLITYKA OCHRONY DANYCH OSOBOWYCH

Urząd Gminy w Przytyku
ul. Zachęta 57, 26-650 Przytyk

		Zgodnie z obowiązującymi przepisami prawa
39.	Rejestr Korespondencji	Art. 6 ust. 1 lit c RODO 5 lat
40	Medale za długoletnie pożycie małżeńskie	Art. 6 ust. 1 lit c RODO Zgodnie z obowiązującymi przepisami prawa
41.	Zamówienia publiczne	Art. 6 ust. 1 lit c RODO Zgodnie z obowiązującymi przepisami prawa
42.	Rozliczanie dotacji pomiędzy gminami na dzieci uczęszczające do przedszkoli publicznych	Art. 6 ust. 1 lit c RODO Zgodnie z obowiązującymi przepisami prawa
43.	Ewidencja Soltysów	Art. 6 ust. 1 lit c RODO Zgodnie z obowiązującymi przepisami prawa
44.	Dane adresowe radnych oraz członków komisji rady gminy	Art. 6 ust. 1 lit c RODO Zgodnie z obowiązującymi przepisami prawa
45.	Wnioski o udostępnienie informacji publicznej	Art. 6 ust. 1 lit c RODO Zgodnie z obowiązującymi przepisami prawa
46.	Rolnicy poszkodowani w wyniku klęsk żywiołowych	Art. 6 ust. 1 lit c RODO Zgodnie z obowiązującymi przepisami prawa
47.	Dowóz uczniów do szkół w tym uczniów niepełnosprawnych	Art. 6 ust. 1 lit c RODO Zgodnie z obowiązującymi przepisami prawa
48.	Wyprawka szkolna	Art. 6 ust. 1 lit c RODO Zgodnie z obowiązującymi przepisami prawa

Urząd Gminy w Przytyku
ul. Zachęta 57, 26-650 Przytyk

49.	Dofinansowanie pracodawcom kosztów kształcenia zawodowego	Art. 6 ust. 1 lit c RODO Zgodnie z obowiązującymi przepisami prawa
50.	Ewidencja użytkowników przydomowych oczyszczalni ścieków	Art. 6 ust. 1 lit c RODO Zgodnie z obowiązującymi przepisami prawa
51.	Rejestr mieszkańców	Art. 6 ust. 1 lit c RODO Zgodnie z obowiązującymi przepisami prawa
52.	Zwrot podatku akcyzowego dla rolników	Art. 6 ust. 1 lit c RODO Zgodnie z obowiązującymi przepisami prawa
53.	Księgowość i finanse	Art. 6 ust. 1 lit c RODO 6 lat
54.	Zakładowy Fundusz Świadczeń Socjalnych	Art. 6 ust. 1 lit. a, b i c RODO 5 lat
55.	Komisja ds. świadczeń socjalnych	Art. 6 ust. 1 lit c RODO 5 lat
56.	Zaświadczenia o braku zaległości w podatkach	Art. 6 ust. 1 lit c RODO Zgodnie z obowiązującymi przepisami prawa
57.	Windykacja należności z tytułu podatków i opłat	Art. 6 ust. 1 lit c RODO Zgodnie z obowiązującymi przepisami prawa
58.	Gospodarka wodna	Art. 6 ust. 1 lit c RODO Zgodnie z obowiązującymi przepisami prawa

Urząd Gminy w Przytyku
ul. Zachęta 57, 26-650 Przytyk

59.	Plany urządzania lasów niestanowiących własności Skarbu Państwa	Art. 6 ust. 1 lit c RODO Zgodnie z obowiązującymi przepisami prawa
60	Monitoring wizyjny	Art. 6 ust. 1 lit f RODO Nie dłużej niż 3 miesiące od nagrania
61.	Ewidencja gruntów i budynków	Art. 6 ust. 1 lit c RODO Zgodnie z obowiązującymi przepisami prawa
62.	Promocja gminy	Art. 6 ust. 1 lit c RODO Zgodnie z obowiązującymi przepisami prawa
63.	Spis rolny	Art. 6 ust. 1 lit c RODO Zgodnie z obowiązującymi przepisami prawa
64.	Rejestr wniosków i miejscowych planów zagospodarowania przestrzennego oraz studium uwarunkowań i kierunków zagospodarowania przestrzennego	Art. 6 ust. 1 lit c RODO Zgodnie z obowiązującymi przepisami prawa
65.	Zapytania ofertowe	Art. 6 ust. 1 lit c RODO Zgodnie z obowiązującymi przepisami prawa
66.	Program " Czyste powietrze"	Art. 6 ust. 1 lit c RODO Zgodnie z obowiązującymi przepisami prawa
67.	Dodatek osłonowy	Art. 6 ust. 1 lit c RODO Zgodnie z obowiązującymi przepisami prawa
68.	Konkursy na stanowiska w jednostkach podległych	Art. 6 ust. 1 lit c RODO

POLITYKA OCHRONY DANYCH OSOBOWYCH

Urząd Gminy w Przytyku
ul. Zachęta 57, 26-650 Przytyk

		Zgodnie z obowiązującymi przepisami prawa
--	--	--

Z up. WÓJTA
mgr Małgorzata Kowalczyk
ZASTĘPCA WÓJTA

Urząd Gminy w Przytyku

ul. Zachęta 57, 26-650 Przytyk

**ZAŁĄCZNIK NR 3 –UPOWAŻNIENIA DO PRZETWARZANIA DANYCH
OSOBOWYCH**

1. Upoważnienia do przetwarzania danych osobowych nadawane są przez IOD, na mocy delegacji uprawnienia do nadawania upoważnień nadanego przez Administratora Danych.
2. Osobą odpowiedzialną za informowanie IOD o konieczności nadania upoważnienia do przetwarzania danych osobowych, jego zmiany lub odwołania, jest ADO
3. Szczegółowa procedura nadawania upoważnień do przetwarzania danych osobowych, ich zmiany lub odwołania, została wskazana poniżej.

Nadanie upoważnienia

1. W przypadku zatrudnienia nowego pracownika, który w ramach swoich obowiązków służbowych będzie przetwarzał dane osobowe, istnieje konieczność nadania mu stosownego upoważnienia do przetwarzania danych osobowych. To samo tyczy się sytuacji, w której dochodzi do zmiany stanowiska pracownika, która łączy się z uzyskaniem dostępu do danych osobowych.
2. ADO wysyła IOD drogą elektroniczną na adres email wniosek o nadanie upoważnienia.
3. Wniosek o nadanie upoważnienia stanowi tabela w pliku Excel, która zawiera:
 3. 1 imię i nazwisko upoważnianego,
 3. 2 stanowisko upoważnianego,
 3. 3 służbowy adres email upoważnianego (jeżeli posiada),
 - 3.4 zbiory danych, do których upoważniany będzie miał dostęp.
4. Wydanie każdego upoważnienia jest odnotowywane przez IOD w prowadzonej przez niego ewidencji osób upoważnionych do przetwarzania danych osobowych.
5. Ewidencja osób upoważnionych do przetwarzania danych osobowych jest prowadzona przez IOD w formie elektronicznej z możliwością wydruku na każde żądanie.

Zmiana zakresu upoważnienia

1. Zakres nadanego pracownikowi upoważnienia może ulegać zmianie (rozszerzeniu bądź zawężeniu) w związku z pełnieniem przez niego określonych zadań w określonym przedziale czasu.

Urząd Gminy w Przytyku
ul. Zachęta 57, 26-650 Przytyk

2. W przypadku zmiany stanowiska pracy łączącej się ze zmianą zakresu danych, które przetwarza pracownik, istnieje konieczność złożenia wniosku o zmianę upoważnienia.
3. W przypadku konieczności zmiany upoważnienia, ADO wysyła IOD drogą elektroniczną na adres email wniosek o zmianę nadanego upoważnienia.
4. Wniosek o zmianę upoważnienia stanowi tabela w pliku Excel, która zawiera:
 - 4.1. imię i nazwisko upoważnianego,
 - 4.2. nowe stanowisko upoważnianego,
 - 4.3. zbiory danych, do których upoważniany będzie miał dostęp w związku ze zmianą stanowiska.
5. Na podstawie otrzymanego wniosku IOD zmienia zakres upoważnienia.
6. Zmiana zakresu wydanego upoważnienia jest odnotowywana przez IOD w prowadzonej ewidencji upoważnień.

Odwołanie upoważnienia

1. Utrata prawa do przetwarzania danych osobowych określonych w upoważnieniu następuje w szczególności w przypadku:
 - 1.1. zmiany stanowiska pracy na stanowisko, na którym nie ma konieczności posiadania dostępu do danych osobowych lub w szczególności, gdy ustaje zasadność i celowość dalszego wykonywania prawa do przetwarzania danych w związku ze zmianą realizowanych przez pracownika zadań wynikających z jego indywidualnego zakresu czynności,
 - 1.2. umyślnego naruszenia zasad ochrony danych osobowych określonych w Ustawie, RODO lub Polityce,
 - 1.3. rozwiązania stosunku pracy,
 - 1.4. rozwiązania umowy cywilnoprawnej.
2. ADO wysyła IOD drogą elektroniczną na adres email wniosek o odwołanie upoważnienia.
3. Wniosek o odwołanie upoważnienia stanowi tabela w pliku Excel, która zawiera:
 - 3.1. imię i nazwisko osoby, której ma zostać odwołane upoważnienie,
 - 3.2. stanowisko osoby, której ma zostać odwołane upoważnienie,
 - 3.3. wskazanie przyczyny odwołania upoważnienia.

POLITYKA OCHRONY DANYCH OSOBOWYCH

Urząd Gminy w Przytyku

ul. Zachęta 57, 26-650 Przytyk

4. Na podstawie wniosku IOD odwołuje upoważnienie.
5. Odwołanie upoważnienia następuje poprzez jego wycofanie w ewidencji upoważnień prowadzonej przez IOD.


Z up. WÓJTA
mgr Magdalena Kowalczyk
ZASTĘPCA WÓJTA

POLITYKA OCHRONY DANYCH OSOBOWYCH

Urząd Gminy w Przytyku

ul. Zachęta 57, 26-650 Przytyk

UPOWAŻNIENIE DO PRZETWARZANIA DANYCH OSOBOWYCH

NR 1/201...

Działając na podstawie art. 29 Rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych),

– udziela się Panu/Pani*:

[redacted]

(imię i nazwisko)

[redacted]

(stanowisko służbowe)

upoważnienia do przetwarzania danych osobowych w rozumieniu 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) do procesu o nazwie:

[redacted]

[redacted]

Jest Pan/Pani* upoważniony/upoważniona* do przetwarzania danych osobowych wyłącznie w zakresie wynikającym z Pana/Pani* zadań służbowych oraz poleceń przełożonego lub wynikających z zawartej umowy cywilno – prawnej

W każdym wypadku upoważnienie traci ważność z chwilą ustania stosunku pracy lub wygaśnięcia umowy.

.....

data i podpis osoby upoważniającej)

- niepotrzebne skreślić

POLITYKA OCHRONY DANYCH OSOBOWYCH

Urząd Gminy w Przytyku

ul. Zachęta 57, 26-650 Przytyk

Osoba upoważniona obowiązana jest przetwarzać dane osobowe zawarte w ww. zbiorach danych osobowych w zakresie i w sposób wymagany do wypełnienia obowiązków służbowych względem Urzędu Gminy w Przytyku, ul. Zachęta 57, 26-650 Przytyk

Osoba upoważniona zobowiązuje się do przetwarzania danych osobowych zgodnie z udzielonym upoważnieniem oraz z przepisami RODO, wydanymi na jego podstawie krajowymi aktami wykonawczymi, w szczególności obowiązującymi w Urzędzie Gminy w Przytyku, ul. Zachęta 57, 26-650 Przytyk wewnętrznymi regulacjami w sprawie ochrony danych osobowych.

Naruszenie ww. obowiązków może skutkować poniesieniem odpowiedzialności karnej na podstawie przepisów określonych w Ustawie oraz stanowi ciężkie naruszenie obowiązków pracowniczych, które może być podstawą rozwiązania umowy o pracę w trybie art. 52 Kodeksu Pracy lub odpowiedzialności cywilnej.

Data i podpis upoważniającego

Data i podpis osoby upoważnionej

Oświadczenie

Oświadczam, że zapoznałam/em się, w zakresie wynikającym z przydzielonych zadań, z obowiązującymi w odniesieniu do ochrony danych osobowych przepisami prawa i regulacjami wewnętrznymi obowiązującymi w Urzędzie Gminy w Przytyku, ul. Zachęta 57, 26-650 Przytyk (w szczególności z Polityką ochrony danych osobowych). Przyjmuję do wiadomości zawarte w nich obowiązki dotyczące ochrony danych osobowych i zobowiązuje się do ich stosowania.

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

Data i podpis osoby upoważnionej

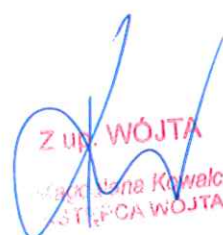
POLITYKA OCHRONY DANYCH OSOBOWYCH

Urząd Gminy w Przytyku

ul. Zachęta 57, 26-650 Przytyk

**ZAŁĄCZNIK NR 4 – WZÓR EWIDENCJI OSÓB UPOWAŻNIONYCH DO
PRZETWARZANIA DANYCH OSOBOWYCH**

Lp.	Imię i nazwisko osoby upoważnionej	Data nadania upoważnienia	Data ustania upoważnienia	Nazwy zbiorów objętych zakresem upoważnienia
1.				
2.				
3.				
4.				
5.				
6.				
7.				
8.				


Z UP. WÓJTA
Marek Józef Kowalczyk
ST. P. CA WÓJTA

POLITYKA OCHRONY DANYCH OSOBOWYCH

Urząd Gminy w Przytyku

ul. Zachęta 57, 26-650 Przytyk

**ZAŁĄCZNIK NR 5 – WZORY WYZNACZENIA ORAZ ODWOŁANIA
INSPEKTORA OCHRONY DANYCH**

Wyznaczenie Inspektora Ochrony Danych

Niniejszym, reprezentując Administratora Danych - Urząd Gminy w Przytyku, ul. Zachęta 57, 26-650 Przytyk z dniem .../.../..... r.

wyznaczam

Pana/ Panią do pełnienia funkcji **Inspektora Ochrony Danych (IOD)** w Urzędzie Gminy w Przytyku, ul. Zachęta 57, 26-650 Przytyk

Upoważniam Pana/ Panią do przetwarzania danych osobowych we wszystkich zbiorach Administratora Danych w zakresie niezbędnym dla należytego wykonywania funkcji Inspektora Ochrony Danych.

Upoważniam Pana/ Panią do wydawania w imieniu Administratora Danych upoważnień do przetwarzania danych osobowych.

Zakres pozostałych obowiązków oraz warunki pełnienia funkcji Inspektora Ochrony Danych określone zostały w Umowie zawartej w dniu/..../..... oraz Polityce ochrony danych osobowych wdrożonej w Urzędzie Gminy w Przytyku, ul. Zachęta 57, 26-650 Przytyk

Data i podpis osoby wyznaczanej do pełnienia funkcji IOD

Data i podpis Administratora Danych


Z. J. WÓJTA
mgr Magdalena Kowalczyk
ZASTĘPCA WÓJTY

Urząd Gminy w Przytyku
ul. Zachęta 57, 26-650 Przytyk
Odwolanie Inspektora Ochrony Danych

Niniejszym, reprezentując Administratora Danych - Urząd Gminy w Przytyku, ul. Zachęta 57, 26-650 Przytyk z dniem .../.../.....,

odwołuję

Panią / Pana

z pełnienia funkcji **Inspektora Ochrony Danych (IOD)** w Urzędzie Gminy w Przytyku, ul. Zachęta 57, 26-650 Przytyk

Data i podpis osoby odwoływanej z pełnienia funkcji IOD

Data i podpis Administratora Danych


Z DP. WÓJTA
mgr Magdalena Kocwańczyk
ZASTĘPCA WÓJTY

POLITYKA OCHRONY DANYCH OSOBOWYCH

Urząd Gminy w Przytyku

ul. Zachęta 57, 26-650 Przytyk

**ZAŁĄCZNIK NR 6 – WZORY WYZNACZENIA ORAZ ODWOŁANIA
ADMINISTRATORA SYSTEMÓW INFORMATYCZNYCH**

Wyznaczenie Administratora Systemów Informatycznych

Niniejszym, reprezentując Administratora Danych - Urząd Gminy w Przytyku, ul. Zachęta 57, 26-650 Przytyk z dniem .../.../.....,

wyznaczam

Panią / Pana

do pełnienia funkcji **Administratora Systemów Informatycznych (ASI)** w Urzędzie Gminy w Przytyku, ul. Zachęta 57, 26-650 Przytyk

Zakres obowiązków oraz warunki pełnienia funkcji Administratora Systemów Informatycznych określone zostały w Polityce ochrony danych osobowych wdrożonej w Urzędzie Gminy w Przytyku, ul. Zachęta 57, 26-650 Przytyk

Data i podpis osoby wyznaczanej do pełnienia funkcji ASI

Data i podpis Administratora Danych


mgr inż. ...
ZASTĘPCA WÓJTA

Urząd Gminy w Przytyku
ul. Zachęta 57, 26-650 Przytyk

Odwołanie Administratora Systemów Informatycznych

Niniejszym, reprezentując Administratora Danych - Urząd Gminy w Przytyku, ul. Zachęta 57, 26-650 Przytyk z dniem .../.../.....,

odwołuję

Panią / Pana

z pełnienia funkcji **Administratora Systemów Informatycznych (ASI)** w Urzędzie Gminy w Przytyku,
ul. Zachęta 57, 26-650 Przytyk

Data i podpis osoby odwoływanej z pełnienia funkcji ASI

Data i podpis Administratora Danych

Z up. WÓJTA
mgr Magdalena Kowalczyk
ZASTĘPCA WÓJTY

Urząd Gminy w Przytyku

ul. Zachęta 57, 26-650 Przytyk

**ZAŁĄCZNIK NR 7 OŚWIADCZENIE PRACOWNIKA O ZAPOZNANIU SIĘ Z
DOKUMENTACJĄ**

.....
(data)

.....
Imię i nazwisko pracownika

Oświadczenie

Oświadczam, że zapoznała(e)m się, rozumiem i będę przestrzegać obowiązków wynikających z przepisów 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) (RODO), Ustawy z dnia 10 maja 2018 r. o ochronie danych osobowych, t.j., Dz. U. z 2019r. poz. 730. oraz dokumentów przyjętych przez – Urząd Gminy w Przytyku, ul. Zachęta 57, 26-650 Przytyk - w związku z przetwarzaniem danych osobowych, a w szczególności:

- Polityki ochrony danych osobowych;

Zobowiązuję się do podejmowania działań zmierzających do zapewnienia bezpieczeństwa przetwarzania danych osobowych poprzez ich ochronę przed niepowołanym dostępem, nieuzasadnioną modyfikacją lub zniszczeniem, nielegalnym ujawnieniem lub pozyskaniem oraz unikaniem tych zachowań, które mogłyby poziom bezpieczeństwa danych osobowych obniżyć.

Zobowiązuję się do zachowania w tajemnicy danych osobowych oraz sposobów ich zabezpieczenia, do których uzyskam dostęp w trakcie zatrudnienia, również po ustaniu zatrudnienia.

Jednocześnie przyjmuje do wiadomości, że za niedopełnienie obowiązków wynikających z niniejszego oświadczenia ponoszę odpowiedzialność na podstawie przepisów Regulaminu pracy, Kodeksu pracy oraz RODO.

.....
Podpis składającego oświadczenie

Potwierdzam odbiór 1 egz. oświadczenia.

.....
Podpis ADO

Z up. WÓJTA
mgr Magdalena Kowalczyk
ZASTĘPCA WÓJTY

Urząd Gminy w Przytyku

ul. Zachęta 57, 26-650 Przytyk

ZAŁĄCZNIK NR 8 REJESTR KATEGORII CZYNNOŚCI PRZETWARZANIA PODMIOTU PRZETWARZAJĄCEGO

Kategorie przetwarzania	Ogólny opis technicznych i organizacyjnych środków bezpieczeństwa (jeżeli jest to możliwe)	Administrator			Inspektor ochrony danych administratora (jeśli powołano)	Nazwy państw trzecich lub organizacji międzynarodowych, do których dane są przekazywane	Dokumentacja odpowiednich zabezpieczeń danych osobowych przekazywanych na podstawie art. 49 ust. 1 akapit drugi
		Nazwa i dane kontaktowe administratora	Nazwa i dane kontaktowe współadministratora (jeżeli dotyczy)	Nazwa i dane kontaktowe przedstawiciela administratora (jeśli wyznaczono)			
		Podstawa prawna					
Lp							
1.							
2.							
3.							
4.							
5.							
6.							
7.							

mgr Magdalena Kowalczyk
ZASTĘPCA WÓJTY

Urząd Gminy w Przytyku

ul. Zachęta 57, 26-650 Przytyk

ZAŁĄCZNIK NR 9 REJESTR CZYNNOŚCI PRZETWARZANIA ADMINISTRATORA

■ kolorem niebieskim oznaczono informacje wymagane w rejestrze przez art. 30 ust. 1 RODO

l p	Nazwa czynności przetwarzania	Jednostka organizacyjna (departament, dział itp.)	Cel przetwarzania	Kategoria osób	Kategorie danych	Podstawa prawna	Źródło danych	Planowany termin usunięcia kategorii danych (jeżeli jest to możliwe)	Nazwa współadministratora i dane kontaktowe (jeżeli dotyczy)	Nazwa podmiotu przetwarzającego i dane kontaktowe (jeżeli dotyczy)	Kategorie odbiorców (innych niż podmiot przetwarzający)	Nazwa systemu lub oprogramowania	Ogólny opis technicznych i organizacyjnych środków bezpieczeństwa zgodnie z art. 32 ust. 1 (jeżeli jest to możliwe)
			Art. 30 ust. 1 pkt b	Art. 30 ust. 1 pkt c	Art. 30 ust. 1 pkt c			Art. 30 ust. 1 pkt f	Art. 30 ust. 1 pkt a	Art. 30 ust. 1 pkt d	Art. 30 ust. 1 pkt d		Art. 30 ust. 1 pkt g
1.													
2.													
3.													
4.													
5.													
6.													

POLITYKA OCHRONY DANYCH OSOBOWYCH

Urząd Gminy w Przytyku
ul. Zachęta 57, 26-650 Przytyk

Instrukcja Zarządzania Systemem Informatycznym
służącym do przetwarzania danych osobowych
wraz z procedurami dotyczącymi cyberbezpieczeństwa i bezpieczeństwa informacji
w Urzędzie Gminy Przytyk
ul. Zachęta 57, 26-650 Przytyk

**INSTRUKCJA ZARZĄDZANIA SYSTEMEM
INFORMATYCZNYM
SŁUŻĄCYM DO PRZETWARZANIA
DANYCH OSOBOWYCH WRAZ Z
PROCEDURAMI DOTYCZĄCYMI
CYBERBEZPIECZEŃSTWA I
BEZPIECZEŃSTWA INFORMACJI**

**Urząd Gminy Przytyk
ul. Zachęta 57, 26-650 Przytyk**

Instrukcja Zarządzania Systemem Informatycznym
służącym do przetwarzania danych osobowych
wraz z procedurami dotyczącymi cyberbezpieczeństwa i bezpieczeństwa informacji
w Urzędzie Gminy Przytyk
ul. Zachęta 57, 26-650 Przytyk

I. Postanowienia ogólne

1. Instrukcja zarządzania systemem informatycznym służącym do przetwarzania danych osobowych zwana dalej „Instrukcją” została opracowana jako dobra praktyka stosowania/przestrzegania przepisów o ochronie danych osobowych.
2. Procedura zarządzania incydentami związanymi z bezpieczeństwem informacji oraz cyberbezpieczeństwem ma na celu zapewnienie ciągłości operacyjnej oraz ograniczenie wpływu przypadków naruszeń bezpieczeństwa zasobów informacyjnych na działalność Urzędu.

II. Podstawa prawna i dokumenty powiązane

1. Polityka ochrony danych osobowych w Urzędzie Gminy Przytyk
2. Ustawa z dnia 10 maja 2018 r. o ochronie danych osobowych (tj. Dz. U. 2019 poz. 1781)
3. 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
4. art. 22 ust.1 pkt 1 Ustawy o krajowym systemie cyberbezpieczeństwa z dnia 05 lipca 2018 r
5. § 20 ust.2 pkt.13 Rozporządzenia Rady Ministrów z dnia 12 kwietnia 2012 r w sprawie Krajowych Ram Interoperacyjności, minimalnych wymagań dla rejestrów publicznych i wymiany informacji w postaci elektronicznej oraz minimalnych wymagań dla systemów teleinformatycznych

III. Definicje użyte w niniejszej Instrukcji oznaczają:

1. **Administrator danych osobowych** - Wójt Gminy Przytyk, który decyduje o środkach i celach przetwarzania danych osobowych, reprezentowany przez właścicieli
2. **Administrator Systemów Informatycznych (ASI)** – osoba wyznaczona przez Administratora Danych, koordynująca działania związane z zapewnieniem bezpieczeństwa systemów informatycznych, w tym również odpowiadająca za nadzór nad zabezpieczeniem danych osobowych przetwarzanych w systemach informatycznych wykorzystywanych przez Administratora Danych,
3. **Dane osobowe** – informacje o zidentyfikowanej lub możliwej do zidentyfikowania osobie fizycznej („osobie, której dane dotyczą”), gdzie poprzez możliwą do zidentyfikowania osobę fizyczną rozumie się osobę, 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

Instrukcja Zarządzania Systemem Informatycznym
służącym do przetwarzania danych osobowych
wraz z procedurami dotyczącymi cyberbezpieczeństwa i bezpieczeństwa informacji
w Urzędzie Gminy Przytyk
ul. Zachęta 57, 26-650 Przytyk
szczególnych czynników określających fizyczną, fizjologiczną, genetyczną, psychiczną,
ekonomiczną, kulturową lub społeczną tożsamość osoby fizycznej,

4. **Osoba upoważniona** – osoba posiadająca formalne upoważnienie wydane przez Administratora danych osobowych.
5. **Przetwarzanie** – operacja 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,
6. **Ustawa** – rozumie się przez to ustawę z dnia 10 maja 2018 r. o ochronie danych osobowych (tj. Dz. U. 2019 poz. 1781)
7. **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 (ogólne rozporządzenie o ochronie danych),
8. **System informatyczny** – zespół współpracujących urządzeń, programów, procedur przetwarzania informacji i narzędzi programowych zastosowanych w celu przetwarzania danych.
9. **Użytkownik systemu** – osoba upoważniona do bezpośredniego dostępu do danych osobowych przetwarzanych w systemie informatycznym.
10. **Zbiór danych osobowych** – oznacza uporządkowany zestaw danych osobowych dostępnych według określonych kryteriów, niezależnie od tego, czy zestaw ten jest scentralizowany, zdecentralizowany czy rozproszony funkcjonalnie lub geograficznie;
11. **Incydent w podmiocie publicznym** - incydent, który powoduje lub może spowodować obniżenie jakości lub przerwanie realizacji zadania publicznego realizowanego przez podmiot publiczny.
12. **Incydent krytyczny** – incydent skutkujący znaczną szkodą dla bezpieczeństwa lub porządku prawnego, interesów międzynarodowych, interesów gospodarczych, działania instytucji publicznych, praw lub wolności obywatelskich lub życia i zdrowia ludzi, klasyfikowany przez właściwy CSIRT NASK.

Instrukcja Zarządzania Systemem Informatycznym
służącym do przetwarzania danych osobowych
wraz z procedurami dotyczącymi cyberbezpieczeństwa i bezpieczeństwa informacji
w Urzędzie Gminy Przytyk
ul. Zachęta 57, 26-650 Przytyk

13. Inspektor Ochrony Danych - osoba wyznaczona przez Administratora Danych Osobowych
zwanego dalej „IOD”

IV. Zakres oraz cel Instrukcji

1. Instrukcja zawiera procedury zarządzania incydentami związanymi z bezpieczeństwem informacji oraz cyberbezpieczeństwem w Urzędzie Gminy w Przytyku.
2. Celem Instrukcji jest określenie podstawowych zasad właściwego zarządzania systemem informatycznym służącym do przetwarzania danych osobowych oraz podstawowych warunków technicznych i organizacyjnych, jakim powinny odpowiadać wchodzące w jego skład, urządzenia, odpowiednio do zagrożeń i kategorii danych objętych ochroną.
3. Instrukcję stosuje się do danych osobowych przetwarzanych w systemach informatycznych, danych osobowych zapisanych w postaci elektronicznej na zewnętrznych nośnikach informacji oraz informacji o sposobach zabezpieczenia danych osobowych.
4. Przy przetwarzaniu danych osobowych w systemach informatycznych należy stosować wysoki poziom bezpieczeństwa, ponieważ urządzenia systemu służącego do przetwarzania danych osobowych połączone są z siecią publiczną.
5. Instrukcja zawiera specyfikację podstawowych środków technicznych ochrony danych osobowych oraz elementów zarządzania systemem informatycznym. W przypadku, gdy z oceny funkcjonowania instrukcji wynika, że zachodzi potrzeba wprowadzenia nowych lub modyfikacji istniejących zasad właściwego zarządzania systemem informatycznym służącym do przetwarzania danych osobowych, wnioski w tej sprawie powinni składać użytkownicy systemu do Administratora Danych Osobowych.

V. Kategorie incydentów

1. Incydent bezpieczeństwa informacji oraz cyberbezpieczeństwa to zdarzenie, którego skutkiem jest lub może być naruszenie bezpieczeństwa aktywów informacyjnych oraz który powoduje lub może spowodować obniżenie jakości lub przerwanie realizacji zadania publicznego realizowanego przez podmiot publiczny. Jego przyczyną może być:
 - a. zdarzenie losowe zewnętrzne (np. klęski żywiołowe, pożary, zakłócenia w dostawie energii elektrycznej itp.), którego wystąpienie może spowodować zniszczenie lub uszkodzenie infrastruktury informatycznej albo dokumentacji papierowej oraz zakłócenie ciągłości pracy systemów nie powodując naruszenia poufności danych;

Instrukcja Zarządzania Systemem Informatycznym
służącym do przetwarzania danych osobowych
wraz z procedurami dotyczącymi cyberbezpieczeństwa i bezpieczeństwa informacji
w Urzędzie Gminy Przytyk
ul. Zachęta 57, 26-650 Przytyk

- b. zdarzenie losowe wewnętrzne (np. błędy w oprogramowaniu , awarie sprzętu itp.), które mogą powodować zakłócenia ciągłości pracy systemów a także prowadzić do zniszczenia lub utraty danych;
 - c. świadome i celowe działania mające na celu naruszenie poufności zasobów informacyjnych, w tym poufności danych.
2. Incydentami bezpieczeństwa informacji w szczególności są:
- a. naruszenie poufności, to jest ujawnienie informacji niepowołanym osobom;
 - b. naruszenie integralności, to jest zniszczenie, uszkodzenie lub przekłamanie informacji;
 - c. naruszenie dostępności, to jest braku dostępu do danych przez uprawnionych użytkowników.
3. Przyczyny incydentów bezpieczeństwa informacji oraz cyberbezpieczeństwa mogą dotyczyć:
- a. niewłaściwego wykorzystywania zasobów informatycznych lub niewłaściwe postępowanie z dokumentacją papierową;
 - b. działania szkodliwego oprogramowania;
 - c. próby omijania systemów zabezpieczeń;
 - d. nieautoryzowanego dostępu do systemów, aplikacji i dokumentów;
 - e. zniszczenia lub kradzieży urządzeń wykorzystywanych do przetwarzania i przechowywania informacji;
 - f. zniszczenia lub kradzieży nośników danych;
 - g. próby wyludzeń informacji;
 - h. ataków socjotechnicznych , ataków z wykorzystaniem technik zagrażających poufności, integralności lub dostępności informacji;
 - i. nieprawidłowości w zakresie zabezpieczenia przechowywania danych, w tym danych osobowych;
 - j. naruszenia zasad obowiązujących w Urzędzie dotyczących bezpieczeństwa informacji, w tym danych osobowych.

VI. IV. Zgłaszanie incydentów związanych z bezpieczeństwem informacji oraz cyberbezpieczeństwem

- 1. W przypadku ujawnienia incydentu pracownik niezwłocznie powiadamia o tym fakcie Inspektora Ochrony Danych oraz Administratora Systemów Informatycznych (kiedy incydent dotyczy systemów komputerowych). Zgłoszenie następuje telefonicznie. Dane kontaktowe IOD oraz ASI znajdują się na stronie internetowej www.przytyk.pl . Telefoniczne zgłoszenie należy następnie potwierdzić szczegółową notatką służbową, którą przekazuje się IOD poprzez

Instrukcja Zarządzania Systemem Informatycznym
służącym do przetwarzania danych osobowych
wraz z procedurami dotyczącymi cyberbezpieczeństwa i bezpieczeństwa informacji
w Urzędzie Gminy Przytyk
ul. Zachęta 57, 26-650 Przytyk
swojego bezpośredniego przełożonego lub bezpośrednio do IOD w przypadku pracowników
zatrudnionych na samodzielnych stanowiskach.

2. Notatka musi zawierać następujące informacje:
 - a. Imię i nazwisko osoby zgłaszającej;
 - b. stanowisko oraz komórka organizacyjna Urzędu;
 - c. dokładne miejsce oraz datę wystąpienia incydentu;
 - d. opis incydentu w sposób adekwatny do posiadanej wiedzy i umiejętności zgłaszającego.
3. Brak umiejętności poprawnego rozpoznania incydentu przez osobę zgłaszającą nie może być przyczyną zaniechania zgłoszenia.
4. W przypadku dłuższej nieobecności IOD incydent należy zgłosić do ASI w sposób określony w pkt.1.

VII. Podejmowanie działań w związku ze zgłaszanymi incydentami związanymi z bezpieczeństwem informacji oraz cyberbezpieczeństwem

1. Zgłoszenie incydentu rejestrowane jest przez IOD. Osoba zgłaszająca incydent powinna w miarę możliwości zabezpieczyć materiał dowodowy (np. zrzut ekranu monitora, zdjęcie niezabezpieczonych materiałów zawierających dane osobowe itp.). Działania związane z obsługą zdarzenia w pierwszej kolejności dotyczą rozpoznania i kwalifikacji zgłoszenia. W przypadku, kiedy zgłoszenie zakwalifikowane zostało jako incydent bezpieczeństwa informacji lub cyberbezpieczeństwa, dokonywana jest jego ocena istotności. Powyższe działania wykonuje IOD w porozumieniu z ASI.
2. Przy ocenie istotności incydentu pod uwagę brane są następujące czynniki:
 - a. powstałe szkody będące wynikiem incydentu;
 - b. wpływ incydentu na działanie systemów;
 - c. wpływ incydentu na ciągłość działania Urzędu;
 - d. koszty usunięcia skutków incydentu;
 - e. szacowany czas naprawy skutków wywołanych incydem;
 - f. oszacowanie zasobów koniecznych do przywrócenia ciągłości działania systemów.
3. Zakwalifikowanie zgłoszenia incydentu jako „falszywy alarm” kończy postępowanie, o czym IOD informuje zgłaszającego.
4. W przypadku zakwalifikowania zdarzenia jako incydentu związanego z bezpieczeństwem informacji lub cyberbezpieczeństwem, IOD wspólnie z ASI podejmuje działania

Instrukcja Zarządzania Systemem Informatycznym
służącym do przetwarzania danych osobowych
wraz z procedurami dotyczącymi cyberbezpieczeństwa i bezpieczeństwa informacji
w Urzędzie Gminy Przytyk
ul. Zachęta 57, 26-650 Przytyk
zabezpieczające i naprawcze zmierzające do zniwelowania szkód powstałych w wyniku incydentu.

5. Poinformowany o wynikach analizy incydentu oraz podjętych działaniach naprawczych IOD informuje ADO. W przypadku nieobecności IOD, Administratora powiadamia ASI.
6. W przypadku stwierdzenia incydentu w podmiocie publicznym lub incydentu krytycznego IOD lub ASI (w przypadku nieobecności IOD) nie później niż w ciągu 24 godzin od momentu wykrycia zgłasza incydent do właściwego CSIRT NASK (Naukowa i Akademicka Sieć Komputerowa - Państwowego Instytutu Badawczego ul. Kolska 12, 01-045 Warszawa).
7. Zgłoszenia do CSIRT NASK przekazywane są w sposób elektroniczny. Procedura zgłoszeń opisana jest pod adresem internetowym <https://incydent.cert.pl> . W przypadku braku możliwości przekazania go w sposób elektroniczny można zgłaszać przy użyciu innych dostępnych środków komunikacji (np. na numer telefonu +48223808274).
8. W zgłoszeniu przekazuje się informacje zgodnie z formularzem oraz zgodnie z treścią art. 23 ust. 1 Ustawy o krajowym systemie cyberbezpieczeństwa z dnia 05 lipca 2018 r.
9. W przypadku stwierdzenia działań zamierzonych, przy jednoczesnym zidentyfikowaniu sprawcy incydentu dotyczącego naruszenia bezpieczeństwa informacji oraz cyberbezpieczeństwa ADO podejmuje decyzję dotyczącą wyciągnięcia ewentualnych konsekwencji dyscyplinarnych wobec sprawcy incydentu. Jednocześnie, w zależności od wagi incydentu mogą być powiadomione organy ścigania.

VIII. Podejmowanie działań w związku ze zgłaszanymi incydentami naruszenia bezpieczeństwa przetwarzania danych osobowych.

1. W przypadku naruszenia ochrony danych osobowych mają zastosowanie przepisy art.33-34 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 - RODO) (Dz. Urz. UE L 119 z dnia 05 kwietnia 2016 r).
2. W przypadku stwierdzenia naruszenia zabezpieczenia systemu informatycznego lub zaistnienia sytuacji, które mogą wskazywać na naruszenie ochrony danych osobowych tj.:
 - a. przypadkowe lub niezgodne z prawem zniszczenie danych;
 - b. przypadkowa lub niezgodna z prawem utrata danych;
 - c. przypadkowa lub niezgodna z prawem modyfikacja danych;
 - d. nieuprawnione ujawnienie danych;

Instrukcja Zarządzania Systemem Informatycznym
służącym do przetwarzania danych osobowych
wraz z procedurami dotyczącymi cyberbezpieczeństwa i bezpieczeństwa informacji
w Urzędzie Gminy Przytyk
ul. Zachęta 57, 26-650 Przytyk

e. nieuprawniony dostęp do danych osobowych.

Każdy pracownik zatrudniony przy przetwarzaniu danych osobowych (pracownik, stażysta, praktykant itp.) jest zobowiązany przerwać przetwarzania danych osobowych i niezwłocznie powiadomić o tym fakcie swojego bezpośredniego przełożonego oraz Inspektora Ochrony Danych i Administratora Systemów Informatycznych (jeżeli naruszenie ma związek z systemami informatycznymi).

3. Fakt naruszenia lub podejrzenia naruszenia ochrony danych osobowych należy potwierdzić pisemnie poprzez niezwłoczne sporządzenie notatki służbowej w której umieszcza się informację o dacie, czasie, miejscu, okolicznościach zdarzenia. Notatkę przekazuje się Inspektorowi Ochrony Danych Urzędu Gminy w Przytyku za pośrednictwem swojego przełożonego lub bezpośrednio w przypadku osób zatrudnionych na samodzielnych stanowiskach. O zdarzeniu IOD niezwłocznie powiadamia ADO.
4. W przypadku dłuższej nieobecności IOD notatkę należy przekazać Administratorowi Systemów Informatycznych Urzędu Gminy w Przytyku.
5. Notatka jest rejestrowana przez IOD i przechowywana w teczce „Rejestr naruszeń ochrony danych osobowych”
6. Zgłoszenia są rejestrowane w „Rejestrze naruszeń ochrony danych osobowych” prowadzonym zgodnie z art.33 ust. 5 RODO.
7. Przy ocenie istotności incydentu pod uwagę brane są następujące czynniki:
 - a. charakter naruszenia ochrony danych osobowych;
 - b. kategorię i przybliżoną liczbę osób których dane dotyczą
 - c. kategorię i przybliżoną liczbę wpisów danych osobowych, których dotyczy naruszenie;
 - d. możliwe konsekwencje naruszenia ochrony danych osobowych;
 - e. wpływ incydentu na ciągłość działania Urzędu;
 - f. koszty usunięcia skutków incydentu;
 - g. szacowany czas naprawy skutków wywołanych incydem.
8. Zakwalifikowanie zgłoszenia incydentu jako „fałszywy alarm” kończy postępowanie o czym IOD informuje zgłaszającego.
9. Sprawdzenie naruszenia lub podejrzenia naruszenia ochrony danych osobowych kończy się sprawozdaniem, które przekazywane jest ADO. Sprawozdanie wykonuje IOD wraz z ASI
10. W przypadku zakwalifikowania zdarzenia jako naruszenie ochrony danych osobowych, które skutkuje ryzykiem naruszenia praw lub wolności osób fizycznych, ADO bez zbędnej zwłoki ,

Instrukcja Zarządzania Systemem Informatycznym
służącym do przetwarzania danych osobowych
wraz z procedurami dotyczącymi cyberbezpieczeństwa i bezpieczeństwa informacji
w Urzędzie Gminy Przytyk
ul. Zachęta 57, 26-650 Przytyk

nie później niż w terminie 72 godzin od stwierdzenia naruszenia powiadamia Urząd Ochrony Danych Osobowych.

11. Zgłoszenia do UODO przekazywane są w sposób elektroniczny. Procedura zgłoszeń opisana jest pod adresem internetowym <https://uodo.gov.pl/pl/134/233>
12. IOD wraz z ASI podejmuje również działania zabezpieczające i naprawcze zmierzające do niwelowania skutków powstałych w wyniku incydentu, jak również działania zaradcze dla uniknięcia wystąpienia podobnych incydentów w przyszłości.
13. Jeżeli zgłoszony incydent naruszenia ochrony danych osobowych może spowodować wysokie ryzyko naruszenia praw lub wolności osób fizycznych, a stosowane w Urzędzie techniczne i organizacyjne środki ochrony danych nie eliminują tego ryzyka, IOD bez zbędnej zwłoki informuje ADO o konieczności zawiadomienia osób, których dane dotyczą o takim naruszeniu i przygotowuje stosowne dokumenty do podpisu
14. Jeżeli zawiadomienie osób, których dane dotyczą wymagałoby niewspółmiernie dużego wysiłku, IOD przygotowuje publiczny komunikat lub wybiera inny stosowny środek, za pomocą którego zawiadomienie zostanie tym osobom przekazane.
15. W przypadku stwierdzenia działań zamierzonych, przy jednoczesnym zidentyfikowaniu sprawcy incydentu dotyczącego naruszenia bezpieczeństwa przetwarzania danych osobowych ADO podejmuje decyzję dotyczącą wyciągnięcia ewentualnych konsekwencji dyscyplinarnych wobec sprawcy incydentu. Jednocześnie, w zależności od wagi incydentu, mogą być powiadomione organa ścigania.

IX. Zabezpieczenia infrastruktury informatycznej i telekomunikacyjnej

Zabezpieczenia odnoszą się do:

1. Technicznych środków zabezpieczenia komputerów przed skutkami awarii zasilania:
Zastosowano UPS-y dla wszystkich serwerów oraz listwy przeciwprzepięciowe dla stacji komputerowych, na których przetwarzanie polega na wprowadzaniu, modyfikacji i usuwaniu danych osobowych.
2. Opisu infrastruktury sieci informatycznej, w której użytkowane są komputery wykorzystywane do przetwarzania danych osobowych
 - 1) Komputery służące do przetwarzania danych osobowych są połączone z lokalną oraz publiczną siecią za pomocą serwera proxy.
 - 2) W przypadku, gdy zbiór danych osobowych przetwarzany jest przy użyciu komputera przenośnego, wymagane zabezpieczenia, to szyfrowanie dysku twardego.

Instrukcja Zarządzania Systemem Informatycznym
służącym do przetwarzania danych osobowych
wraz z procedurami dotyczącymi cyberbezpieczeństwa i bezpieczeństwa informacji
w Urzędzie Gminy Przytyk
ul. Zachęta 57, 26-650 Przytyk

- 3) Programy zainstalowane na komputerach obsługujących przetwarzanie danych osobowych są użytkowane z zachowaniem praw autorskich i posiadają licencje.
3. Sprzętowych i programowych środków ochrony przed nieuprawnionym dostępem do danych osobowych, w tym środków zapewniających rozliczalność wykonywanych operacji.
 - 1) Lokalizacja urządzeń komputerowych (serwerów, komputerów, drukarek) uniemożliwia osobom niepowołanym (np. klientom, pracownikom innych działów,) dostęp do nich.
 - 2) Dostęp do systemu operacyjnego komputera, w którym przetwarzane są dane osobowe zabezpieczony jest za pomocą procesu uwierzytelnienia z wykorzystaniem identyfikatora oraz hasła.
 - 3) Zastosowano systemowe mechanizmy wymuszające okresową zmianę haseł.
4. Sprzętowych i programowych środków ochrony przed szkodliwym oprogramowaniem i nieuprawnionym dostępem do przetwarzanych danych
 - 1) Zastosowano środki ochrony przed szkodliwym oprogramowaniem takim, jak np. robaki, wirusy, konie trojańskie, rootkity, inne.
 - 2) Użyto system Firewall do ochrony dostępu do sieci komputerowej.

X. Zabezpieczenia programów i baz przetwarzających dane osobowe

Opis technicznych i programowych środków bezpieczeństwa zastosowanych w procedurach, aplikacjach i programach oraz innych narzędziach programowych wykorzystywanych do przetwarzania danych osobowych.

1. Dostęp do zbioru danych osobowych (do bazy danych i do programu) wymaga uwierzytelnienia z wykorzystaniem identyfikatora oraz hasła.
2. W większości zastosowano mechanizm wymuszający okresową zmianę haseł dostępu do zbioru danych osobowych na poziomie systemu operacyjnego komputera.
3. W większości zastosowano mechanizm blokady dostępu po 5 próbach nieudanego logowania się.
4. Zastosowano systemowe środki pozwalające na określenie odpowiednich praw dostępu do zasobów informatycznych, w tym zbiorów danych osobowych dla poszczególnych użytkowników systemu informatycznego.
5. Zainstalowano wygaszacze ekranów na stanowiskach, na których przetwarzane są dane osobowe.

Instrukcja Zarządzania Systemem Informatycznym
służącym do przetwarzania danych osobowych
wraz z procedurami dotyczącymi cyberbezpieczeństwa i bezpieczeństwa informacji
w Urzędzie Gminy Przytyk
ul. Zachęta 57, 26-650 Przytyk

6. Zastosowano mechanizm automatycznej blokady dostępu do systemu informatycznego służącego do przetwarzania danych osobowych w przypadku dłuższej nieaktywności pracy użytkownika (automatyczny wygaszacz ekranu po 10 minutach).
7. Zastosowano system antywirusowy na stanowiskach, na których przetwarzane są dane osobowe.

XI. Obowiązki użytkowników systemu

1. Do podstawowych obowiązków użytkowników systemu należy przetwarzanie danych osobowych wyłącznie w celu i zakresie wynikającym z obowiązków służbowych.
2. Użytkownicy systemu zobowiązani są do podejmowania współpracy przy ustaleniu przyczyn naruszenia ochrony danych osobowych oraz usuwania skutków tych naruszeń, w tym zapobieganie ich ewentualnemu ponownemu wystąpieniu.
3. Użytkownicy systemu zobowiązani są do:
 - 1) przestrzegania opracowanych dla systemu zasad przetwarzania danych osobowych oraz procedur i instrukcji;
 - 2) uniemożliwienia dostępu lub podglądu danych osobom nieupoważnionym;
 - 3) informowania Administratora danych osobowych oraz Administratora Systemów Informatycznych o wszelkich naruszeniach, podejrzeniach naruszenia i nieprawidłowościach w sposobie przetwarzania i ochrony danych osobowych;
4. Wykonywania bez zbędnej zwłoki poleceń Administratora danych osobowych w zakresie ochrony danych osobowych, jeśli są one zgodne z przepisami prawa powszechnie obowiązującego.

XII. Procedura korzystania z Internetu

1. Użytkownik zobowiązany jest do korzystania z internetu wyłącznie w celach służbowych
2. Zabrania się zgrywania na dysk twardy komputera oraz uruchamiania jakichkolwiek programów nielegalnych. Zabrania się również zgrywania plików pobranych z niewiadomego źródła. Pliki takie powinny być ściągane tylko za każdorazową zgodą Administratora danych osobowych oraz Administratora Systemów Informatycznych i tylko w uzasadnionych przypadkach.
3. Użytkownik ponosi odpowiedzialność za szkody spowodowane przez oprogramowanie instalowane z Internetu
4. Zabrania się wchodzenia na strony, na których prezentowane są informacje o charakterze przestępczym, hackerskim, pornograficznym, lub innym zakazanym przez prawo (na

Instrukcja Zarządzania Systemem Informatycznym
służącym do przetwarzania danych osobowych
wraz z procedurami dotyczącymi cyberbezpieczeństwa i bezpieczeństwa informacji
w Urzędzie Gminy Przytyk
ul. Zachęta 57, 26-650 Przytyk

większości stron tego typu jest zainstalowane szkodliwe oprogramowanie, infekujące w sposób automatyczny system operacyjny komputera szkodliwym oprogramowaniem)

5. Nie należy w opcjach przeglądarki internetowej włączać opcji autouzupełniania formularzy i zapamiętywania haseł.
6. W przypadku korzystania z szyfrowanego połączenia przez przeglądarkę, należy zwracać uwagę na pojawienie się odpowiedniej ikonki (kłódka) oraz adresu www rozpoczynającego się frazą "https:"

XIII. Procedura korzystania z poczty elektronicznej

1. Przesyłanie danych osobowych z użyciem maila poza organizację może odbywać się tylko przez osoby do tego upoważnione
2. Użytkownicy powinni zwracać szczególną uwagę na poprawność adresu odbiorcy dokumentu.
3. Zaleca się, aby użytkownik podczas przysyłania danych osobowych mailem zawarł w treści prośbę o potwierdzenie otrzymania i zapoznania się z informacją przez adresata.
4. Nie należy otwierać załączników (plików) w mailach nadesłanych przez nieznanego nadawcę lub podejrzanych załączników nadanych przez znanego nadawcę.
5. Nie należy otwierać stron internetowych wskazanych hiperlinkami w mailach, gdyż mogą to być hiperlinki do stron zainfekowanych lub niebezpiecznych.
6. Użytkownicy nie powinni rozsyłać za pośrednictwem maila informacji o zagrożeniach dla systemu informatycznego, „łańcuszków szczęścia", itp.

XIV. Nadawanie, zmiana lub usuwanie uprawnień w systemach informatycznych

1. Pierwsze zarejestrowanie użytkownika w systemie i nadanie odpowiednich uprawnień do systemu przetwarzającego dane osobowe musi być poprzedzone złożeniem przez użytkownika oświadczenia o zachowaniu w tajemnicy danych osobowych i sposobów ich zabezpieczania oraz przetwarzaniu danych osobowych zgodnie z przepisami, a także uzyskaniem formalnego upoważnienia do przetwarzania danych osobowych – zgodnie z procedurą określoną w Rozdziale V Polityki bezpieczeństwa.
2. Po spełnieniu wymagań określonych powyżej, rejestrowanie użytkowników systemu i nadawanie uprawnień w systemach informatycznych, realizowane jest przez Administratora systemu informatycznego.

Instrukcja Zarządzania Systemem Informatycznym
służącym do przetwarzania danych osobowych
wraz z procedurami dotyczącymi cyberbezpieczeństwa i bezpieczeństwa informacji
w Urzędzie Gminy Przytyk
ul. Zachęta 57, 26-650 Przytyk

3. Szczególnie wnikliwej weryfikacji powinny podlegać wnioski dotyczące tworzenia oraz dostępu do kont uprzywilejowanych, związanych z realizacją przywilejów systemowych (administracyjnych) w systemie informatycznym, dających nieograniczone lub duże - z punktu widzenia istniejących zagrożeń, uprawnienia dostępu w stosunku do tego systemu lub przetwarzanych w nim danych osobowych.
4. Przy tworzeniu nowego konta użytkownika w systemie, Administrator systemu informatycznego nadaje mu unikalny identyfikator konta, który nie może być powtórzony dla żadnego innego użytkownika systemu przez cały okres życia tego systemu.
5. Administrator systemu informatycznego powinien przekazywać użytkownikom systemu tymczasowe hasła dostępowe w sposób bezpieczny. W tym celu powinni unikać pośrednictwa osób trzecich lub korzystania do tego celu z niechronionych wiadomości poczty elektronicznej.
6. Procedurę nadawania uprawnień do przetwarzania danych osobowych w systemach należy stosować odpowiednio, w przypadku zmiany uprawnień w systemach informatycznych lub w przypadku odebrania uprawnień w systemach.
7. Zmiany dotyczące użytkownika systemu, takie jak rozwiązanie umowy o pracę lub utrata upoważnienia, są przesłanką do natychmiastowego wyrejestrowania użytkownika z systemu informatycznego oraz unieważnienia hasła i odnotowanie tego faktu w ewidencji osób upoważnionych do przetwarzania danych osobowych.
8. W przypadku wycofania użytkownikowi systemu uprawnień do przetwarzania danych osobowych lub dostępu do systemu informatycznego przetwarzającego te dane, konto użytkownika nie podlega skasowaniu z systemu, ale skutecznemu zablokowaniu przez Administratora systemu informatycznego.
9. Prawa dostępu do danych osobowych użytkownikom, którzy nie są pracownikami etatowymi Administratora danych osobowych powinny mieć charakter czasowy i mogą być przyznawane wyłącznie na okres odpowiadający wykonywanemu zadaniu a na koniec zatwierdzone zatwierdzane.

XV. Metody i środki uwierzytelniania w systemie informatycznym

1. Mając na uwadze zagwarantowanie wysokiego poziomu bezpieczeństwa przetwarzania danych osobowych oraz zagwarantowania użytkownikom systemu rozliczalności wykonywanych przez nich operacji w systemach informatycznych, wszyscy użytkownicy przy uwierzytelnianiu do systemów informatycznych powinni stosować się do poniższych zasad:

Instrukcja Zarządzania Systemem Informatycznym
służącym do przetwarzania danych osobowych
wraz z procedurami dotyczącymi cyberbezpieczeństwa i bezpieczeństwa informacji
w Urzędzie Gminy Przytyk
ul. Zachęta 57, 26-650 Przytyk

- 1) użytkownik systemu powinien posiadać unikalny identyfikator do swojego osobistego i wyłącznego użytku;
 - 2) użytkownik systemu ponosi pełną odpowiedzialność za utworzenie hasła dostępu oraz jego przechowywanie;
 - 3) hasła nie mogą być ujawniane lub przekazywane komukolwiek, bez względu na okoliczności;
 - 4) użytkownik systemu nie powinien przechowywać haseł w widocznych miejscach, nie powinien umieszczać haseł w żadnych automatycznych procesach logowania (skryptach, makrach lub pod klawiszami funkcyjnymi).
2. Administrator systemu informatycznego jest odpowiedzialny za okresowe sprawdzanie, usuwanie lub blokowanie zbędnych identyfikatorów użytkowników systemu oraz kont w systemach.
 3. Wszystkie konta dostępowe (identyfikatory) do systemów informatycznych powinny być chronione hasłem lub innym bezpiecznym sposobem uwierzytelniania.
 4. Identyfikator użytkownika systemu powinien być niepowtarzalny a po wyrejestrowaniu się z systemu informatycznego nie powinien być przydzielany innej osobie.

XVI. Hasła w systemach informatycznych

1. Użytkownicy systemu powinni wybierać hasła dobrej jakości:
 - 1) długości co najmniej 8 znaków;
 - 2) które są łatwe do zapamiętania, a trudne do odgadnięcia;
 - 3) nie są oparte na prostych skojarzeniach, łatwych do odgadnięcia lub wywnioskowania z informacji dotyczących właściciela konta (np. imię, nazwisko, numer telefonu, data urodzenia itp.);
 - 4) w których występuje przynajmniej jedna duża litera, jedna mała litera, jedna cyfra lub znak specjalny;
 - 5) w których nie występują kolejne znaki, które nie są topologiczne (tzn. wynikające z układu klawiszy na klawiaturze, typu „qwer6”, „zaq1xsw2CDE#” itp.).
2. Hasło początkowe, które jest przydzielane przez administratora systemu informatycznego, powinno umożliwiać użytkownikowi systemu zarejestrowanie się w systemie tylko jeden raz i powinno być natychmiast zmienione przez użytkownika systemu.
3. Użytkownik systemu jest zobowiązany zmieniać hasło, w którego posiadaniu się znajduje:

Instrukcja Zarządzania Systemem Informatycznym
służącym do przetwarzania danych osobowych
wraz z procedurami dotyczącymi cyberbezpieczeństwa i bezpieczeństwa informacji
w Urzędzie Gminy Przytyk
ul. Zachęta 57, 26-650 Przytyk

- 1) okresowo, zgodnie z wymaganiami dla danego systemu informatycznego (przed upływem terminu ważności hasła);
- 2) w przypadku ujawnienia lub podejrzenia ujawnienia hasła.
4. Zmiana haseł użytkowników systemu powinna być wymuszana przez system co 30 dni, w przypadku braku wymuszenia przez system, użytkownik systemu jest zobowiązany samodzielnie zmienić hasło co 30 dni.
5. Wszelkie urządzenia sprzętowe lub programowe, które na początku posiadały hasło domyślne, powinny mieć zmienione hasło zgodnie z przyjętymi wymogami dotyczącymi formułowania haseł.
6. Należy unikać ponownego lub cyklicznego używania haseł, które już kiedyś były wykorzystywane.
7. Hasła powinny być utrzymywane w tajemnicy również po upływie ich ważności.
8. Hasła nie powinny być przechowywane oraz przesyłane w systemach w postaci jawnej.

XVII. Rozpoczęcie, zawieszenie i zakończenie pracy w systemie

1. Przed przystąpieniem do pracy z systemem informatycznym, użytkownik systemu zobowiązany jest dokonać sprawdzenia stanu urządzeń informatycznych oraz oględzin swojego stanowiska pracy, ze zwróceniem szczególnej uwagi, czy nie zaszły okoliczności wskazujące na naruszenie ochrony danych osobowych.
2. W przypadku stwierdzenia bądź podejrzenia, iż miało miejsce naruszenie ochrony danych osobowych, użytkownik systemu zobowiązany jest powiadomić o tym fakcie Administratora danych osobowych oraz Administratora systemów informatycznych.
3. Kończąc pracę, użytkownik systemu obowiązany jest do wylogowania się z systemu informatycznego i zabezpieczenia stanowiska pracy, w szczególności wszelkiej dokumentacji, wydruków oraz elektronicznych nośników informacji, na których znajdują się dane osobowe i umieszczenia ich w zamykanych szafkach.
4. Stacje robocze powinny być tak skonfigurowane, aby w przypadku nieobecności użytkownika systemu dłużej niż 10 minut uruchamiał się wygaszacz ekranu odblokowywany hasłem. Alternatywnie może obowiązywać wymaganie wylogowania się z systemu lub blokowania stacji roboczej w przypadku chwilowego opuszczenia stanowiska pracy

Instrukcja Zarządzania Systemem Informatycznym
służącym do przetwarzania danych osobowych
wraz z procedurami dotyczącymi cyberbezpieczeństwa i bezpieczeństwa informacji
w Urzędzie Gminy Przytyk
ul. Zachęta 57, 26-650 Przytyk

XVIII. Kopie zapasowe

1. Kopie zapasowe danych tworzone są przez specjalistyczne oprogramowanie zarządzane przez upoważnionego współpracownika - informatyka.
2. Kopie całościowe sporządzane są codziennie na magnetycznych nośnikach.
3. Każdy nośnik jest opisany numerem. Wszystkie są ewidencjonowane w formularzu kopii bezpieczeństwa, zgodnie z procedurami informatyka.
4. Codzienne kopie przechowywane są przez 2 tygodnie. Tygodniowe kopie przechowywane są przez 4 tygodnie. Miesięczne kopie przechowywane są przez 2 lata, a roczne kopie przez 6 lat.
5. Dostęp do kopii ma upoważniony informatyk.
6. Kopie przechowywane są na innej kondygnacji budynku niż serwerownia, połączony z budynkiem serwerowni łącznikiem.
7. ASI sprawuje nadzór nad wykonywaniem kopii zapasowych oraz weryfikuje ich poprawność.
8. Niszczenie kopii bezpieczeństwa odbywa się poprzez jej fizyczne zniszczenie.
9. Administrator systemu informatycznego odpowiedzialny za tworzenie kopii zapasowych zobowiązany jest przestrzegać terminów sporządzania kopii zapasowych oraz okresowo dokonywać kontroli możliwości odtworzenia danych zapisanych na tych kopiach pod kątem ewentualnej przydatności w sytuacji awarii systemu.

XVI. Przechowywanie nośników elektronicznych zawierających dane osobowe

1. Dane osobowe mogą być przechowywane:
 - 1) na serwerach
 - 2) na stacjach roboczych
 - 3) na wymiennych nośnikach elektronicznych.
2. Wymienne nośniki elektroniczne, o ile nie są użytkowane, powinny być przechowywane w zamykanych szafkach.
3. Okres przechowywania nośników elektronicznych zawierających dane osobowe powinien być ustalony przez osobę kierującą komórką organizacyjną, w której te dane są przetwarzane.
4. Na każdym nośniku powinna być odnotowywana data maksymalnego okresu przechowywania np. data ustania celu przetwarzania danych osobowych.
5. Nośniki elektroniczne zawierające dane osobowe, dla których cel przetwarzania ustał powinny być pozbawiane zapisu tych danych a w przypadku gdy nie jest to możliwe, należy je zniszczyć w sposób uniemożliwiający odczytanie/odzyskanie danych osobowych.

Instrukcja Zarządzania Systemem Informatycznym
służącym do przetwarzania danych osobowych
wraz z procedurami dotyczącymi cyberbezpieczeństwa i bezpieczeństwa informacji
w Urzędzie Gminy Przytyk
ul. Zachęta 57, 26-650 Przytyk

XVII. Ochrona systemu przed działaniem szkodliwego oprogramowania

1. Za zaplanowanie i zapewnienie ochrony antywirusowej odpowiada ASI, w tym za zapewnienie odpowiedniej ilości licencji dla użytkowników.
2. Na każdej stacji roboczej w sieci oraz serwerze przetwarzającym dane osobowe powinno być zainstalowane oprogramowanie antywirusowe skanujące.
3. Oprogramowanie antywirusowe powinno być zainstalowane tak, aby użytkownik systemu nie był w stanie wyłączyć lub pominąć etapu skanowania.
4. Kontrola antywirusowa powinna być przeprowadzana na wszystkich nośnikach magnetycznych i optycznych, służących zarówno do przetwarzania danych osobowych w systemie, jak i do celów instalacyjnych.
5. Nowe wersje oprogramowania antywirusowego oraz uaktualnienia bazy sygnatur wirusów wykonują się automatycznie.
6. Wyznaczone osoby mają prawo odłączyć od sieci stację roboczą, na której zostanie zlokalizowany wirus, jeśli uznają, że dalsze pozostawienie go w sieci zagraża innym stacjom roboczym.

XVIII. Funkcjonalność systemu informatycznego

1. System informatyczny służący do przetwarzania danych osobowych powinien zapewniać dla każdej osoby, której dane osobowe są przetwarzane w tym systemie — z wyjątkiem systemów służących do przetwarzania danych osobowych ograniczonych wyłącznie do edycji tekstu w celu udostępnienia go na piśmie — automatyczne odnotowywanie po zatwierdzeniu przez użytkownika systemu operacji wprowadzenia danych, informacji o dacie pierwszego wprowadzenia danych do systemu oraz o identyfikatorze osoby wprowadzającej dane.
2. W przypadku zbierania danych osobowych od osoby, której dane nie dotyczą należy zapewnić w systemie informatycznym odnotowywanie informacji o źródle pochodzenia danych. Proces ten nie musi odbywać się automatycznie.
3. Dla każdego systemu służącego do przetwarzania danych osobowych, z którego udostępniane są dane osobowe odbiorcom danych, należy zapewnić odnotowanie komu, kiedy i w jakim zakresie dane osobowe zostały udostępnione, chyba, że dane pochodzą z jawnego zbioru danych osobowych.

Instrukcja Zarządzania Systemem Informatycznym
służącym do przetwarzania danych osobowych
wraz z procedurami dotyczącymi cyberbezpieczeństwa i bezpieczeństwa informacji
w Urzędzie Gminy Przytyk
ul. Zachęta 57, 26-650 Przytyk

4. W przypadku zgłoszenia sprzeciwu, o którym mowa w art. 4 pkt 25 RODO wobec przetwarzania danych osobowych system powinien zapewniać odnotowywanie tej informacji.
5. Zabronione jest nadawanie ukrytych znaczeń elementom numerów porządkowych w aplikacjach ewidencjonujących osoby fizyczne.

XIX. Zasady monitorowania, przeglądu i konserwacji systemu

1. Za prawidłowość przeprowadzenia przeglądów, zapewnienia jakości, konserwację i dokumentowanie zmian w systemach odpowiada Administrator systemu informatycznego.
2. Przeglądy, naprawy i konserwacje systemu informatycznego, które będą przeprowadzane w miejscu użytkowania tego systemu wymagają obecności Administratora systemu informatycznego lub innej wyznaczonej osoby.
3. W przypadku gdy konieczne jest dokonanie przeglądu, naprawy lub konserwacji systemu informatycznego poza miejscem jego użytkowania, z urzędnika należy wymontować element, na którym zapisane są dane osobowe, o ile jest to możliwe. W przeciwnym wypadku należy zawrzeć z podmiotem dokonującym naprawy umowę powierzenia.
4. Osoby nie będące pracownikami, które prowadzą prace serwisowe na rzecz Administratora danych osobowych przed rozpoczęciem prac, powinny być poddane weryfikacji tożsamości przez Administratora systemu informatycznego lub inną wyznaczoną do tego celu osobę.
5. Przegląd programów i narzędzi programowych powinien być przeprowadzany w przypadku zmiany wersji oprogramowania aplikacji, zmiany wersji oprogramowania bazy danych lub wykonania zmian w projekcie systemu spowodowanych koniecznością naprawy, konserwacji lub modyfikacji systemu.

XX. Przetwarzanie danych poza obszarem przetwarzania

1. W przypadku przekazywania urządzeń lub nośników zawierających dane osobowe w tym dane wrażliwe, poza obszar przetwarzania danych osobowych, zabezpiecza się je w sposób zapewniający poufność, integralność i rozliczalność tych danych, przez co rozumie się:
 - 1) ograniczenie dostępu do danych osobowych hasłem zabezpieczającym dane przed osobami nieupoważnionymi;
 - 2) stosowanie metod kryptograficznych;
 - 3) stosowanie odpowiednich zabezpieczeń fizycznych;
 - 4) stosowanie odpowiednich zabezpieczeń organizacyjnych.

Instrukcja Zarządzania Systemem Informatycznym
służącym do przetwarzania danych osobowych
wraz z procedurami dotyczącymi cyberbezpieczeństwa i bezpieczeństwa informacji
w Urzędzie Gminy Przytyk
ul. Zachęta 57, 26-650 Przytyk

W zależności od stopnia zagrożenia zalecane jest stosowanie kombinacji wyżej wymienionych zabezpieczeń.

2. Dane osobowe przetwarzane na komputerach przenośnych powinny być zabezpieczone w sposób zapewniający poufność tych danych, w szczególności dane te powinny być zabezpieczone metodami kryptograficznymi.

XXI. Zasady komunikacji w sieci teleinformatycznej

1. Przesyłanie danych osobowych drogą teletransmisji powinno odbywać się wyłącznie przy wykorzystaniu wymaganych zabezpieczeń chroniących przed nieuprawnionym dostępem, w szczególności takich jak ochrona kryptograficzna.
2. Inne technologie sieciowe takie jak sieci lokalne oparte na falach radiowych nie mogą być wykorzystywane do przekazu informacji, o ile połączenie nie jest szyfrowane. Takie połączenia mogą być używane jedynie dla wymiany poczty elektronicznej o ile wiadomo, że nie zawiera ona danych osobowych.
3. Administrator systemu informatycznego powinien chronić system przed zagrożeniami pochodzącymi z sieci publicznej poprzez wdrożenie logicznych zabezpieczeń chroniących przed nieuprawnionym dostępem, poprzez:
 - 1) kontrolę przepływu informacji pomiędzy systemem informatycznym a siecią publiczną;
 - 2) kontrolę działań inicjowanych z sieci publicznej i systemu informatycznego.
4. Kontrola opisana powyżej powinna być dokumentowana przez osoby wykonujące te czynności.

XIX. Szkolenia

Brak wiedzy i umiejętności poprawnego rozpoznania i klasyfikacji oraz oceny poziomu istotności incydentu po stronie zgłaszającego nie może być przyczyną zaniechania powiadomienia osób odpowiedzialnych w jednostce o zaistniałym incydencie lub podejrzeniu jego wystąpienia. Dlatego w miarę posiadanych zasobów, co najmniej raz do roku należy przeprowadzać okresowe szkolenia pracowników Urzędu w zakresie zarządzania incydentami. Niezależnie od prowadzonych szkoleń wskazane jest przeprowadzanie szkolenia każdego nowo zatrudnionego pracownika celem zapewnienia znajomości zasad prawidłowego zgłaszania incydentów.

Instrukcja Zarządzania Systemem Informatycznym
służącym do przetwarzania danych osobowych
wraz z procedurami dotyczącymi cyberbezpieczeństwa i bezpieczeństwa informacji
w Urzędzie Gminy Przytyk
ul. Zachęta 57, 26-650 Przytyk

XXII. Postanowienia końcowe

1. Niezależnie od odpowiedzialności określonej w przepisach prawa powszechnie obowiązującego, naruszenie zasad określonych w niniejszej Instrukcji może być podstawą rozwiązania stosunku pracy bez wypowiedzenia z osobą, która dopuściła się naruszenia.
2. W sprawach nieuregulowanych w Instrukcji mają zastosowanie przepisy **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 (ogólne rozporządzenie o ochronie danych),
3. Użytkownicy systemu zobowiązani są do bezwzględnego stosowania przy przetwarzaniu danych osobowych postanowień zawartych w niniejszej Instrukcji, w wypadku odrębnych od zawartych w niniejszej Instrukcji uregulowań występujących w innych procedurach obowiązujących u Administratora danych, użytkownicy systemu mają obowiązek stosowania zapisów dalej idących, których stosowanie zapewni wyższy poziom ochrony danych osobowych przetwarzanych w systemie informatycznym.


Z up. WÓJTA
mgr Magdalena Komelczyk
ZASTĘPCA WÓJTA