UCHWAŁA I/5/2024
ZARZĄDU CELOWEGO ZWIĄZKU GMIN „EKO-LOGICZNI"
z dnia 21 sierpnia 2024 r.
w sprawie określenia zasad bezpieczeństwa danych osobowych w Celowym Związku Gmin „Eko-Logiczni"

Na podstawie art. 5 ust. 2, art. 24 ust. 2 oraz art. 37 ust.1 i 6 Rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (Dz.U. UE seria L 119, z dnia 4 maja 2016),

Zarząd Celowego Związku Gmin „Eko- Logiczni"
uchwala, co następuje:

§1.

Wprowadza się do stosowania w Celowym Związku Gmin „Eko-Logiczni" Politykę Bezpieczeństwa Danych Osobowych stanowiącą załącznik do niniejszej uchwały.

§2.

Zobowiązuje się:

1) członków Zgromadzenia Związku,
2) członków Zarządu Związku,
3) pracowników Biura Celowego Związku Gmin „Eko-Logiczni" ,
4) osoby zatrudnione przez Biuro Celowego Związku Gmin „Eko-Logiczni" na jakiejkolwiek innej podstawie prawnej

– do ochrony i bezpiecznego przetwarzania tych danych, zgodnie z dokumentami określonymi w §1 niniejszej uchwały.

§3.

Wykonanie uchwały powierza się Zarządowi Celowego Związku Gmin „Eko-Logiczni"

§4.

Traci moc uchwała nr IV/14/2022 Zarządu Celowego Związku Gmin „Eko- Logiczni" z dnia 9 marca 2022 r. w sprawie określenia zasad bezpieczeństwa danych osobowych w Celowym Związku Gmin „Eko- Logiczni".

§5.

Uchwała wchodzi w życie z dniem podjęcia.

Jurij Rusij
Przewodniczący Zarządu
Celowego Związku Gmin
„Eko-Logiczni"

UCHWAŁA I/5/2024
ZARZĄDU CELOWEGO ZWIĄZKU GMIN „EKO-LOGICZNI"
z dnia 21 sierpnia 2024 r.

w sprawie określenia zasad bezpieczeństwa danych osobowych w Celowym Związku Gmin „Eko-Logiczni"

Na podstawie art. 5 ust. 2, art. 24 ust. 2 oraz art. 37 ust.1 i 6 Rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (Dz.U. UE seria L 119, z dnia 4 maja 2016),

Zarząd Celowego Związku Gmin „Eko- Logiczni"
uchwala, co następuje:

§1.

Wprowadza się do stosowania w Celowym Związku Gmin „Eko-Logiczni" Politykę Bezpieczeństwa Danych Osobowych stanowiącą załącznik do niniejszej uchwały.

§2.

Zobowiązuje się:

1) członków Zgromadzenia Związku,
2) członków Zarządu Związku,
3) pracowników Biura Celowego Związku Gmin „Eko-Logiczni" ,
4) osoby zatrudnione przez Biuro Celowego Związku Gmin „Eko-Logiczni" na jakiejkolwiek innej podstawie prawnej

– do ochrony i bezpiecznego przetwarzania tych danych, zgodnie z dokumentami określonymi w §1 niniejszej uchwały.

§3.

Wykonanie uchwały powierza się Zarządowi Celowego Związku Gmin „Eko-Logiczni"

§4.

Traci moc uchwała nr IV/14/2022 Zarządu Celowego Związku Gmin „Eko- Logiczni" z dnia 9 marca 2022 r. w sprawie określenia zasad bezpieczeństwa danych osobowych w Celowym Związku Gmin „Eko- Logiczni".

§5.

Uchwała wchodzi w życie z dniem podjęcia.

Jurij Nagaj
Przewodniczący Zarządu
Celowego Związku Gmin
„Eko-Logiczni"

Załącznik nr 1
do Uchwały Nr 1/5/2024
zarządu CZG
„Eko-Logiczni"
z dnia 21 sierpnia 2024 r.

POLITYKA
BEZPIECZEŃSTWA DANYCH OSOBOWYCH
W CELOWYM ZWIĄZKU GMIN „EKO-LOGICZNI"

METRYKA DOKUMENTU

Nazwa jednostki organizacyjnej	Celowy Związek Gmin „Eko-Logiczni"		
Tytuł dokumentu	Polityka Bezpieczeństwa Danych Osobowych w Celowym Związku Gmin „Eko-Logiczni" (PBDO)		
System	System Ochrony Danych Osobowych (SODO)		
Rodzaj	Dokument wiodący		
Zastosowanie	Celowy Związek Gmin „Eko-Logiczni", Biuro Celowego Związku Gmin „Eko-Logiczni", Zgromadzenie Związku, Zarząd Związku.		
Status	Dokument finalny	Liczba stron	75

HISTORIA ZMIAN

Wersja	Data wersji	Opis zmiany	Akcja	Rozdział	Autor	Zatwierdził
1.0	9.03.2022 r.	Nie dotyczy	Ustanowienie nowej Polityki bezpieczeństwa danych osobowych	Wszystkie	Zastępca IOD	Zarząd Celowego Związku Gmin „Eko-Logiczni".

SPIS TREŚCI

Rozdział I. Postanowienia ogólne 7
Rozdział II. Definicje i skróty użyte w Polityce 8
Rozdział III. Zakresy odpowiedzialności za przetwarzanie i ochronę danych osobowych 10
Rozdział IV. Uwzględnienie ochrony danych w fazie projektowania (privacy by desing) – tworzenie nowych zbiorów danych 15
Rozdział V. Prawa i wolności osób, których dane dotyczą 17
Rozdział VI. Zasady dotyczące przetwarzania danych osobowych 23
Rozdział VII. Domyślna ochrona danych osobowych 24
Rozdział VIII. Wykaz budynków, pomieszczeń lub części pomieszczeń, tworzących obszar, w którym przetwarzane są dane osobowe 24
Rozdział IX. Rejestr Czynności Przetwarzania 24
Rozdział X. Określenie środków technicznych i organizacyjnych niezbędnych do zapewnienia poufności, integralności i rozliczalności przetwarzanych danych osobowych 25
Rozdział XI. Zarządzanie dostępem do danych osobowych 28
Rozdział XII. Udostępnianie i powierzanie danych osobowych 30
Rozdział XIII. Zarządzanie ryzykiem danych osobowych 32
Rozdział XIV. Kontrola przetwarzania i stanu zabezpieczenia danych osobowych 34
Rozdział XV. Postępowanie w przypadku stwierdzenia naruszenia bezpieczeństwa danych osobowych 35
Rozdział XVI. Postanowienia końcowe 38

SPIS ZAŁĄCZNIKÓW

Załącznik numer 1:	Wzór wniosku o utworzenie nowego zbioru danych lub czynności przetwarzania w ramach istniejącego zbioru danych
Załącznik numer 2:	Rejestr czynności przetwarzania
Załącznik numer 3:	Klauzula informacyjna – zbieranie danych od osoby
Załącznik numer 4:	Klauzula informacyjna – zbieranie danych z innych źródeł
Załącznik numer 5:	Wykaz pomieszczeń lub części pomieszczeń tworzących obszar, w którym są przetwarzane dane osobowe
Załącznik numer 6:	Ogólna Polityka Informacyjna
Załącznik numer 7:	Wzór upoważnienia do przetwarzania danych osobowych
Załącznik numer 7a	Wzór zobowiązania do zachowania w tajemnicy treści danych osobowych
Załącznik numer 8:	Wniosek o udostępnienie danych osobowych
Załącznik numer 9:	Wzór ewidencji udostępnień danych osobowych
Załącznik numer 10:	Wzór umowy powierzenia przetwarzania danych
Załącznik numer 11:	Wzór ewidencji umów powierzenia przetwarzania danych osobowych
Załącznik numer 12:	Ankieta identyfikacji ryzyk
Załącznik numer 13:	Plan postępowania z ryzykiem
Załącznik numer 14:	Rejestr ryzyk bezpieczeństwa informacji
Załącznik numer 15:	Karta oceny naruszenia/podejrzenia wystąpienia naruszenia
Załącznik numer 16:	Rejestr Naruszeń
Załącznik numer 17:	Zawiadomienie osoby fizycznej o naruszeniu
Załącznik numer 18:	Wzór zgody na przetwarzanie danych osobowych razem z klauzulą informacyjną
Załącznik numer 19:	Lista osób zapoznanych z Polityką Bezpieczeństwa Danych Osobowych

ROZDZIAŁ I.

POSTANOWIENIA OGÓLNE

1. Niniejsza „Polityka Bezpieczeństwa Danych Osobowych" zwana dalej Polityką, została opracowana w Celowym Związku Gmin „Eko-Logiczni". Polityka określa zasady i wymagania w zakresie bezpieczeństwa danych osobowych przetwarzanych w każdej firmie (zarówno tradycyjnie jak i w systemach informatycznych).

2. Polityka obejmuje swym zakresem Celowy Związek Gmin „Eko-Logiczni", w tym wszystkie jego organy oraz jednostki i komórki organizacyjne.

3. Polityka została opracowana proporcjonalnie do realizowanych w Celowym Związku Gmin „Eko-Logiczni" czynności przetwarzania w oparciu o art. 24 ust. 2 Rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych).

4. Celem Polityki jest zapewnienie powszechnego stanu, w ramach którego przetwarzanie realizowane w Celowym Związku Gmin „Eko-Logiczni":
   - odbywa się w zgodzie z Rozporządzeniem;
   - chroni prawa i wolności osób, których dane dotyczą;
   - gwarantuje stopień bezpieczeństwa odpowiadający ryzyku poszczególnych czynności przetwarzania (zabezpiecza przed przypadkowym lub niezgodnym z prawem zniszczeniem danych, utratą, modyfikacją, nieuprawnionym ujawnieniem lub nieuprawnionym dostępem do danych osobowych, które są przesyłane, przechowywane lub przetwarzane w inny sposób).

5. Dla skutecznego realizowania założeń Polityki, Celowy Związek Gmin „Eko-Logiczni" zapewnia:
   - zastosowanie rozwiązań organizacyjnych, proceduralnych i technicznych w firmie zabezpieczeń przed zagrożeniami danych osobowych;
   - prowadzenie szkoleń pracowników w zakresie zasad przetwarzania i bezpieczeństwa danych osobowych;
   - okresowe szacowanie ryzyka występujących zagrożeń dla zbiorów danych osobowych lub poszczególnych czynności przetwarzania;
   - bieżącą kontrolę i nadzór nad przetwarzaniem danych osobowych;
   - monitorowanie skuteczności zastosowanych środków ochrony danych.

ROZDZIAŁ II.

DEFINICJE I SKRÓTY UŻYTE W POLITYCE

W niniejszej Polityce następujące wyrażenia i określenia mają znaczenie zgodnie z podanymi poniżej definicjami:

1. **Administrator Danych Osobowych (Administrator, ADO)** – oznacza osobę fizyczną lub prawną, organ publiczny, jednostkę lub inny podmiot, który samodzielnie lub wspólnie z innymi ustala cele i sposoby przetwarzania danych osobowych; Celowy Związek Gmin „Eko-Logiczni" posiada status Administratora Danych Osobowych dla danych przetwarzanych w swojej bieżącej działalności. Ilekroć w Polityce będzie mowa o „ADO", „Administratorze" lub „Administratorze Danych Osobowych" należy rozumieć, że jest to Celowy Związek Gmin „Eko-Logiczni".
2. **Inspektor Ochrony Danych (IOD)** – osoba, wyznaczona przez ADO, realizuje zadania wynikające z art. 39 Rozporządzenia, polegające na informowaniu, monitorowaniu przestrzegania Rozporządzania, udzielaniu zaleceń co do oceny skutków dla ochrony danych oraz monitorowania jej wykonania, współpracy z organem nadzorczym (PUODO) oraz pełniąca funkcję punktu kontaktowego dla organu, a także realizująca inne zadania i obowiązki;
3. **Informatyk** – pracownik Administratora właściwy ds. informatyki. Szczegółowy zakres zadań wynika z Regulaminu Organizacyjnego;
4. **Pracownik** – każda osoba zatrudniona przez Administratora w jakiejkolwiek formie prawnej i upoważniona przez niego do przetwarzania danych osobowych, w szczególności pracownicy samorządowi w rozumieniu przepisów Ustawy z dnia 21 listopada 2008 r. o pracownikach samorządowych, pracownicy w rozumieniu Ustawy z dnia 26 czerwca 1974 r. - Kodeks pracy, a także zleceniobiorcy, przyjmujący, stażyści, praktykanci i wolontariusze.
5. **Dane osobowe** – oznaczają informacje o zidentyfikowanej lub możliwej do zidentyfikowania osobie fizycznej („osobie, której dane dotyczą"); możliwa do zidentyfikowania osoba fizyczna to osoba, którą można bezpośrednio lub pośrednio zidentyfikować, w szczególności na podstawie identyfikatora takiego jak imię i nazwisko, numer identyfikacyjny, dane o lokalizacji, identyfikator internetowy lub jeden bądź kilka szczególnych czynników określających fizyczną, fizjologiczną, genetyczną, psychiczną, ekonomiczną, kulturową lub społeczną tożsamość osoby fizycznej;
6. **Dane genetyczne** – oznaczają dane osobowe dotyczące odziedziczonych lub nabytych cech genetycznych osoby fizycznej, które ujawniają niepowtarzalne informacje

o fizjologii lub zdrowiu tej osoby i które wynikają w szczególności z analizy próbki biologicznej pochodzącej od tej osoby fizycznej;

7. **Dane biometryczne** – oznaczają dane osobowe, które wynikają ze specjalnego przetwarzania technicznego, dotyczą cech fizycznych, fizjologicznych lub behawioralnych osoby fizycznej oraz umożliwiają lub potwierdzają jednoznaczną identyfikację tej osoby, takie jak wizerunek twarzy lub dane daktyloskopijne;
8. **Dane dotyczące zdrowia** – oznaczają dane osobowe o zdrowiu fizycznym lub psychicznym osoby fizycznej – w tym o korzystaniu z usług opieki zdrowotnej – ujawniające informacje o stanie jej zdrowia;
9. **Naruszenie ochrony danych osobowych** – oznacza naruszenie bezpieczeństwa prowadzące do przypadkowego lub niezgodnego z prawem zniszczenia, utracenia, zmodyfikowania, nieuprawnionego ujawnienia lub nieuprawnionego dostępu do danych osobowych przesyłanych, przechowywanych lub w inny sposób przetwarzanych;
10. **Polityka** – rozumie się przez to Politykę Bezpieczeństwa Danych Osobowych w Celowym Związku Gmin „Eko-Logiczni";
11. **Komórka organizacyjna** – zgodnie ze znaczeniem przyjętym w Regulaminie Organizacyjnym.
12. **Kierownik** – zgodnie ze znaczeniem przyjętym w Regulaminie Organizacyjnym. Jeśli zaś w Polityce mowa jest o Kierowniku należy przez to rozumieć także jego zastępcę.
13. **Odbiorca danych** – oznacza osobę fizyczną lub prawną, organ publiczny, jednostkę lub inny podmiot, któremu ujawnia się dane osobowe, niezależnie od tego, czy jest stroną trzecią;
14. **Powierzenie przetwarzania danych** – zlecenie wykonania czynności przetwarzania danych podmiotowi przetwarzającemu w drodze odrębnej umowy zawartej na piśmie lub stosownego pisemnego zapisu do umowy wyłącznie w zakresie i celu w nich przewidzianym;
15. **Podmiot przetwarzający** – oznacza osobę fizyczną lub prawną, organ publiczny, jednostkę lub inny podmiot, który przetwarza dane osobowe w imieniu administratora;
16. **Przetwarzanie danych** – oznacza operację 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;
17. **Rozporządzenie/RODO** – Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku

z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (Dz.U.UE.L.2016.119.1);

18. **Zarządzanie ryzykiem** – skoordynowane działania w celu identyfikacji, minimalizacji lub eliminacji prawdopodobieństwa oraz skutków realizacji zagrożeń;

19. **Zbiór danych** – oznacza uporządkowany zestaw danych osobowych dostępnych według określonych kryteriów, niezależnie od tego, czy zestaw ten jest scentralizowany, zdecentralizowany czy rozproszony funkcjonalnie lub geograficznie;

20. **Zgoda** – osoby, której dane dotyczą oznacza dobrowolne, konkretne, świadome i jednoznaczne okazanie woli, którym osoba, której dane dotyczą, w formie oświadczenia lub wyraźnego działania potwierdzającego, przyzwala na przetwarzanie dotyczących jej danych osobowych;

ROZDZIAŁ III.

ZAKRESY ODPOWIEDZIALNOŚCI ZA PRZETWARZANIE I OCHRONĘ DANYCH OSOBOWYCH

1. Postanowienia ogólne

Za przetwarzanie danych osobowych oraz ich ochronę zgodnie z postanowieniami Rozporządzenia oraz Polityki Bezpieczeństwa Danych Osobowych odpowiadają:

1.1. Administrator Danych Osobowych lub osoba działająca w jego imieniu (ADO);

1.2. Inspektor Ochrony Danych (IOD);

1.3. Informatyk;

1.4. Każdy pracownik Administratora;

1.5. Członkowie Zarządu i Zgromadzenie.

2. Administrator Danych Osobowych

2.1. Administratorem Danych Osobowych jest Celowy Związek Gmin „Eko-Logiczni" w imieniu, którego kompetencje Administratora wypełnia Zarząd Związku.

2.2. W imieniu ADO obowiązki określone w Rozporządzeniu pełni Zarząd Związku – w przedmiocie podejmowania samodzielnych decyzji o celach i sposobach przetwarzania danych osobowych.

Do obowiązków Administratora należy:

- Ustanowienie i bieżąca aktualizacja odpowiednio do celów i zakresu przetwarzanych danych osobowych – polityki bezpieczeństwa i procedur zarządzania tym bezpieczeństwem.
- Nadzorowanie wdrożenia i stosowania środków przewidzianych w ustanowionej Polityce Bezpieczeństwa Danych Osobowych.
- Zapewnienie odpowiednich relacji z podmiotem, któremu powierzono przetwarzanie danych lub z osobą, której dane dotyczą.
- Zapewnienie właściwego i niezwłocznego włączania IOD we wszystkie sprawy dotyczące ochrony danych osobowych.

3. Inspektor Ochrony Danych (IOD)

3.1. IOD po przeprowadzeniu oceny (przeprowadzonej na podstawie aktu wydanego przez Grupę Roboczą art. 29: „Wytyczne dotyczące Inspektorów Ochrony Danych" z dnia 13 grudnia 2016 r., WP 243, rev. 01) został wyznaczony przez ADO na podstawie art. 37 ust. 1 lit. c Rozporządzenia i podlega bezpośrednio Administratorowi.

3.2. IOD realizuje następujące zadania przewidziane przez Rozporządzenie:

3.2.1. informuje ADO oraz pracowników, którzy przetwarzają dane osobowe, o obowiązkach spoczywających na nich na mocy Rozporządzenia oraz innych przepisów o ochronie danych, a także doradza im w tej sprawie;

3.2.2. monitoruje przestrzeganie Rozporządzenia, innych przepisów o ochronie danych oraz niniejszej Polityki Bezpieczeństwa Danych Osobowych,

3.2.3. prowadzi działania zwiększające świadomość, szkolenia personelu uczestniczącego w operacjach przetwarzania oraz powiązane z tym audyty;

3.2.4. udziela na żądanie zaleceń co do oceny skutków dla ochrony danych oraz monitoruje jej wykonanie zgodnie z art. 35 Rozporządzenia;

3.2.5. współpracuje z organem nadzorczym;

3.2.6. pełnieni funkcję punktu kontaktowego dla organu nadzorczego w kwestiach związanych z przetwarzaniem, w tym z uprzednimi konsultacjami, o których mowa w art. 36 Rozporządzenia,

3.2.7. w stosownych przypadkach prowadzi konsultacje we wszelkich innych sprawach;

3.2.8. oraz inne zadania i obowiązki wyznaczone przez ADO, w warunkach w których te zadania i obowiązki nie powodują konfliktu interesów.

3.3. IOD jest osobą, wyznaczoną na podstawie posiadanych kwalifikacji zawodowych, a w szczególności wiedzy fachowej na temat prawa i praktyk w dziedzinie ochrony danych oraz umiejętności wypełnienia zadań, o których mowa w art. 39 Rozporządzenia.

3.4. IOD w zakresie swych czynności dotyczących ochrony danych osobowych posiada wyznaczony zakres czynności oraz stosowne uprawnienia udzielone przez Administratora do wydawania poleceń wszystkim użytkownikom systemów informatycznych oraz pracownikom przetwarzającym dane osobowe w systemach tradycyjnych, obejmujące wymagania wynikające z przepisów prawa oraz z zatwierdzonych przez ADO dokumentów systemu ochrony danych osobowych, tj. Polityki Bezpieczeństwa Danych Osobowych.

3.5. ADO zobowiązany jest zgłosić IOD do rejestracji lub wykreślić z rejestru prowadzonego przez organ nadzorczy, tj. Prezesa Urzędu Ochrony Danych Osobowych.

3.6. ADO korzystając z uprawnienia z art. 38 ust. 6 Rozporządzenia określa inne zadania i obowiązki IOD, do których w szczególności należą:

3.6.1. Nadzór nad treścią Polityki Bezpieczeństwa Danych Osobowych oraz innych dokumentów związanych z ochroną danych osobowych stosowanych przez Administratora oraz ich aktualizacji.

3.6.2. Prowadzenie i bieżące aktualizowanie Rejestru Czynności Przetwarzania (w oparciu o informacje własne lub przekazane przez pozostałych pracowników Administratora).

3.6.3. Udział w kontrolach prowadzonych przez Organ Nadzorczy.

3.6.4. Informowanie Administratora o prowadzonej przez Organ Nadzorczy kontroli i jej wynikach.

3.6.5. Przedstawianie Administratorowi uwag i zastrzeżeń dotyczących przeprowadzonych przez organ kontroli oraz przedkładanie opinii w sprawie zatwierdzenia protokołu kontroli.

3.6.6. Podejmowanie odpowiednich działań w przypadku wykrycia naruszeń bezpieczeństwa danych osobowych;

3.6.7. Inicjowanie i nadzór nad wdrażaniem nowych narzędzi, procedur organizacyjnych oraz sposobów zarządzania systemami informatycznymi, które prowadzą do wzmocnienia bezpieczeństwa przy przetwarzaniu danych osobowych.

3.6.8. Monitorowanie działania i skuteczności zabezpieczeń wdrożonych w celu ochrony danych osobowych.

3.6.9. Nadzór nad działaniami Informatyka w zakresie realizowanych obowiązków dotyczących ochrony danych osobowych.

3.6.10. Nadzorowanie i realizacja procesu nadawania upoważnień pracownikom Administratora do przetwarzania danych osobowych.

3.6.11. Nadzorowanie i organizacja realizacji obowiązku informacyjnego.

3.6.12. Nadzór nad fizycznym zabezpieczeniem obszarów, w których przetwarzane są dane osobowe.

3.6.13. Opiniowanie w sprawie udostępniania danych osobowych odbiorcom danych.

3.6.14. Opiniowanie umów dotyczących powierzenia przetwarzania danych osobowych podmiotom przetwarzającym.

3.6.15. Wydawanie pisemnych zaleceń wszelkim osobom przetwarzającym dane osobowe celem przetwarzania ich zgodnie Rozporządzeniem oraz Polityką Bezpieczeństwa Danych Osobowych.

3.6.16. Opracowywanie planu kontroli lub audytów w zakresie ochrony danych osobowych przetwarzanych przez Administratora.

4. Informatyk

4.1. Podlega bezpośrednio IOD w zakresie bezpieczeństwa danych osobowych przetwarzanych w systemach informatycznych. Jest odpowiedzialny za bieżące funkcjonowanie systemów i sieci teleinformatycznych, za przestrzeganie zasad i wymagań bezpieczeństwa systemów i sieci, oraz za ochronę przetwarzanych w nich danych osobowych. Odpowiada za zadania wynikające z regulaminu organizacyjnego, tj.:

4.1.1. koordynowanie prac związanych z komputeryzacją jednostek organizacyjnych Administratora,

4.1.2. analiza stanu informatycznego jednostek organizacyjnych Administratora oraz opracowywanie raportów o stanie informatyki,

4.1.3. przygotowywanie wniosków oraz opiniowanie propozycji zakupu sprzętu i oprogramowania,

4.1.4. wdrażanie, rozpowszechnianie i administrowanie systemów i programów komputerowych,

4.1.5. administrowanie siecią komputerową,

4.1.6. archiwizacja danych komputerowych,

4.1.7. przygotowanie i aktualizacja strony internetowej Administratora,

4.1.8. administrowanie monitoringu,

4.1.9. wprowadzanie informacji i obsługa biuletynu informacji publicznej.

4.2. Ponadto Informatyk odpowiada za:

4.2.1. Opracowywanie projektów szczególnych wymagań bezpieczeństwa CZG „Eko-Logiczni" dla poszczególnych systemów i sieci teleinformatycznych oraz przedstawianie propozycji ich uaktualnienia.

4.2.2. Wdrażanie procedur bezpieczeństwa oraz nadzór nad funkcjonowaniem systemów i sieci teleinformatycznej.

4.2.3. Wdrażanie procedur ochrony antywirusowej oraz prowadzi profilaktykę antywirusową.

4.2.4. Opracowanie planów awaryjnych i planu napraw systemów i sieci teleinformatycznej.

4.2.5. Informowanie IOD (oraz ADO w przypadkach szczególnie istotnych dla bezpieczeństwa przetwarzanych danych) o stwierdzonych: incydentach bezpieczeństwa w zakresie funkcjonowania systemów i sieci teleinformatycznych, wykrytych podatnościach i zagrożeniach dla bezpieczeństwa informacji, bieżące prowadzenie ich ewidencji.

4.2.6. Proponowanie zmian mających na celu poprawę bezpieczeństwa systemów i sieci teleinformatycznej.

4.2.7. Systematyczne wykonywanie kopii bezpieczeństwa i kopii archiwalnych baz danych i zbiorów danych osobowych zgodnie z ustalonym planem.

4.2.8. W przypadku współpracy z zewnętrzną firmą informatyczną organizuje i nadzoruje pracę przedstawicieli tych firm, dba o przestrzeganie wymaganych zasad bezpieczeństwa.

4.2.9. Dbanie o bezpieczeństwo oraz prawidłowe funkcjonowanie systemów informatycznych.

4.2.10. Utrzymywanie i aktualizowanie list autoryzowanych użytkowników systemu komputerowego uprawnionych do przetwarzania danych osobowych.

4.2.11. Prowadzenie nadzoru sprzętu oraz oprogramowania pod kątem kontroli nieuprawnionych zmian ich konfiguracji.

4.2.12. Dokonywanie analizy zgłoszonych przypadków incydentów infekcji wirusowych lub innych, wskazujących na nieautoryzowane próby ingerencji w systemie bezpieczeństwa oraz, w zależności od stopnia zagrożenia funkcjonowania systemu bezpieczeństwa, podejmowanie odpowiednich kroków zaradczych zapewnienie strategii, uregulowań, instrukcji i procedur bezpieczeństwa.

4.2.13. Zabezpieczanie niszczenia nośników zgodnie z obowiązującymi procedurami.

4.2.14. Doskonalenie z zakresu wiedzy o bezpieczeństwie systemów informatycznych.

5. Pracownicy Administratora

5.1. Każdy pracownik zobowiązany jest do ochrony danych osobowych w sposób zgodny z przepisami Rozporządzenia oraz Polityki Bezpieczeństwa Danych Osobowych.

5.2. Dostęp do określonego zbioru danych osobowych oraz do wykonywania określonych czynności przetwarzania pracownik uzyskuje na podstawie pisemnego upoważnienia.

5.3. Pracownicy zobowiązani są do zachowania w tajemnicy danych osobowych oraz sposobów ich zabezpieczenia. Obowiązek ten istnieje także po ustaniu zatrudnienia.

5.4. Naruszenie obowiązku ochrony danych osobowych, a w szczególności obowiązku zachowania danych osobowych w tajemnicy, stanowi ciężkie naruszenie obowiązków pracowniczych i może być podstawą rozwiązania stosunku pracy w trybie art. 52 Kodeksu Pracy.

5.5. Każdy pracownik zobowiązany jest zapoznać się z obowiązującymi przepisami ochrony danych osobowych i bezpieczeństwa informacji zawartymi w Polityce Bezpieczeństwa Danych Osobowych – Celowego Związku Gmin „Ekologicani" oraz potwierdzić to swoim podpisem na liście osób zapoznanych z PBDO stanowiącej załącznik numer 18 do Polityki.

ROZDZIAŁ IV.

UWZGLĘDNIENIE OCHRONY DANYCH W FAZIE PROJEKTOWANIA (PRIVACY BY DESING) – TWORZENIE NOWYCH ZBIORÓW DANYCH

1. Zasady dotyczące zbierania i przetwarzania danych osobowych określone w tym rozdziale obowiązują dla sytuacji tworzenia nowych zbiorów danych osobowych lub nowych czynności przetwarzania w ramach zbioru.

2. Uprawnienie do podejmowania decyzji w sprawie tworzenia nowych zbiorów danych osobowych lub nowych czynności przetwarzania w ramach zbioru przysługuje wyłącznie Administratorowi.

3. Administrator może upoważnić pracowników do wydawania decyzji w sprawie utworzenia nowego zbioru danych lub czynności przetwarzania w ramach zbioru.

   3.1. Każda decyzja o utworzeniu nowego procesu przetwarzania danych osobowych oraz doborze odpowiednich środków technicznych i organizacyjnych (wprowadzonych w celu skutecznej realizacji zasad ochrony danych, spełnienia wymogów RODO oraz ochrony praw osób, których dane dotyczą) poprzedzona jest procesem zarządzania ryzykiem, w ramach którego uwzględnia się:

      3.1.1. stan wiedzy technicznej,
      3.1.2. koszt wdrożenia,
      3.1.3. charakter, zakres, kontekst i cele przetwarzania danych,
      3.1.4. ryzyko naruszenia praw lub wolności osób fizycznych o różnym prawdopodobieństwie wystąpienia i wadze zagrożenia.

4. Pracownicy wnioskują na piśmie do Administratora o podjęcie decyzji w sprawie utworzenia nowego zbioru danych lub czynności przetwarzania w ramach istniejącego zbioru. Wzór wniosku stanowi załącznik numer 1 do Polityki.
   4.1. Wniosek wymaga uzyskania uprzedniej pisemnej opinii IOD dotyczącej możliwości zbierania i utworzenia zbioru danych osobowych.
   4.2. IOD w szczególności rozstrzyga o formie i trybie wykonania obowiązku informacyjnego oraz o kwestii konieczności przeprowadzenia oceny skutków dla ochrony danych.
   4.3. Opinia wydawana jest możliwie jak najszybciej, jednak nie dłużej niż w terminie 14 dni od daty otrzymania zapytania wraz z informacjami, określonymi w pkt. 5 niniejszego Rozdziału.
5. Osoby wnioskujące do Administratora w sprawie utworzenia nowego zbioru danych lub czynności przetwarzania w ramach zbioru, w terminie 30 dni przed rozpoczęciem procesu zbierania danych osobowych i utworzeniu nowego zbioru zgłaszają swój zamiar IOD, podając jednocześnie informacje dotyczące:
   5.1. Nazwy zbioru oraz/lub nazwy czynności przetwarzania.
   5.2. Formy prowadzenia zbioru (papierowa czy elektroniczna).
   5.3. Istniejących w momencie składania wniosku regulacji wewnętrznych, które będą odnosić się do tworzonego zbioru.
   5.4. Podstawy prawnej zbierania danych lub pozostałych dopuszczeń określonych w art. 6 Rozporządzenia.
   5.5. Zakresu zbieranych danych (z zaznaczeniem czy przetwarzane będą szczególne kategorie danych lub dane biometryczne lub dane genetyczne).
   5.6. Celu zbierania danych.
   5.7. Podmiotu zbierającego dane.
   5.8. Źródle pochodzenia danych (od osoby lub z innych źródeł).
   5.9. Zamiaru udostępniania lub powierzania przetwarzania danych na zewnątrz z oznaczeniem podmiotów przetwarzających lub odbiorców danych.
   5.10. Wykazu stosowanych środków i mechanizmów zabezpieczeń.
   5.11. Infrastruktury systemu informatycznego służącego do przetwarzania danych osobowych.
   5.12. Obszaru przetwarzania danych osobowych.
   5.13. Przewidywanego terminu usunięcia danych.
   5.14. Ewentualnego przekazania danych osobowych do odbiorców z państw trzecich (z udokumentowaniem odpowiednich zabezpieczeń).
6. Osoby podejmujące decyzję o utworzeniu zbioru danych osobowych zobowiązane są do uwzględnienia opinii IOD i wynikających z niej wskazań i zaleceń w opiniowanych przez niego kwestiach.

7. W momencie utworzenia nowego zbioru danych osobowych lub czynności przetwarzania w ramach zbioru informację na ten temat IOD odnotowuje w Rejestrze Czynności Przetwarzania, który stanowi załącznik numer 2 do Polityki.

ROZDZIAŁ V.

PRAWA I WOLNOŚCI OSÓB, KTÓRYCH DANE DOTYCZĄ

1. Osobom fizycznym, których dane przetwarza Administrator, przysługują uprawnienia do:
   1.1. uzyskania informacji na temat przetwarzania jej danych osobowych w momencie ich pozyskania (bezpośrednio od osoby jak i z innych źródeł),
   1.2. dostępu do danych, które jej dotyczą,
   1.3. sprostowania danych, które jej dotyczą,
   1.4. usunięcia danych, które jej dotyczą (tzw. prawo do bycia zapomnianym),
   1.5. ograniczenia przetwarzania,
   1.6. uzyskania informacji o usunięcie danych lub ich sprostowaniu,
   1.7. przenoszenia danych,
   1.8. sprzeciwu względem dalszego przetwarzania danych,
   1.9. nie podlegania decyzji Administratora, która opiera się wyłącznie na zautomatyzowanym przetwarzaniu, w tym profilowaniu, a która decyzja wywołuje wobec osoby skutki prawne lub w podobny sposób istotnie wpływa na osobę.
2. Przed zrealizowaniem żądania osoby uprawnionej:
   2.1. Jeżeli osobą przyjmującą wniosek lub żądanie osoby, której dane dotyczą, jest Administrator, przypisuje on dany wniosek lub żądanie do IOD, który po rozpoznaniu przekazuje informację zwrotną o dalszym sposobie postępowania.
   2.2. Jeżeli wniosek lub żądanie osoby, której dane dotyczą trafia bezpośrednio do pracownika, ten niezwłocznie przekazuje informację o wpływie wniosku lub żądania do IOD. Brak przekazania wniosku lub żądania osoby, której dane dotyczą jest podstawą poniesienia przez pracownika odpowiedzialności dyscyplinarnej.
   2.3. Pracownicy obsługujący wniosek lub żądanie podejmują działania zmierzające do potwierdzenia tożsamości osoby składającej żądanie. Żądanie to wymaga udokumentowania.
   2.4. Uwierzytelnienie osoby, której dane dotyczą polega na uzyskaniu: imienia i nazwiska oraz okoliczności związanej ze sprawą wnioskującego. Środkiem uwierzytelnienia bez względu na kategorię osób może być adres e-mail zwyczajowo wykorzystywany do kontaktów z osobą, której dane dotyczą.

2.5. Jeżeli pracownik w dalszym ciągu ma uzasadnione wątpliwości co do tożsamości osoby składającej żądanie w przedmiocie realizacji uprawnień, może zażądać dodatkowych informacji niezbędnych do potwierdzenia tożsamości osoby, której dane dotyczą.

3. Ogólne zasady informowania i komunikacji z osobami, których dane dotyczą:

3.1. Administrator o realizacji uprawnień przysługujących osobie, której dane są przetwarzane każdorazowo informuje na piśmie (w formie tradycyjnej lub elektronicznej);

3.2. Administrator w miarę możliwości ułatwia osobie, której dane dotyczą, wykonywanie przysługujących jej praw;

3.3. Administrator odmawia osobie wykonania praw jej przysługujących jedynie w sytuacji, w której nie jest w stanie zidentyfikować osoby, której dane dotyczą;

3.4. bez zbędnej zwłoki lub w terminie miesiąca od otrzymania żądania Administrator informuje osobę o działaniach podjętych w związku z otrzymanym żądaniem;

3.5. Administrator ma możliwość przedłużenia terminu o kolejne dwa miesiące w przypadku żądania o skomplikowanym charakterze lub dużej liczby żądań – co wymaga poinformowania w ramach odrębnego pisma;

3.6. jeżeli Administrator nie może podjąć działań w związku z otrzymanym żądaniem osoby, najpóźniej w terminie 1 miesiąca od otrzymania żądania, informuje o powodach niepodjęcia działań oraz o możliwości wniesienia skargi do organu nadzorczego oraz o możliwości skorzystania ze środków ochrony prawnej przed sądem;

3.7. realizacja uprawnień przysługujących osobie, której dane dotyczą jest wolna od opłat, chyba że żądania osoby są ewidentnie nieuzasadnione lub nadmierne (ze względu na ustawiczny charakter). W takim wypadku Administrator może pobrać rozsądną opłatę lub odmówić podjęcia działań w związku z żądaniem. Na Administratorze spoczywa obowiązek wykazania, że żądanie osoby miało ewidentnie nieuzasadniony lub nadmierny charakter.

4. Informacje podawane w przypadku zbierania danych od osoby, której dane dotyczą:

4.1. pracownicy poszczególnych komórek organizacyjnych w momencie w którym dochodzi do pierwszego utrwalenia informacji o osobie, której dane dotyczą, dołączają do treści uzupełnianych przez tę osobę formularzy tzw. klauzule informacyjne;

4.2. w przypadku korespondencyjnej obsługi spraw osoby, której dane dotyczą, udostępnienie klauzul informacyjnych następuje w pierwszym piśmie stanowiącym odpowiedź na złożony wniosek;

4.3. klauzule informacyjne są opracowywane przez pracowników zgodnie z załącznikiem numer 3 do Polityki: „Klauzula informacyjna – zbieranie danych od osoby";

4.4. informacje potrzebne do zasilenia klauzuli informacyjnej odpowiednimi danymi pracownicy pobierają z Rejestru Czynności Przetwarzania, który stanowi załącznik numer 2 do niniejszej Polityki;

4.5. Administrator dodatkowo realizuje ogólną politykę informacyjną przez swoją stronę internetową oraz Biuletyn Informacji Publicznej zgodnie z załącznikiem numer 6 do Polityki: „Ogólna polityka Informacyjna".

5. Informacje podawane w przypadku pozyskiwania danych osobowych w sposób inny niż od osoby, której dane dotyczą:

5.1. w sytuacji kiedy pracownicy poszczególnych komórek organizacyjnych pozyskają informacje dotyczące osoby z innych źródeł, są zobowiązani do przekazania tej osobie w nieprzekraczalnym terminie do 30 dni tzw. klauzulę informacyjną,

5.2. klauzula informacyjna jest opracowywana przez pracowników zgodnie z załącznikiem numer 4 do Polityki: „Klauzula informacyjna – zbieranie danych z innych źródeł",

5.3. informacje potrzebne do zasilenia klauzuli informacyjnej odpowiednimi danymi pracownicy pobierają z Rejestru Czynności Przetwarzania, który stanowi załącznik numer 2 do niniejszej Polityki.

6. Prawo dostępu do danych, przysługujące osobie której dane dotyczą:

6.1. Administrator umożliwia osobom, których dane dotyczą uzyskanie dostępu do ich danych,

6.2. Administrator na żądanie osoby udziela potwierdzenia/zaprzecza, czy przetwarzane są dane osoby składającej żądanie,

6.3. Administrator na żądanie osoby udziela informacji o: celu przetwarzania, kategoriach danych osobowych, odbiorcach lub kategoriach odbiorców danych, planowany okres przechowywania danych osobowych (oraz o ile to możliwe: kryteria ustalenia tego okresu), prawie wniesienia skargi do organu nadzorczego, źródle danych, zautomatyzowanym podejmowaniu decyzji/profilowaniu, stosowanych zabezpieczeniach w przypadku przekazywania danych osobowych do państwa trzeciego,

6.4. Administrator na żądanie osoby dostarcza kopię danych osobowych, które podlegały przetwarzaniu. Udostępnienie pierwszej kopii danych jest wolne od opłat, natomiast za każde kolejne Administrator może pobrać opłatę administracyjną.

6.5. Prawo uzyskania kopii danych nie może wpływać niekorzystnie na prawa i wolności innych osób. Wymaga się aby kopia danych przekazana do

udostępnienia była wolna od danych osób trzecich (np. poprzez anonimizację lub zaciemnienie kopii).

7. Prawo do sprostowania danych:

   7.1. Administrator na żądanie osoby, której dane dotyczą umożliwia niezwłoczne sprostowanie danych, które nie są prawidłowe,

   7.2. Administrator na żądanie osoby, której dane dotyczą umożliwia uzupełnienie niekompletnych danych osobowych,

   7.3. IOD informuję każdego odbiorcę danych, któremu uprzednio przekazano dane objęte sprostowaniem lub uzupełnieniem. IOD na żądanie osoby informuje o tych odbiorcach.

8. Prawo do usunięcia danych („prawo do bycia zapomnianym"):

   8.1. Administrator umożliwia na żądanie osoby, której dane dotyczą usunięcie jej danych bez zbędnej zwłoki w następujących przypadkach:

      8.1.1. ustał cel dla którego przetwarzanie danych było niezbędne,

      8.1.2. osoba wycofała zgodę na której opiera się przetwarzanie danych przez Administratora i brak jest innej podstawy prawnej przetwarzania,

      8.1.3. osoba, której dane dotyczą wniosła sprzeciw co do dalszego przetwarzania a Administrator nie wykaże nadrzędnych prawnie uzasadnionych podstaw przetwarzania,

      8.1.4. dane osobowe były przetwarzane niezgodnie z prawem,

      8.1.5. dane osobowe muszą zostać usunięte ze względu na przewidziany w unijnym lub krajowym porządku prawnym obowiązek,

      8.1.6. dane osobowe zostały zebrane w związku z oferowaniem usług społeczeństwa informacyjnego (tj. świadczenie usług drogą elektroniczną).

   8.2. Administrator odmówi spełnienia żądania usunięcia danych w zakresie w jakim przetwarzanie jest niezbędne:

      8.2.1. do korzystania z prawa do wolności wypowiedzi i informacji,

      8.2.2. do wywiązania się z prawnego obowiązku wymagającego przetwarzania na mocy prawa Unii lub prawa państwa członkowskiego, któremu podlega Administrator,

      8.2.3. do ustalenia, dochodzenia lub obrony roszczeń.

   8.3. IOD informuje każdego odbiorcę danych, któremu uprzednio przekazano dane o wniesionym żądaniu usunięcia danych. IOD na żądanie osoby informuje o tych odbiorcach.

9. Prawo do ograniczenia przetwarzania:

9.1. Administrator umożliwia na żądanie osoby, której dane dotyczą ograniczenie przetwarzanie jej danych w następujących przypadkach:

9.1.1. zakwestionowano prawidłowość danych osoby (ograniczenie przetwarzania trwa przez czas pozwalający sprawdzić prawidłowość danych),

9.1.2. przetwarzanie danych jest niezgodne z prawem, a osoba której dane dotyczą, sprzeciwia się usunięciu danych żądając w zamian ograniczenia ich wykorzystywania,

9.1.3. Administrator nie potrzebuje już danych osobowych do przyjętych celów przetwarzania, ale są one potrzebne osobie, której dane dotyczą do ustalenia, dochodzenia lub obrony roszczeń,

9.1.4. osoba, której dane dotyczą wniosła sprzeciw wobec przetwarzania (ograniczenie przetwarzania trwa do czasu wyjaśnienia czy prawnie uzasadnione podstawy występujące po stronie Administratora są nadrzędne wobec podstaw sprzeciwu osoby).

9.2. Uznanie przez Administratora żądania osoby, której dane dotyczą w przedmiocie ograniczenia przetwarzania powoduje, że przez czas trwania ograniczenia jedyną dopuszczalną formą przetwarzania danych przez Administratora jest ich przechowywanie. Dane przeznaczone do ograniczonego przetwarzania zostają stosownie oznakowane klauzulą „ograniczone przetwarzanie".

9.3. Dane osobowe względem, których przetwarzanie zostało ograniczone wyłącznie w przypadku:

9.3.1. zgody osoby, której dane dotyczą;

9.3.2. ustalenia, dochodzenia lub obrony roszczeń;

9.3.3. ochrony praw innej osoby fizycznej lub prawnej (z uwagi na ważne względu interesu publicznego UE lub państwa członkowskiego),

mogą być przetwarzane w zakresie szerszym niż wyłącznie przechowywanie.

9.4. Zanim Administrator podejmie decyzję o uchyleniu ograniczenia przetwarzania, informuje się o tym osobę, która zażądała ograniczenia.

9.5. Administrator informuje każdego odbiorcę danych, któremu uprzednio przekazano dane o wniesionym żądaniu ograniczenia przetwarzania danych. Administrator na żądanie osoby informuje ją o tych odbiorcach.

10. Prawo do przenoszenia danych:

10.1. IOD przekazuje na żądanie osoby zestaw jej danych osobowych (w ustrukturyzowanym, powszechnie używanym formacie nadającym się do odczytu maszynowego, np. pliki txt, xml, doc), który uprzednio dostarczyła.

Administrator nie utrudnia/nie uniemożliwia przesyłania przekazanego zestawu danych osobie, której dane dotyczą innemu administratorowi.

10.2. Administrator na żądanie osoby, której dane dotyczą, może przekazać zestaw danych bezpośrednio innemu administratorowi – o ile jest to techniczne możliwe.

10.3. Realizacja prawa do przenoszenia danych jest możliwa jeżeli: przetwarzanie odbywa się na podstawie zgody lub na podstawie umowy; przetwarzanie odbywa się w sposób zautomatyzowany.

10.4. Skorzystanie przez osobę z prawa do przenoszenia danych nie niweluje możliwości skorzystania z prawa do usunięcia danych (prawo do bycia zapomnianym).

10.5. Realizacja prawa do przenoszenia danych nie może niekorzystnie wpływać na prawa i wolności innych osób – tym samym jest to przesłanka do odmowy realizacji prawa do przenoszenia danych.

11. Prawo do sprzeciwu:
    11.1. Umożliwia się osobom, których dane dotyczą, wniesienie sprzeciwu co do dalszego przetwarzania jej danych oraz respektuje się to uprawnienie w sytuacji kiedy podstawą prawną przetwarzania danych jest prawnie uzasadniony interes realizowany przez ADO.
    11.2. W momencie wniesienia zasadnego sprzeciwu nie wolno już przetwarzać danych osobowych objętych sprzeciwem. Wyjątkiem od tej sytuacji jest wykazanie przez ADO ważnych, prawnie uzasadnionych podstaw do przetwarzania – nadrzędnych względem interesów, praw i wolności osoby, której dane dotyczą; lub wykazanie podstaw do ustalenia, dochodzenia lub obrony roszczeń.
12. Zautomatyzowane podejmowanie decyzji w indywidualnych przypadkach/profilowanie: Administrator nie podejmuje decyzji w indywidualnych przypadkach w sposób zautomatyzowany – dotyczy to również profilowania.

ROZDZIAŁ VI.

ZASADY DOTYCZĄCE PRZETWARZANIA DANYCH OSOBOWYCH

1. Zgodnie z Rozporządzeniem Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych) Administrator Danych Osobowych musi wykazać, że przetwarzane przez niego dane są:
    1.1. przetwarzane zgodnie z prawem, rzetelnie i w sposób przejrzysty dla osoby, której dane dotyczą;
    1.2. zbierane w konkretnych, wyraźnych i prawnie uzasadnionych celach i nieprzetwarzane dalej w sposób niezgodny z tymi celami;
    1.3. adekwatne, stosowne oraz ograniczone do tego, co niezbędne do celów, w których są przetwarzane
    1.4. prawidłowe i w razie potrzeby uaktualniane; należy podjąć wszelkie rozsądne działania, aby dane osobowe, które są nieprawidłowe w świetle celów ich przetwarzania, zostały niezwłocznie usunięte lub sprostowane;
    1.5. przechowywane w formie umożliwiającej identyfikację osoby, której dane dotyczą, przez okres nie dłuższy, niż jest to niezbędne do celów, w których dane te są przetwarzane;
    1.6. przetwarzane w sposób zapewniający odpowiednie bezpieczeństwo danych osobowych, w tym ochronę przed niedozwolonym lub niezgodnym z prawem

przetwarzaniem oraz przypadkową utratą, zniszczeniem lub uszkodzeniem, za pomocą odpowiednich środków technicznych lub organizacyjnych.

ROZDZIAŁ VII.

DOMYŚLNA OCHRONA DANYCH OSOBOWYCH

1. Zasada domyślnej ochrony danych jest realizowana poprzez:
   1.1. wdrażanie odpowiednich środków technicznych i organizacyjnych w ten sposób aby domyślnie przetwarzane były wyłącznie te dane osobowe, które są niezbędne dla osiągnięcia każdego konkretnego celu przetwarzania – co zostało zapewnione w ramach Rejestru Czynności Przetwarzania. Niezbędność danych odnosi się do ilości danych, zakresu, okresu przechowywania oraz ich dostępności.
   1.2. wdrażanie odpowiednich środków technicznych i organizacyjnych zapewniających aby dane osobowe nie były udostępniane nieokreślonej liczbie osób fizycznych.

ROZDZIAŁ VIII.

WYKAZ BUDYNKÓW, POMIESZCZEŃ LUB CZĘŚCI POMIESZCZEŃ, TWORZĄCYCH OBSZAR, W KTÓRYM PRZETWARZANE SĄ DANE OSOBOWE

Zidentyfikowane zbiory zawierające dane osobowe w wersji papierowej i elektronicznej są przetwarzane i przechowywane w budynkach należących do Administratora, mieszczących się w poniższych lokalizacjach:

1. Siedziba Administratora: 36-030 Błażowa, ul. Armii Krajowej 42a

Szczegółowy wykaz komórek organizacyjnych i pomieszczeń poszczególnych obiektów tworzących obszar dla zbiorów, w których są przetwarzane dane osobowe, zawiera załącznik 5 do niniejszej Polityki Bezpieczeństwa: „Wykaz pomieszczeń lub części pomieszczeń tworzących obszar, w którym są przetwarzane dane osobowe".

ROZDZIAŁ IX.

REJESTR CZYNNOŚCI PRZETWARZANIA

1. ADO, spełniając kryterium, o którym mowa w art. 30 ust. 5 Rozporządzenia, prowadzi Rejestr Czynności Przetwarzania, który stanowi załącznik numer 2 do niniejszej Polityki.

2. Za bieżące utrzymanie Rejestru Czynności Przetwarzania odpowiada Inspektor Ochrony Danych.
3. Obowiązek informowania IOD o wszelkich zmianach dotyczących zbiorów lub czynności przetwarzania spoczywa na:
   3.1. Informatyku;
   3.2. Administratorze;
   3.3. Pracownikach Administratora;
   w zakresie właściwych dla nich zbiorów danych lub czynności przetwarzania.
4. Podmioty, o których mowa w pkt. 3 niniejszego rozdziału są zobowiązane raz do roku przeprowadzić badanie aktualności posiadanych informacji z treścią bieżącego Rejestru Czynności Przetwarzania.
5. Zaniechanie lub uchybienie obowiązkom, o których mowa w pkt. 3 i 4 może stanowić naruszenie obowiązków pracowniczych i być podstawą odpowiedzialności dyscyplinarnej.
6. W rejestrze zamieszcza się wszystkie następujące informacje:
   6.1. imię i nazwisko lub nazwę oraz dane kontaktowe Administratora oraz wszelkich współadministratorów, a także gdy ma to zastosowanie – przedstawiciela administratora oraz inspektora ochrony danych;
   6.2. cele przetwarzania;
   6.3. opis kategorii osób, których dane dotyczą, oraz kategorii danych osobowych;
   6.4. kategorie odbiorców, którym dane osobowe zostały lub zostaną ujawnione, w tym odbiorców w państwach trzecich lub w organizacjach międzynarodowych;
   6.5. gdy ma to zastosowanie, przekazania danych osobowych do państwa trzeciego lub organizacji międzynarodowej, w tym nazwa tego państwa trzeciego lub organizacji międzynarodowej, oraz informację o dokumentacji odpowiednich zabezpieczeń;
   6.6. jeżeli jest to możliwe, planowane terminy usunięcia poszczególnych kategorii danych;
   6.7. jeżeli jest to możliwe, ogólny opis technicznych i organizacyjnych środków bezpieczeństwa.

ROZDZIAŁ X.

OKREŚLENIE ŚRODKÓW TECHNICZNYCH I ORGANIZACYJNYCH NIEZBĘDNYCH DO ZAPEWNIENIA POUFNOŚCI, INTEGRALNOŚCI I ROZLICZALNOŚCI PRZETWARZANYCH DANYCH OSOBOWYCH

W systemie ochrony danych osobowych wyróżnia się następujące cechy informacji:

- Poufność – zapewnia, że informacja nie jest udostępniana lub ujawniana nieautoryzowanym osobom, podmiotom lub procesom;
- Dostępność – właściwość bycia dostępnym i możliwym do wykorzystania na żądanie w złożonym czasie przez kogoś lub coś, kto lub co ma do tego prawo;
- Integralność – właściwość zapewniająca, że dane nie zostały zmienione lub zniszczone w sposób nieautoryzowany;
- Rozliczalność – właściwość zapewniająca, że działanie podmiotu (np. Użytkownika) mogą być jednoznacznie przypisane tylko temu podmiotowi.

Zastosowane zabezpieczenia (techniczne i organizacyjne) powinny być adekwatne do stwierdzonych zagrożeń mających wpływ na poziom ryzyka dla poszczególnych systemów, rodzajów zbiorów, kategorii i zakresu przetwarzanych danych osobowych.

W celu zapewnienia przetwarzanym danym osobowym atrybutów **poufności** stosuje się następujące zabezpieczenia:

- Po zakończeniu pracy zamykanie pomieszczeń biurowych na klucz;
- Zbiory danych osobowych w formie papierowej są przechowywane, co najmniej w meblach biurowych zamykanych na klucz;
- Obowiązuje polityka zarządzania kluczami;
- Obowiązuje zakaz udzielania informacji dotyczących danych osobowych na podstawie prośby o takie dane w formie zapytania telefonicznego, za wyjątkiem spraw związanych z wykonywaniem obowiązków służbowych;
- Niszczenie brudnopisów, błędnych lub zbędnych kopii materiałów zawierających dane osobowe w sposób uniemożliwiający odczytanie zawartej w nich treści tylko z wykorzystaniem niszczarek do papieru i w uzasadnionych przypadkach płyt CD – klasy, co najmniej P3;
- Przebywanie osób nieuprawnionych w obszarze przetwarzania danych osobowych jest dopuszczalne jedynie w obecności osoby upoważnionej do przetwarzania danych osobowych. W przypadku pomieszczeń technicznych wchodzących w skład obszaru przetwarzania, w których rozlokowane są elementy systemu informatycznego, przebywanie osób możliwe jest wyłącznie w obecności Informatyka;
- Obowiązuje polityka „czystego biurka" i „czystego ekranu";
- W przypadku zawieszenia pracy z systemem informatycznym w związku z tymczasowym opuszczeniem stanowiska pracy, użytkownik zobowiązany jest do: zablokowania dostępu do użytkowanego systemu komputerowego, w tym również do informacji prezentowanych na jego wyświetlaczu.
- Zapewnione jest zdalne monitorowanie sieci z jednej centralnej lokalizacji za pomocą specjalistycznego systemu.

- Systemy informatyczne służące do przetwarzania danych osobowych chroni się przed zagrożeniami pochodzącymi z sieci publicznej z wykorzystaniem ścian ogniowych;
- W celu podniesienia poziomu bezpieczeństwa sieci lokalnej poprzez wykrywanie i blokowanie ataków w czasie rzeczywistym w CZG „Eko-Logicmi" zastosowano – system zapobiegania przed włamaniami (ang. *Intrusion Prevention System – IPS*);
- Zastosowano zabezpieczenie hasłem wygaszanie ekranu w przypadku dłuższej nieaktywności użytkownika;
- Dostęp do systemu oraz wrażliwych funkcji poprzez zdublowane uwierzytelnianie użytkowników do systemu operacyjnego oraz identyfikatora i hasła do wykorzystywanej aplikacji (przy użyciu minimalnie 12 znakowego hasła alfanumerycznego);
- Wyznaczono Inspektora Ochrony Danych;
- Osoby upoważnione do przetwarzania danych osobowych przed dopuszczeniem do tych danych są szkolone w zakresie obowiązujących przepisów o ochronie danych osobowych, procedur przetwarzania danych oraz informowane o podstawowych zagrożeniach związanych z przetwarzaniem danych osobowych. Osoby te są zobowiązane do podpisania stosownego oświadczenia;
- Do danych osobowych mają dostęp jedynie osoby posiadające upoważnienie nadane przez ADO;
- Osoby zatrudnione przy przetwarzaniu danych osobowych obowiązane są do zachowania ich w tajemnicy;
- Tymczasowe wydruki z danymi osobowymi są po ustaniu ich przydatności niszczone w niszczarkach;
- Zapewniono klauzule poufności z wszystkimi podmiotami zewnętrznymi mającymi dostęp do danych osobowych przetwarzanych przez Administratora.

W celu zapewnienia przetwarzanym danym osobowym atrybutów **dostępności i integralności** stosuje się następujące zabezpieczenia:

- Wykonywanie kopii zapasowych danych i programów oraz bezpieczny sposób ich przechowywania;
- Systemy służące do przetwarzania danych osobowych posiadają architekturę klient-serwer, wobec czego wszystkie informacje przechowywane są na serwerze, przez co możliwe jest lepsze zabezpieczenie danych. Serwer decyduje, kto ma prawo do odczytywania, kopiowania i zmiany danych;
- Komputery przenośne i elektroniczne nośniki informacji użytkowane przez Administratora zawierające dane osobowe podczas transportu,

przechowywania i użytkowania są zabezpieczone w sposób zapewniający poufność i integralność tych danych np. z wykorzystaniem środków ochronnych kryptograficznej. Odpowiedzialność za powierzony elektroniczny nośnik informacji ponosi bezpośrednio jego użytkownik.
- Stosowanie zasad wykonywania okresowych przeglądów systemu informatycznego;
- Opracowano i wdrożono "Politykę bezpieczeństwa danych osobowych";
- Zapewnia się bezpieczeństwo nośników informacji zawierających dane osobowe w przypadku, gdy zachodzi konieczność naprawy sprzętu, w którym te nośniki są zamontowane (wymontowanie w przypadku naprawy poza siedzibą Administratora lub nadzór nad serwisem jego siedzibie ADO);
- Zastosowano system ochrony ciągłości zasilania, zmniejszający ryzyko utraty danych znajdujących się aktualnie w pamięci operacyjnej serwerów, a nawet uszkodzenia CZG „Eko-Logiczni" z pamięci masowej.

W celu zapewnienia przetwarzanym danym osobowym atrybutów **rozliczalności** stosuje się następujące zabezpieczenia:

- Zakaz używania nośników elektronicznych nie dopuszczonych do użytku przez Informatyka;
- Stosowanie procedury rozpoczęcia, zawieszenia, zakończenia pracy przez użytkownika systemu informatycznego;
- Stosowane są zasady postępowania w przypadku stwierdzenia naruszenia ochrony danych osobowych;
- System informatyczny pozwala zdefiniować odpowiednie prawa dostępu do jego zasobów;
- Wprowadzono mechanizmy autoryzacji odpowiednio zabezpieczone przed dostępem osób trzecich;
- Identyfikator użytkownika, który utracił upoważnienie do przetwarzania danych, nie jest przydzielany innej osobie.

ROZDZIAŁ XI.

ZARZĄDZANIE DOSTĘPEM DO DANYCH OSOBOWYCH

1. Postanowienia ogólne

Na zasadach określonych w niniejszym rozdziale, polecenie przetwarzania danych osobowych oraz upoważnienie do przetwarzania danych osobowych mogą wynikać

z zakresu czynności, przyjętej polityki zastępstw, pełnomocnictwa (prokury), zarządzenia, zawartej umowy lub wniosku stanowiącego załącznik numer 7 do Polityki.

2. Nadawanie uprawnień do przetwarzania danych osobowych osobom zatrudnianym w Celowym Związku Gmin „Eko-Logiczni"

2.1. W przypadku pracowników, za polecenie przetwarzania danych osobowych oraz upoważnienie do przetwarzania danych osobowych poczytuje się zakres czynności. Zakres czynności wydaje się każdemu pracownikowi do zawartej umowy o pracę i przechowuje w aktach osobowych pracowników.

2.2. W przypadku pracowników oddelegowanych do zastępowania innego pracownika w czasie jego nieobecności, za polecenie przetwarzania danych osobowych poczytuje się przyjętą politykę zastępstw, zaś za upoważnienie do przetwarzania danych osobowych uznaje się zakres czynności pracownika zastępowanego.

2.3. Szczególnymi rodzajami polecenia przetwarzania danych osobowych oraz upoważnienia do przetwarzania danych osobowych są pełnomocnictwo i prokura. Uprawniają one pełnomocników oraz prokurentów do przetwarzania danych osobowych w zakresie niezbędnym do wykonania pełnomocnictwa (prokury).

2.4. Polecenie przetwarzania danych osobowych oraz upoważnienie do przetwarzania danych osobowych mogą wynikać z zarządzenia. Dotyczy to w szczególności zarządzeń w sprawie powołania komisji lub zespołów do wykonywania określonych zadań oraz wyznaczenia poszczególnych osób do wykonywania zadań lub pełnienia funkcji. W takim przypadku, kopię zarządzenia przechowuje się wraz z dokumentacją dotyczącą przedmiotu zarządzenia.

2.5. W przypadku osób zatrudnionych na podstawie stosunku prawnego innego rodzaju, niż stosunek pracy, za polecenie przetwarzania danych osobowych oraz upoważnienie do przetwarzania danych osobowych uznaje się zawartą umowę. Umowa powinna jasno określać zakres prac powierzonych do wykonania.

2.6. W pozostałych przypadkach, polecenie przetwarzania danych osobowych oraz upoważnienie do przetwarzania danych osobowych nadaje Zarząd Związku na podstawie wniosku stanowiącego załącznik numer 7 do Polityki. Integralną częścią tych wniosków jest zobowiązanie do zachowania w tajemnicy treści danych osobowych, stanowiące załącznik numer 7a do Polityki.

2.7. Operacje przetwarzania, takie 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 wykonywane są zgodnie z obowiązującymi

przepisami prawa oraz przyznanym zakresem kompetencji. Zakres kompetencji wynika z upoważnienia do przetwarzania danych osobowych.

2.8. Administrator odbiera od każdej zatrudnionej osoby zobowiązanie do zachowania w tajemnicy treści danych osobowych. Zobowiązanie musi pozostawiać w mocy zarówno w trakcie świadczenia stosunku pracy jak i po jego rozwiązania lub wygaśnięciu. Zobowiązanie może być elementem umowy lub osobnym dokumentem. Wzór zobowiązania stanowi załącznik numer 7a do Polityki.

ROZDZIAŁ XII.

UDOSTĘPNIANIE I POWIERZANIE DANYCH OSOBOWYCH

Udostępnianie danych osobowych poza strukturę.

1. Udostępnienie danych osobowych, czyli przekazywanie i ujawnienie ich innym osobom lub podmiotom, jest możliwe pod warunkiem ziszczenia się jednej z poniższych przesłanek (podmiot zwracający się o udostępnienie danych będzie w stanie wykazać, że przesłanka taka zachodzi):
   1.1. osoba, której dane dotyczą, wyrazi zgodę na udostępnienie danych osobowych (np. osoba chcąca pozyskać od ADO dane osobowe pracownika posiada udzielone przez niego upoważnienie/pełnomocnictwo do uzyskania dostępu do danych – np. w kontekście weryfikacji zatrudnienia przez Banki),
   1.2. udostępnienie danych jest niezbędne dla zrealizowania uprawnienia lub spełnienia obowiązku wynikającego z przepisu prawa (podmiot wnoszący o udostępnienie przedstawia podstawę prawną udostępnienia danych),
   1.3. udostępnienie danych jest konieczne do realizacji umowy, gdy osoba, której dane dotyczą, jest jej stroną lub gdy jest to niezbędne do podjęcia działań przed zawarciem umowy na żądanie osoby, której dane dotyczą,
   1.4. udostępnienie danych jest niezbędne do wykonania określonych prawem zadań realizowanych dla dobra publicznego (konieczność wskazania ogólnej podstawy prawnej),
   1.5. udostępnienie danych jest niezbędne dla wypełnienia prawnie usprawiedliwionych celów realizowanych przez ADO albo odbiorców danych, a przetwarzanie nie narusza praw i wolności osoby, której dane dotyczą (np. udostępnienie danych w celu umożliwienia wystąpienia z roszczeniem cywilnoprawnym, udostępnienie danych w ramach zawartej umowy).
2. Pracownik, do którego wpłynie zapytanie o udostępnienie danych osobowych (osobiście od osoby zainteresowanej, telefonicznie lub drogą elektroniczną), nie może samodzielnie podjąć decyzji o udostępnieniu danych osobowych.

3. Pracownik, który otrzyma zapytanie o udostępnienie danych osobowych powiadamia o tym fakcie IOD.
4. W celu zbadania wystąpienia przesłanek wymienionych w pkt. 2 i udokumentowania procesu udostępnienia danych osobowych, zainteresowana osoba lub podmiot zobowiązane są do wypełnienia wniosku o udostępnienie danych osobowych – stanowiącego załącznik 8 do niniejszej Polityki.
   4.1. Uzupełniony wniosek zostaje przekazany do IOD. Decyduje on o zgodzie lub braku zgody na udostępnienie danych osobowych.
   4.2. Pracownik, do którego wpłynął wniosek udostępnia dane osobowe w przypadku pozytywnej opinii wyrażonej przez IOD.
5. W sytuacji wystąpienia zgody na udostępnienie danych osobowych, IOD odnotowuje ten fakt w Ewidencji udostępnień danych osobowych, której wzór stanowi załącznik 9 do niniejszej Polityki.
6. Odnotowanie to powinno zawierać informacje o: dacie udostępnienia, osobie która dokonała faktycznej czynności udostępnienia danych osobowych, osobie której dane zostały udostępnione, zakresie danych które zostały udostępnione, osobie/podmiocie któremu udostępniono dane osobowe oraz określeniu przesłanki udostępnienia danych osobowych.
7. W uzasadnionych przypadkach, zgodę na udostępnienie danych osobowych może udzielić ADO, jeśli osoby rozpatrujące wniosek o udostępnienie nie są w stanie wspólnie ustalić wystąpienia zasadności przesłanki legalizującej udostępnienie danych osobowych odbiorcy danych.

Powierzanie przetwarzania danych osobowych

W Celowym Związku Gmin „Eko-Logiczni" występują przypadki powierzania przetwarzania danych podmiotom zewnętrznym. W związku z tym zasady opisane w poniższych punktach wymagają stosowania zawartych w nich działań.

1. Powierzenie przetwarzania danych osobowych Podmiotom Przetwarzającym (podmiotom którym powierza się dane do przetwarzania) następuje w drodze umowy zawartej na piśmie. Zalecany wzór umowy powierzenia przetwarzania danych stanowi załącznik nr 10 do niniejszej Polityki.
2. Za przygotowanie właściwej umowy powierzenia przetwarzania danych odpowiedzialny jest Administrator, działając we współpracy z osobą odpowiedzialną za obsługę prawną oraz IOD.
3. Przekazanie zbiorów Podmiotowi Przetwarzającemu w celu ich przetwarzania nie powoduje zmiany właściwego ADO.

4. Podmiot Przetwarzający, któremu powierzono przetwarzanie danych obowiązany jest wykorzystywać powierzone mu dane wyłącznie w celach i w zakresie, które zostały wskazane w zawartej z nim umowie.
5. Podmiot Przetwarzający, któremu powierzono przetwarzanie danych obowiązany jest w szczególności do stosowania się do zapisów umownych, mówiących o zabezpieczeniu danych osobowych, zawartych we wzorze umowy powierzenia przetwarzania danych osobowych, stanowiącej załącznik numer 10 do niniejszej Polityki.
6. Administrator, w momencie doboru podwykonawcy lub podmiotu, który w związku z zawieraną umową uzyska dostęp do danych osobowych przetwarzanych w placówce, przekazuje o tym fakcie informację do IOD, informując o zakresie przewidywanych do powierzenia danych oraz zbiorze/zbiorach z którego/których nastąpi powierzenie.
7. Dokonując wyboru podmiotu, z którym zawarta ma być umowa powierzenia przetwarzania danych osobowych, osoby zaangażowane w proces podpisania umowy zobowiązane są dokonać oceny tego podmiotu, aby gwarantował on wdrożenie odpowiednich środków technicznych i organizacyjnych, by przetwarzanie spełniało wymogi powszechnie obowiązującego prawa i chroniło prawa osób, których dane dotyczą.
8. W sytuacji, gdy powierzenie przetwarzania danych osobowych dotyczyć by miało danych przetwarzanych w formie elektronicznej, lub powierzenie związane byłoby z obsługą teleinformatyczną – Administrator konsultuje zasadność zawarcia umowy powierzenia z Informatykiem (w kontekście spełniania przez podmiot przetwarzający odpowiednich zabezpieczeń w zakresie ochrony danych osobowych w sferze teleinformatycznej).
9. Administrator przekazuje informację o fakcie, zawarciu stosownej umowy do IOD.
10. Wzór ewidencji podmiotów którym ADO powierza dane osobowe do przetwarzania, stanowi załącznik 11 do niniejszej Polityki. Za aktualizację powyższej listy odpowiedzialny jest IOD.

ROZDZIAŁ XIII.

ZARZĄDZANIE RYZYKIEM DANYCH OSOBOWYCH

1. Zarządzanie ryzykiem danych osobowych realizowane na podstawie art. 24, 25, 28, 32 oraz 35 Rozporządzenia odbywa się cyklicznie w odniesieniu do źródeł ryzyka, tj.:
   a. Zbiorów danych osobowych przetwarzanych w bieżącej działalności Administratora. Aktualny wykaz zbiorów danych osobowych jest zawarty w treści załącznika numer 2 Rejestr Czynności Przetwarzania do niniejszej Polityki;

b. Aktywów informacyjnych wykorzystywanych przy przetwarzaniu informacji, np. serwery fizyczne, serwery wirtualne, klastry, zabezpieczenia sieciowe, stacje robocze, komputery przenośne, oprogramowanie, bazy danych, wzory dokumentów, informacje utrwalone w formie cyfrowej lub innej.

2. Proces zarządzania ryzykiem jest uruchamiany:

a) przez Inspektora Ochrony Danych raz do roku w pierwszym kwartale, w zakresie przez niego określonym (wybór niektórych lub grup lub wszystkich źródeł ryzyka);

b) przez:
   - Informatyka;
   - Administratora;

   we właściwych im zakresach (dla właściwych im źródeł ryzyka) każdorazowo na skutek istotnych zmian stosowanych środków technicznych lub organizacyjnych, które mają na celu zapewnienie bezpieczeństwa informacji (tj. ustanowienie nowego zabezpieczenia lub rezygnacja ze stosowanego zabezpieczenia),

c) przez IOD, każdorazowo na skutek zidentyfikowanego naruszenia bezpieczeństwa danych osobowych lub podejrzenia jego wystąpienia, którego wartość wyniesie 2 lub więcej,

d) przez Kierownika komórki organizacyjnej, w której podjęto decyzję o przekazaniu danych osobowych/informacji do przetwarzania podmiotowi przetwarzającemu,

e) przez Inspektora Ochrony Danych, kiedy podjęto decyzję o utworzeniu nowego zbioru danych osobowych (w celu zagwarantowania realizacji zasady prywatności w fazie projektowania zgodnie z postanowieniami niniejszej Polityki).

3. Wszystkie rozpoczęte procesy zarządzania ryzykiem, o których mowa w pkt. 2 niniejszego rozdziału – poza dorocznym procesem, o którym mowa w pkt. 2 lit. a – kończą się najpóźniej po upływie 2 tygodni od rozpoczęcia procesu.

4. Zarządzanie ryzykiem danych osobowych odbywa się w następującym cyklu:

a) identyfikacja źródeł ryzyka,
b) określenie oczekiwanego wyniku materializacji ryzyka,
c) identyfikacja zagrożeń, które doprowadzą do materializacji ryzyka,
d) określenie stosowanych obecnie działań zapobiegających,
e) ocena ryzyka (wpływ i prawdopodobieństwo),
f) szacowanie ryzyka,
g) zaproponowanie sugerowanych działań zaradczych,
h) określenie ewentualnych szans wynikających z materializacji ryzyka,
i) opracowanie planu postępowania z ryzykiem – dla ryzyk, których wartość przekracza próg akceptowalności.

j) ocena planu postępowania z ryzykiem przez Informatyka z uwzględnieniem obecnego stanu wiedzy technicznej,
k) ocena planu postępowania z ryzykiem przez Głównego Księgowego na okoliczność możliwości pokrycia planowanych rozwiązań zgodnie z bieżącym planem finansowym,
l) decyzja Administratora (akceptacja, modyfikacja lub odrzucenie) w sprawie przedstawionego planu postępowania z ryzykiem,
m) realizacja zatwierdzonych planów postępowania z ryzykiem przez wyznaczonych pracowników,
n) monitorowanie realizacji planu postępowania z ryzykiem,
o) prowadzenie zbiorczego rejestru ryzyk bezpieczeństwa informacji.

5. Narzędziem umożliwiającym dokumentowanie procesu identyfikacji ryzyka, zagrożeń, ich ocenę oraz przedstawienie sugestii zabezpieczeń jest załącznik numer 12: „Ankieta Identyfikacji Ryzyk".

6. Plan postępowania z ryzykiem, jego ocena, decyzja Administratora oraz monitorowanie realizacji planu dokumentowane są zgodnie z załącznikiem numer 13: „Plan Postępowania z Ryzykiem". Informacje o realizacji poszczególnych etapów planów postępowania z ryzykiem są przekazywane do IOD.

7. IOD prowadzi rejestr ryzyk bezpieczeństwa informacji zgodnie załącznikiem numer 14: „Rejestr Ryzyk Bezpieczeństwa Informacji".

ROZDZIAŁ XIV.

KONTROLA PRZETWARZANIA I STANU ZABEZPIECZENIA DANYCH OSOBOWYCH

1. Nadzór i kontrola nad ochroną przetwarzanych danych osobowych organizowana jest przez ADO samodzielnie, a w jego imieniu czynności te przeprowadza IOD lub w uzasadnionych przypadkach, na polecenie ADO – audytor wewnętrzny.

2. Kontrole przetwarzania i stanu bezpieczeństwa przeprowadzane są raz do roku lub doraźnie.

3. Czynności kontrolne przeprowadzane są przez osobę, o której mowa w pkt. 1 niniejszego rozdziału, osobiście lub przez wyznaczonych, podległych jej pracowników.

4. Kontrolą, o której mowa w pkt. 1, mogą zostać objęte komórki organizacyjne Administratora, w których przetwarzane są w zbiorach dane osobowe.

5. W ramach utrzymania wysokiego poziomu bezpieczeństwa przetwarzanych danych osobowych mogą być prowadzone przez osoby funkcyjne (IOD/Informatyk) czynności kontrolne w określonych obszarach systemu bezpieczeństwa danych osobowych.

6. Z czynności kontrolnych sporządzany jest protokół, w którym dokonuje się dokładnego opisu zakresu kontroli i czynności przeprowadzonych w jej trakcie. We wnioskach protokołu dokonuje się całościowej oceny stanu ochrony danych przetwarzanych w kontrolowanej komórce organizacyjnej Administratora oraz wskazuje występujące w tym zakresie uchybienia wraz ze sposobami i terminem ich usunięcia.

7. Protokół sporządzany jest w dwóch egzemplarzach i podpisywany jest przez osoby wykonujące czynności kontrolne oraz obowiązkowo przez Kierownika kontrolowanej komórki organizacyjnej. Jeden egzemplarz protokołu pozostaje w kontrolowanej komórce organizacyjnej, drugi przechowywany jest u IOD.

8. Osobom wymienionym w pkt. 1 przysługuje prawo do wykonania czynności sprawdzających w zakresie weryfikacji usunięcia przez komórkę uchybień i wykonania innych zaleceń wskazanych w protokole kontrolnym. Z czynności tych spisywany jest protokół. W przypadku niewykonania zaleceń pokontrolnych informuje się pisemnie o tym fakcie Administratora wnioskując o podjęcie działań dyscyplinujących przewidzianych w Kodeksie Pracy.

9. IOD ma prawo do kontroli podmiotów, którym dokonano powierzenia przetwarzania danych w trybie określonym w niniejszym Rozdziale, o ile w umowie o powierzeniu przetwarzania istnieją stosowne postanowienia w tym zakresie.

ROZDZIAŁ XV.

POSTĘPOWANIE W PRZYPADKU STWIERDZENIA NARUSZENIA BEZPIECZEŃSTWA DANYCH OSOBOWYCH

1. Za naruszenie bezpieczeństwa danych osobowych uznaje się każde zdarzenie, które prowadzi do przypadkowego lub niezgodnego z prawem zniszczenia, utraconia, zmodyfikowania, nieuprawnionego ujawnienia lub nieuprawnionego dostępu do danych osobowych przesyłanych, przechowywanych lub przetwarzanych w inny sposób. Zidentyfikowanie naruszenia, które dotyczy bezpieczeństwa danych osobowych, powoduje konieczność zastosowania przedstawionych niżej zasad.
2. Naruszenie praw i wolności osób fizycznych związane z przetwarzaniem danych osobowych to sytuacja, kiedy osoba, której dane dotyczą może doznać lub doznała

uszczerbku fizycznego lub szkód majątkowych lub niemajątkowych, które m.in. polegają na:

2.1. dyskryminacji,
2.2. kradzieży tożsamości lub oszustwie dotyczącym tożsamości,
2.3. naruszeniu dobrego imienia,
2.4. naruszeniu poufności danych chronionych tajemnicą zawodową,
2.5. nieuprawnionym odwróceniu pseudonimizacji,
2.6. wszelkiej innej znacznej szkodzie gospodarczej lub społecznej.

3. Każda osoba, która powzięnie wiadomość o zaistnieniu jednej z sytuacji określonych w pkt. 1 niniejszego Rozdziału, jest zobowiązana do niezwłocznego zawiadomienia o powyższym swego bezpośredniego przełożonego, IOD, a także Informatyka.

4. IOD każdorazowo dokonuje oceny czy wykryty lub zgłoszony incydent/podejrzenie wystąpienia incydentu powoduje, że naruszenie praw i wolności osób fizycznych, których incydent dotyczy, jest prawdopodobne. Prawdopodobieństwo ocenia w oparciu o Wytyczne w sprawie powiadomień o naruszeniu ochrony danych osobowych na mocy rozporządzenia 2016/679 z dnia 3 października 2017 r. (WP 250), w skali od 1 do 3 przy czym:

4.1. dla wartości 1 przyjmuje się, że jest mało prawdopodobne, by naruszenie skutkowało ryzykiem naruszenia praw lub wolności osób fizycznych;
4.2. dla wartości 2 przyjmuje się, że jest prawdopodobne, by naruszenie skutkowało ryzykiem naruszenia praw lub wolności osób fizycznych;
4.3. dla wartości 3 przyjmuje się, że jest wręcz pewne, że naruszenie skutkuje ryzykiem naruszenia praw lub wolności osób fizycznych.

5. W przypadku stwierdzenia naruszenia przetwarzania danych w systemie informatycznym IOD oraz Informatyk mogą zadecydować ponadto o natychmiastowym zablokowaniu lub ograniczeniu dostępu do zbioru danych osobie podejrzanej o dokonanie naruszenia, z jednoczesnym powiadomieniem o tym fakcie bezpośredniego przełożonego tej osoby.

6. W szczególnie uzasadnionych przypadkach IOD w porozumieniu z ADO mogą podjąć decyzję o całkowitym lub czasowym zablokowaniu dostępu do zbioru (np. utrata integralności zbioru danych powodującą możliwość jego całkowitej lub częściowej utraty, włamanie do zbioru z możliwością zniszczenia części lub całości danych).

7. Ocena incydentu dokonywana jest na załączniku numer 15 „Karta oceny naruszenia/podejrzenia wystąpienia naruszenia".

8. Każdy zgłoszony lub wykryty incydent, bez względu na jego ocenę, wymaga opisania:

8.1. charakteru naruszenia danych osobowych; kategorię i przybliżoną ilość osób, których dane dotyczą; kategorię i przybliżoną liczbę wpisów danych osobowych, których dotyczy naruszenie;

8.2. imienia i nazwiska oraz danych kontaktowych osoby, od której można uzyskać więcej informacji (osoba odpowiedzialna za obsługę incydentu);

8.3. możliwych konsekwencji zaistniałego naruszenia ochrony danych osobowych;

8.4. zastosowanych lub proponowanych przez Administratora środków w celu zaradzenia naruszeniu ochrony danych osobowych.

9. Okoliczności przytoczone wyżej, dokumentowane są przez IOD w ramach załącznika numer 14 „Karta oceny naruszenia/podejrzenia wystąpienia naruszenia".

10. Incydenty, którym przypisano wartość 1 uwzględnia się w załączniku numer 16 „Rejestr Naruszeń".

11. Incydenty, którym przypisano wartość 2:

11.1. stają się przedmiotem zgłoszenia do właściwego organu nadzorczego (obecnie Prezes Urzędu Ochrony Danych Osobowych). Zgłoszenie jest dokonywane w przeciągu 72 godzin od stwierdzenia naruszenia poprzez przesłanie do organu kopii uzupełnionego załącznika numer 14 „Karta oceny naruszenia/podejrzenia wystąpienia naruszenia";

11.2. uwzględnia się w załączniku numer 15 „Rejestr Naruszeń".

12. Incydenty, którym przypisano wartość 3:

12.1. stają się przedmiotem zgłoszenia do właściwego organu nadzorczego (obecnie Prezes Urzędu Ochrony Danych Osobowych). Zgłoszenie jest dokonywane w przeciągu 72 godzin od stwierdzenia naruszenia poprzez przesłanie do organu uzupełnionego załącznika numer 14 „Karta oceny naruszenia/podejrzenia wystąpienia naruszenia";

12.2. stają się przedmiotem niezwłocznie przekazywanego zawiadomienia, kierowanego do każdej osoby fizycznej objętej incydentem, zgodnie z załącznikiem numer 17 „Zawiadomienie osoby fizycznej o naruszeniu";

12.3. uwzględnia się w załączniku numer 16 „Rejestr Naruszeń".

13. Nie zawiadamia się osób fizycznych o naruszeniu jeżeli:

13.1. ADO wdrożył odpowiednie techniczne i organizacyjne środki ochrony i środki te zostały zastosowane do danych osobowych, których dotyczy naruszenie (np. dostęp do kradzieży laptopa, jednak dane na nim zgromadzone zostały zaszyfrowane w sposób uniemożliwiający odczyt osobom nieuprawnionym);

13.2. ADO niezwłocznie zastosował odpowiednie środki techniczne i organizacyjne eliminujące prawdopodobieństwo wysokiego ryzyka naruszenia praw i wolności osoby, której dane dotyczą;

13.3. Zawiadomienie wymagałoby niewspółmiernie dużego wysiłku. W takim wypadku wydany zostanie publiczny komunikat (a jeżeli naruszenie dotyczy tylko pracowników Administratora - komunikat wewnętrzny), za pomocą którego osoby, których dane dotyczą, zostają poinformowane w równie skuteczny sposób o okolicznościach zawartych w załączniku numer 17 „Zawiadomienie osoby fizycznej o naruszeniu".

14. Incydenty zawarte w załączniku numer 16 „Rejestr Naruszeń" uwzględnia się w przeprowadzanym corocznie lub doraźnie procesie zarządzania ryzykiem bezpieczeństwa informacji.

15. W przypadku podjęcia decyzji o złożeniu do organów ścigania karnego zawiadomienia o uzasadnionym podejrzeniu popełnienia przestępstwa stosuje się zasady postępowania określone w tej kwestii w odrębnych wewnętrznych aktach organizacyjnych.

16. Określony w niniejszym Rozdziale tryb postępowania ma zastosowanie także w przypadku zaistnienia sytuacji, której okoliczności będą dawały podstawę do skierowania skargi do organu nadzorczego w związku z działaniem podmiotów zewnętrznych w odniesieniu do danych osobowych, których Administratorem Danych Osobowych jest Celowy Związek Gmin „Eko-Logiczni" w sposób niezgodny z Ustawą i Rozporządzeniem.

17. Wszelkich informacji prasowych na temat zaistniałego zdarzenia może udzielać wyłącznie Administrator lub działający z jego upoważnienia pracownicy.

ROZDZIAŁ XVI.

POSTANOWIENIA KOŃCOWE

1. Polityka Bezpieczeństwa Danych Osobowych jest dokumentem wewnętrznym i nie może być udostępniania osobom postronnym w żadnej formie.

2. Zarząd Związku jest zobowiązany zapoznać z treścią „Polityki Bezpieczeństwa Danych Osobowych" podległych pracowników.

3. Użytkownik zobowiązany jest złożyć oświadczenie o tym, iż został zaznajomiony z przepisami RODO, ustawy o ochronie danych osobowych oraz wydanymi na ich podstawie aktami wykonawczymi oraz instrukcjami obowiązującymi u ADO, a także o zobowiązaniu się do ich przestrzegania.

4. Użytkownicy zobowiązani są do stosowania przy przetwarzaniu danych osobowych postanowień zawartych w niniejszej „Polityce".

5. Szczegółowe zasady przetwarzania danych osobowych określone w niniejszej Polityce, przez podmioty zewnętrzne, regulują stosowne umowy zawarte z nimi w tym zakresie.

6. Procedura udzielenia upoważnienia do przetwarzania danych osobowych dotyczy także osób, które uzyskują dostęp do danych osobowych w trakcie świadczenia pracy na podstawie innej umowy niż stosunek pracy lub wynikających z umów zawartych z innymi podmiotami, np. praktyki studenckie, staże pracownicze.

7. W sprawach nieuregulowanych w niniejszej „Polityce Bezpieczeństwa Danych Osobowych" mają zastosowanie przepisy Rozporządzenia.

Załącznik 1. Wzór formularza wniosku w sprawie utworzenia nowego zbioru danych lub czynności przetwarzania w ramach istniejącego zbioru

WNIOSEK O UTWORZENIE NOWEGO ZBIORU DANYCH LUB CZYNNOŚCI PRZETWARZANIA W RAMACH ISTNIEJĄCEGO ZBIORU DANYCH		
Miejscowość, data		
Adresat wniosku		**Zarząd Związku**
Wnioskodawca	Organizacja lub komórka organizacyjna	
	Stanowisko służbowe	
Nazwa nowego zbioru danych oraz nazwa czynności przetwarzania zawierających się w tym zbiorze albo nazwa czynności przetwarzania mającej zostać dodaną do istniejącego zbioru danych		
Formy prowadzenia zbioru (papierowa czy elektroniczna)		
Regulacja wewnętrzna w Urzędzie odnosząca się do tworzonego zbioru/lub nowych czynności przetwarzania w ramach zbioru		
Podstawa prawna zbierania danych lub pozostałych dopuszczeń określonych w art. 6 RODO		
Zakres zbieranych danych		
Cel zbierania danych.		
Podmiot zbierający dane.		
Źródło pochodzenia danych		
Zamiar udostępniania lub powierzania przetwarzania danych na zewnątrz z oznaczeniem podmiotów przetwarzających lub odbiorców danych		
Wykaz planowanych do stosowania środków i mechanizmów zabezpieczeń		
Infrastruktura systemu informatycznego służącego do przetwarzania danych osobowych		

Obszar przetwarzania danych osobowych	
Przewidywany terminu usunięcia danych	
Zamiar przekazania danych osobowych do odbiorców z państw trzecich (z udokumentowaniem odpowiednich zabezpieczeń)	
Opinia IOD (pełna treść opinii stanowi załącznik numer 1 do wniosku)	*Uzupełnia IOD*

Załącznik 2. Wzór rejestru czynności przetwarzania

Zbiór danych osobowych	Czynność Przetwarzania	Dotychczasowy zbiór danych osobowych (UODO)	Forma przetwarzania danych	Cele przetwarzania danych osobowych	Pola informacyjne/zakres danych/szczególne kategorie danych osobowych/kategorie danych osobowych	Opis kategorii osób, których dane dotyczą	Podstawa prawna przetwarzania danych	Systemy Informatyczne wykorzystywane do przetwarzania danych osobowych	Przewidywany termin usunięcia poszczególnych kategorii danych	Ogólny opis technicznych i organizacyjnych środków bezpieczeństwa	Kategorie odbiorców, którym dane osobowe zostały lub zostaną ujawnione (w tym odbiorców w państwach trzecich)	Nazwa państwa trzeciego/dokumentacja odpowiednich zabezpieczeń
1.												
2.												
3.												
4.												
5.												
6.												
7.												

Zbiór danych osobowych	Czynności Przetwarzania	Dotychczasowy zbiór danych osobowych (TAK/NIE)	Forma przetwarzania danych	Cele przetwarzania danych osobowych	Pola informacyjne/zakres danych/szczególne kategorie danych osobowych/kategorie danych osobowych	Opis kategorii osób, których dane dotyczą	Podstawa prawna przetwarzania danych	Systemy Informatyczne wykorzystywane do przetwarzania danych osobowych	Przewidywany termin usunięcia poszczególnych kategorii danych	Ogólny opis technicznych i organizacyjnych środków bezpieczeństwa	Kategorie odbiorców, którym dane osobowe zostały lub zostaną ujawnione (w tym odbiorców państwach trzecich)	Nazwa państwa trzeciego/dokumentacja odpowiednich zabezpieczeń
1.												

Załącznik 3. Wzór klauzuli informacyjnej – zbieranie danych od osoby

Klauzula informacyjna:

Na podstawie art. 13 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), niniejszym informujemy, że:

1. Administratorem Pana/Pani danych osobowych jest Celowy Związek Gmin „Eko-Logiczni" z siedzibą pod adresem 36-030 Błażowa, ul. Armii Krajowej 42a w imieniu którego obowiązki administratora wypełnia Zarząd Związku;
2. Administrator danych osobowych wyznaczył inspektora ochrony danych, z którym kontakt jest możliwy pod adresem: **iod@czgekologiczni.pl**;
3. Pana/Pani dane będą przetwarzane w celu *PROSZĘ PODAĆ CEL*, a podstawę prawną przetwarzania Pana/Pani danych osobowych stanowi *PROSZĘ OKREŚLIĆ PODSTAWY PRAWNE (RODO+PRZEPIS PRAWA KRAJOWEGO)*;
4. Pana/Pani dane osobowe nie będą przekazywane innym podmiotom;
5. Pana/Pani dane osobowe będą przechowywane przez okres PROSZĘ PODAĆ ILOŚĆ LAT lub do momentu wcześniejszego usunięcia danych;
6. Posiada Pan/Pani prawo żądania dostępu do danych, które Pana/Pani dotyczą, ich sprostowania, usunięcia lub ograniczenia przetwarzania. Posiada Pan/Pani prawo do wniesienia sprzeciwu wobec przetwarzania oraz prawo do przenoszenia danych;
7. Posiada Pan/Pani uprawnienie do cofnięcia zgody udzielonej na przetwarzanie danych w dowolnym momencie;
8. Posiada Pan/Pani prawo do wniesienia skargi do organu nadzorczego (tj. do Prezesa Urzędu Ochrony Danych Osobowych);
9. Podanie przez Pana/Panią danych osobowych jest dobrowolne, brak ich podania nie powoduje żadnych skutków.
10. Pana/Pani dane osobowe nie będą przedmiotem procesów, w ramach których miałoby dojść do zautomatyzowanego podejmowania decyzji, w tym profilowania.

Załącznik 4. Wzór klauzuli informacyjnej – zbieranie danych z innych źródeł

Klauzula informacyjna:

Na podstawie art. 13 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), niniejszym informujemy, że:

1. Administratorem Pana/Pani danych osobowych jest Celowy Związek Gmin „Eko-Logiczni" z siedzibą pod adresem 36-030 Błażowa, ul. Armii Krajowej 42a w imieniu którego obowiązki Administratora wypełnia Zarząd Związku;
2. Administrator danych osobowych wyznaczył inspektora ochrony danych, z którym kontakt jest możliwy pod adresem: **iod@czgekologiczni.pl;**
3. Pana/Pani dane będą przetwarzane w celu *PROSZĘ PODAĆ CEL*, a podstawę prawną przetwarzania Pana/Pani danych osobowych stanowi *PROSZĘ OKREŚLIĆ PODSTAWĘ PRAWNĄ (RODO+PRZEPIS PRAWA KRAJOWEGO)*;
4. Administrator pozyskał dane na Pana/Pani temat w zakresie: *PROSZĘ PODAĆ ZAKRES*;
5. Źródłem pozyskania Pana/Pani danych osobowych jest: *PROSZĘ OKREŚLIĆ PODMIOT LUB POWSZECHNIE DOSTĘPNE ŹRÓDŁO DANYCH*;
6. Pana/Pani dane osobowe nie będą przekazywane innym podmiotom;
7. Pana/Pani dane osobowe będą przechowywane przez okres PROSZĘ PODAĆ ILOŚĆ LAT lub do momentu wcześniejszego usunięcia danych;
8. Posiada Pan/Pani prawo żądania dostępu do danych, które Pana/Pani dotyczą, ich sprostowania, usunięcia lub ograniczenia przetwarzania. Posiada Pan/Pani prawo do wniesienia sprzeciwu wobec przetwarzania oraz prawo do przenoszenia danych;
9. Posiada Pan/Pani uprawnienie do cofnięcia zgody udzielonej na przetwarzanie danych w dowolnym momencie;
10. Posiada Pan/Pani prawo do wniesienia skargi do organu nadzorczego (tj. do Prezesa Urzędu Ochrony Danych Osobowych);
11. Podanie przez Pana/Panią danych osobowych jest dobrowolne, brak ich podania nie powoduje żadnych skutków.
12. Pana/Pani dane osobowe nie będą przedmiotem procesów, w ramach których miałoby dojść do zautomatyzowanego podejmowania decyzji, w tym profilowania.

Załącznik 5. Wzór wykazu pomieszczeń lub części pomieszczeń tworzących obszar, w którym przetwarzane są dane osobowe

Legenda:

1: Opis pomieszczeń (miejsc przetwarzania DO):

(U) – pomieszczenie osób przetwarzających dane osobowe
(S) – serwer
(A) – pomieszczenie Administratora Systemu Informatycznego
(KB) – miejsce przechowywania kopii bezpieczeństwa
(Z) – pomieszczenie, w którym wykonywane są kopie bezpieczeństwa
(KA) – miejsce przechowywania kopii archiwalnych

2: Opis zastosowanych zabezpieczeń fizycznych i organizacyjnych:

(DK) – drzwi do pomieszczeń zamykane na klucz;
(SZK) – szafa zamykana na klucz,
(SPPOZ) – system przeciwpożarowy.
(DM) – wzmocnione drzwi z podwójnymi zamkami, antywłamaniowe
(SM) – szafa metalowa na akta
(KL) – klimatyzacja
(SAW) – system antywłamaniowy
(CCTV) – system monitoringu wizyjnego
(SKD) – system kontroli dostępu fizycznego
(COFO) – całodobowa ochrona fizyczna
(Hg) – higrometr
(RAW) – rolety antywłamaniowe
(KwO) – kraty w oknach
(UPS) – UPS na stacjach roboczych
(CUPS) – centralny UPS w serwerowni

Komórka organizacyjna	Lokalizacja	Budynek	Pomieszczenia	*Zabezpieczenia*

Załącznik 6. Wzór ogólnej polityki informacyjnej

RODO

Ochrona danych osobowych jest jednym z kluczowych zadań realizowanych przez Celowy Związek Gmin „Eko-Logiczni" z siedzibą pod adresem 36-030 Błażowa, ul. Armii Krajowej 42a (dalej: CZG „Eko-Logiczni"). Na bieżąco będziemy informować Państwa o ważnych zmianach w przepisach prawa, w tym o prawach osób, których dane dotyczą. Parlament Europejski opublikował w 2016 roku Rozporządzenie 2016/679 w sprawie ochrony danych osobowych, zwane RODO. Będzie ono miało zastosowanie w Unii Europejskiej od 25 maja 2018 roku.

PRZETWARZANIE DANYCH OSOBOWYCH
Najczęściej zadawane pytania wynikające z tzw. obowiązku informacyjnego:

Co to jest RODO?	Jest to skrót od Rozporządzenia o Ochronie Danych Osobowych. RODO wprowadza m. in. nowe prawa dla osób fizycznych, których dane są przetwarzane. Jednym z obowiązków administratorów, którzy przetwarzają dane osobowe jest informowanie osób o przetwarzaniu ich danych osobowych.
Dlaczego CZG „Eko-Logiczni" przetwarza moje dane osobowe?	CZG „Eko-Logiczni" przetwarza Państwa dane, aby prowadzić działalność wynikającą z przepisów prawa, w tym m.in.: świadczyć usługi na rzecz społeczności lokalnej, dokonywać poboru opłat za gospodarowanie odpadami komunalnymi
Czy mogę mieć dostęp do swoich danych?	Tak. Mogą Państwo mieć pełen dostęp do swoich danych osobowych. Mogą Państwo również zarządzać swoimi zgodami na przetwarzanie danych w zakresie w jakim zbieranie danych osobowych nie jest obowiązkiem prawnym gminy.
Kto jest administratorem moich danych osobowych?	Administratorem Państwa danych osobowych przetwarzanych w Biurze jest **Zarząd Związku z siedzibą pod adresem 36-030 Błażowa, ul. Armii Krajowej 42a** Celowy Związek Gmin „Eko-Logiczni" odpowiada za przetwarzanie danych w sposób bezpieczny, zgodny z obowiązującymi przepisami prawa. W sprawach ochrony danych osobowych mogą Państwo skontaktować się ze Związkiem poprzez email: **biuro@czgekologiczni.pl**.
Jak mogę skontaktować się z inspektorem ochrony danych?	Z inspektorem ochrony danych w Biurze mogą Państwo skontaktować się pod adresem poczty elektronicznej: **iod@czgekologiczni.pl**. Inspektorem ochrony danych jest Tomasz Mielech IOD.
W jakim celu CZG „Eko-Logiczni" przetwarza moje dane osobowe?	Państwa dane osobowe są przetwarzane przez CZG „Eko-Logiczni" w celu: • prowadzenia spraw z zakresu: – utrzymania porządku i czystości w gminach członkowskich, – postępowań egzekucyjnych w administracji, – zamówień publicznych, – skarg i wniosków; • organizacji bezpieczeństwa osób i mienia przebywających na obszarze Biura Związku.

Kto jest odbiorcą moich danych?	CZG „Eko-Logiczni" nie przewiduje udostępniać Państwa danych osobowych podmiotom innym, niż te którym CZG „Eko-Logiczni" powierzył do przetwarzania dane osobowe na podstawie umów powierzenia przetwarzania danych osobowych (tzw. podmioty przetwarzające).
Czy moje dane osobowe będą przekazywane do państwa trzeciego lub organizacji międzynarodowej?	Obecnie nie planujemy przekazywać Państwa danych osobowych poza Europejski Obszar Gospodarczy.
Jak długo Państwa dane osobowe będą przechowywane przez CZG „Eko-Logiczni"?	Dane osobowe będą przechowywane przez okres niezbędny do realizacji Państwa spraw i wniosków oraz ewentualnie po ich zakończeniu w celu wypełnienia obowiązku prawnego (wynikającego w przepisach ustawy z dnia 14 lipca 1983 r. o narodowym zasobie archiwalnym i archiwach oraz aktach wykonawczych do tej ustawy) ciążącego na Urzędzie, a następnie zostaną usunięte lub przekazane do archiwum państwowego.
Jakie uprawnienia mi przysługują?	W związku z przetwarzaniem przez CZG „Eko-Logiczni" danych osobowych przysługuje Państwu prawo do: dostępu do treści swoich danych (art. 15 RODO), do sprostowania danych (art. 16. RODO), do usunięcia danych (art. 17 RODO), do ograniczenia przetwarzania danych (art. 18 RODO), do przenoszenia danych (art. 20 RODO), do wniesienia sprzeciwu wobec przetwarzania danych (art. 21 RODO), prawo do niepodlegania decyzjom podjętym w warunkach zautomatyzowanego przetwarzania danych, w tym profilowania (art. 22 RODO).
Do kogo mogę wnieść skargę?	W przypadku uznania, iż przetwarzanie Państwa danych przez CZG „Eko-Logiczni" narusza przepisy RODO przysługuje Państwu prawo wniesienia skargi do organu nadzorczego Prezesa Urzędu Ochrony Danych Osobowych.
Czy podanie danych osobowych jest dobrowolne czy obligatoryjne?	Podanie przez Państwa danych jest dobrowolne, jednakże w celu dokonania prawidłowej obsługi Państwa wniosków niezbędne. Brak podania danych, niejednokrotnie może utrudnić lub całkowicie uniemożliwić załatwianie spraw w sposób zgodny z Państwa oczekiwaniami. Przepisy szczególne mogą jednak przewidywać sytuacje w których podanie danych osobowych jest obowiązkowe, np. z zakresu prawa podatkowego.
Skąd CZG „Eko-Logiczni" ma moje dane osobowe?	Źródłem Państwa danych osobowych są pisma złożone do Biura CZG „Eko-Logiczni". W przypadku pozyskiwania danych osobowych w sposób inny niż od osób, których dane dotyczą, źródłem danych są inne organy administracji publicznej lub osoby trzecie. Wówczas CZG „Eko-Logiczni" ma obowiązek poinformować Państwa o źródle pozyskania ich danych, chyba że przepis szczególny zwalnia CZG „Eko-Logiczni" z tego obowiązku.

Czy moje dane osobowe będą przetwarzane w sposób zautomatyzowany?	Państwa dane osobowe nie będą przetwarzane w sposób zautomatyzowany, w tym nie będą profilowane.

ZASADY ROZPATRYWANIA WNIOSKÓW DOTYCZĄCYCH OBSŁUGI PRAW KLIENTA W ZAKRESIE DANYCH OSOBOWYCH

Klient indywidualny (również osoba fizyczna prowadząca indywidualne gospodarstwo rolne) i Klient instytucjonalny (osoba fizyczna prowadząca działalność gospodarczą, spółka cywilna, spółka partnerska, spółka jawna) jest uprawniony do złożenia wniosku w zakresie obsługi jego praw wynikających z RODO, a CZG „Eko-Logiczni" zobowiązany jest do jego rozpatrzenia według poniższych zasad:

Klient może zgłosić wniosek w każdej chwili, poczynając od 25 maja 2018 r.
CZG „Eko-Logiczni" rozpatruje wniosek złożony przez Klienta lub osobę działającą w jego imieniu:

- w ciągu miesiąca, licząc od dnia otrzymania żądania.
- w przypadku, gdy żądanie lub liczba żądań Klienta ma skomplikowany charakter, termin udzielenia odpowiedzi może zostać wydłużony o kolejne dwa miesiące; w terminie miesiąca od otrzymania żądania, inspektor ochrony danych poinformuje Klienta listownie o przedłużeniu terminu, z podaniem przyczyn opóźnienia.
- w przypadku niepodjęcia działań w związku z żądaniem Klienta, inspektor ochrony danych niezwłocznie – najpóźniej w ciągu miesiąca od otrzymania żądania, poinformuje Klient listownie o powodach niepodjęcia działań oraz możliwości wniesienia skargi do organu nadzorczego oraz skorzystania ze środków ochrony prawnej przed sądem.

Klient może złożyć wniosek o realizację swoich praw i wolności. Wniosek Klienta powinien zawierać dane adresowe oraz rodzaj i szczegóły żądania.
Klient może złożyć wypełniony wniosek w Biurze lub przesłać go za pośrednictwem poczty elektronicznej na adres **iod@czgekologiczni.pl.**
Bieg terminu rozpatrywania wniosku rozpoczyna się od dnia otrzymania przez CZG „Eko-Logiczni" żądania Klienta.
Klient uprawniony jest do złożenia skargi w przypadku niedotrzymania terminu udzielenia odpowiedzi przez CZG „Eko-Logiczni".
W imieniu CZG „Eko-Logiczni" inspektor ochrony danych udziela Klientowi odpowiedzi na złożony wniosek na piśmie, listem poleconym za zwrotnym potwierdzeniem odbioru lub za pośrednictwem poczty elektronicznej jeżeli jest to zgodne z życzeniem Klienta.
CZG „Eko-Logiczni" nie pobiera żadnych opłat i prowizji za przyjęcie i rozpatrzenie wniosku.
Właściwym dla CZG „Eko-Logiczni" organem nadzoru w zakresie danych osobowych jest Prezes Urzędu Ochrony Danych Osobowych.

W przypadku pytań dotyczących wniosku prosimy o kontakt z inspektorem ochrony danych pod adresem e-mail: **iod@czgekologiczni.pl.**

Podstawa prawna: Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (Dz. U. UE L. 119 z dnia 4 maja 2016 r.)

Załącznik 7. Wzór wniosku o nadanie uprawnień do przetwarzania danych osobowych

Miejscowość, data (DD/MM/RRRR)

WNIOSEK O NADANIE UPRAWNIEŃ DO PRZETWARZANIA DANYCH OSOBOWYCH

1.	**WNIOSKUJĄCY**	
	Imię i nazwisko	
	Organizacja	
	Stanowisko	
2.	**UPRAWNIANY**	
	Imię i nazwisko	
	Organizacja	
	Stanowisko	
3.	**ZAKRES UPRAWNIEŃ**	
	Pouczenie	W polu „zakres upoważnienia" należy wpisać zbiory danych oraz czynności przetwarzania w ramach poszczególnych zbiorów, do których uprawniona ma zostać osoba, której dotyczy wniosek.
	Zakres upoważnienia	
	Okres ważności	
4.	**TREŚĆ WNIOSKU**	
	Wnioskuję o wydanie polecenia przetwarzania danych osobowych oraz upoważnienie do przetwarzania danych osobowych w formie papierowej oraz do obsługi systemu informatycznego służącego do przetwarzania danych osobowych w zakresie oznaczonych zbiorów danych i czynności przetwarzania.	(Podpis Wnioskodawcy)
5.	**NADANIE UPRAWNIEŃ**	
	Na podstawie art. 29 oraz 32 ust. 4 Rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku	(Podpis członków zarządu)

	z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych) **upoważniam do przetwarzania danych osobowych** w zakresie zgodnym z przedmiotowym wnioskiem oraz **polecam przetwarzać dane osobowe** w granicach udzielonego upoważnienia, przestrzegając przyjętych standardów bezpieczeństwa oraz obowiązujących przepisów prawa.	

Załącznik 7a. Wzór zobowiązania do zachowania w tajemnicy treści danych osobowych

ZOBOWIĄZANIE DO ZACHOWANIA POUFNOŚCI

Oświadczam, iż zapoznano mnie z przepisami dotyczącymi ochrony danych osobowych, tj. Rozporządzeniem Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych) oraz z wprowadzonymi i wdrożonymi przez Administratora dokumentami i procedurami związanymi z ochroną danych osobowych - w szczególności z „Polityką Bezpieczeństwa Danych Osobowych". **Przyjmuję do wiadomości zawarte w nich obowiązki i zobowiązuję się do ich przestrzegania.** Ponadto, zobowiązuję się do:

1. zachowania tajemnicy prawnie chronionej (w tym służbowej lub zawodowej), tj. w szczególności do nierozpowszechniania, w jakiejkolwiek formie, jakichkolwiek znanych mi informacji, wiadomości i materiałów do których uzyskam dostęp w ramach wykonywanych obowiązków;
2. nieujawniania danych osobowych nieuprawnionym osobom lub jednostkom organizacyjnym w jakiejkolwiek formie bez zgody Administratora lub uprawnionego przełożonego;
3. zabezpieczenia danych osobowych przed dostępem ze strony osób nieuprawnionych, w szczególności przed ich kradzieżą, przywłaszczeniem, zagubieniem, uszkodzeniem lub zniszczeniem;
4. korzystania ze sprzętu elektronicznego i oprogramowania służbowego wyłącznie do realizacji zadań wynikających z wykonywania moich obowiązków;
5. wykorzystywania jedynie legalnego oprogramowania pochodzącego od Administratora oraz zaniechania prób samodzielnego instalowania oprogramowania pochodzącego z innych źródeł;
6. wnoszenia, wynoszenia i użytkowania komputerów przenośnych bądź innych nośników danych wyłącznie za wiedzą i zgodą Administratora lub uprawnionego przełożonego;
7. należytej dbałości o powierzone mi dokumenty, sprzęt i oprogramowanie.

Informacje, wiadomości i materiały objęte tajemnicą, o której mowa powyżej, to w szczególności: dane osobowe jakiejkolwiek treści i w jakiejkolwiek postaci, dokumenty wytwarzane w toku pracy, korespondencja tradycyjna i elektroniczna, dane zawarte w pamięci komputerów i elektronicznych nośników informacji należących do Administratora, informacje o obowiązujących zasadach bezpieczeństwa.

Zobowiązanie to jest ważne bezterminowo. Oznacza to, że obowiązuje zarówno w okresie sprawowania powierzonej mi funkcji jak i po zaprzestaniu jej wykonywania. Zwolnić od zachowania tajemnicy może mnie jedynie sąd.

Proszę wybrać jedną z poniższych opcji, w zależności od tego, komu nadawane są uprawnienia:

W przypadku osób zatrudnionych na podstawie ***stosunku pracy:***

Jestem świadomy(a), że naruszenie obowiązków pracowniczych w zakresie wskazanym powyżej może stanowić przyczynę uzasadniającą wypowiedzenie przez Pracodawcę umowy o pracę lub rozwiązanie przez Pracodawcę tejże umowy, bez wypowiedzenia, z winy pracownika, zgodnie z przepisami ustawy z dnia 26 czerwca 1974 r. Kodeks Pracy.

W przypadku osób zatrudnionych na podstawie ***umów cywilnoprawnych:***

Jestem świadomy(a), że naruszenie wyżej wymienionych obowiązków może stanowić przyczynę uzasadniającą wypowiedzenie (rozwiązanie) przez Zleceniodawcę (Zamawiającego) umowy zlecenie (umowy o dzieło) ze skutkiem natychmiastowym.

W przypadku ***stażystów oraz praktykantów:***

Jestem świadomy(a), że naruszenie wyżej wymienionych obowiązków może stanowić przyczynę uzasadniającą przerwanie realizowanego stażu lub praktyki zawodowej.

W przypadku ***wolontariuszy:***

Jestem świadomy(a), że naruszenie wyżej wymienionych obowiązków może stanowić przyczynę uzasadniającą wypowiedzenie umowy o wolontariat ze skutkiem natychmiastowym.

1.	**Imię i nazwisko**	
2.	**Data zobowiązania**	
3.	**Podpis zobowiązanego**	

Załącznik 8. Wzór wniosku o udostępnienie danych osobowych

Wniosek o udostępnienie danych osobowych		
Wnioskodawca:		
Adresat wniosku:		
Podstawa udostępnienia:	Zgoda osoby, której dane dotyczą	
	Uprawnienie lub obowiązek wynikający z przepisu prawa (precyzyjnie oznaczony przepis)	
	Zawarta umowa (oznaczenie umowy)	
	Zadania realizowane dla dobra publicznego	
	Prawnie usprawiedliwione cele realizowane przez wnioskodawcę	
Dokument potwierdzający podstawę udostępnienia:	Opis dokumentu: (załącznik do wniosku)	
Opinia IOD:		
Decyzja IOD o udostępnieniu danych:		
Data realizacji wniosku:		
Podpis osoby realizującej:		

Załącznik 9. Wzór ewidencji udostępnień danych osobowych

L.p.	Data udostępnienia danych	Podmiot, któremu dane udostępniono (nazwa, adres)	Osoba której dane udostępniono	Podstawa prawna udostępnienia danych	Cel i zakres udostępnionych danych	Imię i nazwisko pracownika udostępniającego DO

Załącznik 10. Wzór umowy powierzenia przetwarzania danych osobowych

UMOWA POWIERZENIA PRZETWARZANIA
DANYCH OSOBOWYCH NR DB/MM/RRR
(Umowa)

Zawarta w dniu ……, w……, której stronami są odpowiednio:

Celowy Związek Gmin „Eko-Logiczni" z siedzibą pod adresem 36-030 Iłażowa, ul. Armii Krajowej 42a, zwanym dalej **„ADO"**,

reprezentowanym przez:

Pana/Panią …… * ……

a

Nazwa Podmiotu, Kod pocztowy, ulica i numer nieruchomości, wpisaną do rejestru przedsiębiorców prowadzonego przez Sąd Rejonowy dla Miasto, XIII Wydział Gospodarczy Krajowego Rejestru Sądowego, pod nr KRS 0000000000, NIP 0000000000, REGON 0000000000, o kapitale zakładowym …… zł, wpłaconym w całości, zwaną dalej **„Procesorem"**,

reprezentowaną przez:

Pana/Panią …… * ……

Pana/Panią …… * ……

Pana/Panią …… * ……

ADO i Procesor są zwani dalej łącznie **„Stronami"**, a każdy z nich z osobna **„Stroną"**.

§ 1

PRZEDMIOT UMOWY

1. ADO i Procesor zawierają umowę powierzenia przetwarzania danych osobowych, zwaną dalej "Umową", na mocy której ADO powierza Procesorowi przetwarzanie danych osobowych, w zakresie wskazanym w Załączniku nr 1.
2. Powierzenie danych osobowych Procesorowi następuje w celu wykonania umowy lub umów zawartej pomiędzy Stronami (dalej: „Umowa główna" lub „Umowy główne"), określonej (określonych) w Załączniku nr 1.
3. Zakres powierzenia, wskazany w Załączniku nr 1, może zostać w każdym momencie rozszerzony albo ograniczony przez ADO. Ograniczenie albo rozszerzenie może być dokonane poprzez przesłanie przez ADO do Procesora nowej wersji Załącznika nr 1 drogą elektroniczną (na adres e-mail wskazany w Załączniku nr 1).
4. Procesor może przetwarzać powierzone mu dane osobowe wyłącznie w zakresie i celu określonym w Umowie oraz w celu i zakresie niezbędnym do świadczenia usług określonych w Umowie głównej (Umowach głównych).

§ 2

OŚWIADCZENIA I OBOWIĄZKI PROCESORA

1. Procesor niniejszym oświadcza, że posiada zasoby infrastrukturalne, doświadczenie, wiedzę oraz wykwalifikowany personel, w zakresie umożliwiającym należyte wykonanie Umowy, w zgodzie z obowiązującymi przepisami prawa. W szczególności Procesor oświadcza, że znane mu są zasady przetwarzania i zabezpieczenia danych osobowych wynikające z 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, dalej jako: „RODO");
2. Przetwarzać powierzone dane osobowe wyłącznie na podstawie Umowy, która stanowi udokumentowane polecenie ADO.
3. Udzielać dostępu do powierzonych danych osobowych wyłącznie osobom, które ze względu na zakres wykonywanych zadań otrzymały od Procesora upoważnienie do ich przetwarzania oraz wyłącznie w celu wykonywania obowiązków wynikających z Umowy;
4. Zapewnić, aby osoby upoważnione do przetwarzania danych osobowych zobowiązały się do zachowania tajemnicy;
5. Wdrożyć odpowiednie środki techniczne i organizacyjne, aby zapewnić stopień bezpieczeństwa odpowiadający ryzyku naruszenia praw lub wolności osób fizycznych, których dane osobowe będą przetwarzane na podstawie Umowy);
6. W miarę możliwości wspierać ADO (poprzez stosowanie odpowiednich środków technicznych i organizacyjnych) w realizacji obowiązku odpowiadania na żądania osób, których dane dotyczą, w zakresie wykonywania ich praw określonych w rozdziale III RODO;
7. Pomagać ADO, w zakresie:

a. dokonywania zgłaszania naruszeń ochrony danych osobowych organowi nadzorczemu oraz zawiadamiania osób, których dane dotyczą o takim naruszeniu (obowiązki Procesora w odniesieniu do zgłaszania naruszeń zostały określone w § 7 Umowy);

b. dokonywania przez administratora danych oceny skutków dla ochrony danych oraz przeprowadzania konsultacji administratora danych z organem nadzorczym;

8. Prowadzić, w formie pisemnej (w tym elektronicznej), rejestr wszystkich kategorii czynności przetwarzania dokonywanych w imieniu ADO;
9. Udostępniać ADO, na każde żądanie, nie później niż w terminie 3 Dni Roboczych, wszelkie informacje niezbędne do wykazania spełnienia przez ADO obowiązków wynikających z właściwych przepisów prawa, w szczególności z RODO;
10. Umożliwić ADO lub audytorowi upoważnionemu przez ADO przeprowadzanie audytów na zasadach określonych w § 4 Umowy;
11. Niezwłocznie informować ADO, jeżeli zdaniem Procesora wydane mu polecenie stanowi naruszenie RODO lub innych przepisów krajowych lub unijnych o ochronie danych.
12. Przechowywać dane osobowe tylko tak długo, jak to określiła ADO.

§ 3
PODPOWIERZENIE

1. Procesor nie może powierzyć czynności przetwarzania danych osobowych określonych Umową innym osobom lub podmiotom, bez uprzedniej pisemnej lub elektronicznej zgody ADO.
2. ADO może wyrazić zgodę na dalsze powierzenie przez Procesora przetwarzania danych osobowych innym podmiotom przetwarzającym. Procesor jest zobowiązany do informowania o wszelkich planowanych zmianach dotyczących dodania lub zastąpienia dalszych podmiotów przetwarzających. Dalsze powierzenie bez zgody ADO stanowi nienależyte wykonanie Umowy, o którym mowa w § 6ust. 8Umowy.
3. Procesor zapewnia, że będzie korzystał wyłącznie z usług takich dalszych podmiotów przetwarzających, które zapewniają wystarczające gwarancje wdrożenia odpowiednich środków technicznych i organizacyjnych, by przetwarzanie spełniało wymogi RODO oraz przepisów obowiązującego prawa z zakresu ochrony danych osobowych, wskazanych w § 2 ust. 1 pkt 2, które Procesor zobowiązany jest przestrzegać przed dniem 25 maja 2018 r., a także chroniło prawa osób, których dane dotyczą.
4. Procesor zapewni w umowie z dalszym podmiotem przetwarzającym, że na podmiot ten zostaną nałożone obowiązki odpowiadające obowiązkom Procesora określonym w Umowie, w szczególności obowiązek zapewnienia wystarczających gwarancji wdrożenia odpowiednich środków technicznych i organizacyjnych, by przetwarzanie odpowiadało wymogom RODO.

§ 4
AUDYT

1. ADO jest uprawniony do przeprowadzenia audytu zgodności przetwarzania danych osobowych przez Procesora z Umową oraz obowiązującymi przepisami prawa.
2. ADO poinformuje Procesora co najmniej cztery dni Robocze przed planowaną datą audytu o zamiarze jego przeprowadzenia. Jeżeli z ważnych powodów, w ocenie Procesora, audyt nie może zostać przeprowadzony we wskazanym terminie Procesor powinien poinformować o tym fakcie ADO wskazując uzasadnienie dla takiej oceny. W takim przypadku Strony wspólnie ustalą późniejszy termin audytu.
3. Po przeprowadzonym audycie przedstawiciel ADO sporządzi protokół pokontrolny, który podpisują przedstawiciele obu podmiotów. Procesor zobowiązuje się w terminie uzgodnionym z ADO, dostosować do zaleceń pokontrolnych zawartych w protokole, mających na celu usunięcie uchybień i poprawę bezpieczeństwa przetwarzania danych osobowych.

§ 5

ZGŁASZANIE NARUSZEŃ

1. Procesor jest zobowiązany do wdrożenia i stosowania procedur służących wykrywaniu naruszeń ochrony danych osobowych oraz wdrażaniu właściwych środków naprawczych.
2. Po stwierdzeniu naruszenia ochrony powierzonych mu przez ADO danych osobowych Procesor, bez zbędnej zwłoki, jednak w miarę możliwości nie później niż w ciągu 24 godzin od wykrycia naruszenia, zgłasza je ADO. Przedmiotem zgłoszenia są informacje o okolicznościach oraz przyczynie naruszenia.
3. Do czasu uzyskania instrukcji postępowania z naruszeniem od ADO, Procesor bez zbędnej zwłoki podejmuje wszelkie rozsądne działania mające na celu ograniczenie i naprawienie negatywnych skutków naruszenia.
4. Procesor jest zobowiązany do dokumentowania wszelkich naruszeń ochrony powierzonych mu danych osobowych, w tym okoliczności naruszenia ochrony danych osobowych, jego skutków oraz podjętych działań zaradczych. Procesor jest zobowiązany na każde żądanie ADO niezwłocznie udostępnić mu dokumentację, o której mowa w zdaniu poprzedzającym.
5. Procesor nie będzie bez wyraźnej instrukcji ADO powiadamiał o naruszeniu:
    a. osób, których dane dotyczą ani
    b. organu nadzorczego.

§ 6

CZAS TRWANIA UMOWY ORAZ ZASADY ODPOWIEDZIALNOŚCI

1. Umowa zostaje zawarta na czas określony i przestaje obowiązywać wraz z zakończeniem obowiązywania Umowy (Umów) głównej (głównych).
2. ADO może rozwiązać Umowę z zachowaniem 1-miesięcznego okresu wypowiedzenia.
3. ADO uprawniony jest do wypowiedzenia Umowy ze skutkiem natychmiastowym w przypadku zaistnienia ważnych powodów, w tym także w razie naruszenia przez Procesora lub dalszy podmiot przetwarzający przepisów RODO, innych obowiązujących przepisów prawa lub Umowy, a w szczególności, gdy:
    a. organ nadzoru nad przestrzeganiem zasad przetwarzania danych osobowych stwierdzi, że Procesor lub dalszy podmiot przetwarzający nie przestrzega zasad przetwarzania danych osobowych;
    b. prawomocne orzeczenie sądu powszechnego wykaże, że Procesor lub dalszy podmiot przetwarzający nie przestrzega zasad przetwarzania danych osobowych;
    c. ADO w wyniku przeprowadzenia audytu, o którym mowa w § 4 Umowy stwierdzi, że Procesor lub dalszy podmiot przetwarzający nie przestrzega zasad przetwarzania danych osobowych wynikających z Umowy lub obowiązujących przepisów prawa lub Procesor nie zastosuje się do zaleceń pokontrolnych, o których mowa w § 4 ust. 3.

§ 7

POSTANOWIENIA KOŃCOWE

1. Umowa podlega prawu polskiemu. Umowa została sporządzona w 2 egzemplarzach, po jednym dla każdej Strony.
2. W sprawach, które nie zostały uregulowane Umową, znajdują zastosowanie odpowiednie przepisy Kodeksu cywilnego, RODO oraz innych obowiązujących przepisów z zakresu ochrony danych osobowych.
3. Zmiany Umowy są możliwe wyłącznie w formie pisemnej pod rygorem nieważności, z zastrzeżeniem sytuacji, w których Umowa wprost przewiduje inną formę dokonywania zmian.
4. Procesor nie może przenieść praw lub obowiązków wynikających z Umowy bez pisemnej zgody ADO.
5. O ile Umowa główna (Umowy główne) nie stanowi (nie stanowią) inaczej, wszelkie spory w związku z Umową zostaną poddane pod rozstrzygnięcie sądu powszechnego miejscowo właściwego ze względu na siedzibę ADO.

....

ADO **PROCESOR**

Załącznik nr 1
Lista umów głównych o których mowa w §1 umowy powierzenia

1. *Nazwa i numer umowy, data i miejsce zawarcia, dane stron umowy:*
    a. **Zakres danych powierzonych w celu wykonania umowy:**
        i. .....
        ii. .....
        iii. .....
        iv. .....
        v. .....
    b. **Email kontaktowy Procesora:** .....
2. *Nazwa i numer umowy, data i miejsce zawarcia, dane stron umowy:*
    a. **Zakres danych powierzonych w celu wykonania umowy:**
        i. .....
        ii. .....
        iii. .....
        iv. .....
        v. .....
    b. **Email kontaktowy Procesora:** .....

Załącznik 11. Wzór ewidencji umów powierzenia przetwarzania danych osobowych

L.p.	Nazwa procesora (Podmiot, któremu powierzono zbiór)	Numer umowy powierzenia	Data podpisania umowy powierzenia	Nazwa powierzonego zbioru danych osobowych	Data i zakres kontroli u procesora	Uwagi

Załącznik 12. Wzór ankiety identyfikacji ryzyk

1. W ramach ankiety prosimy o zidentyfikowanie zagrożeń w parze z wynikiem jakiego można się spodziewać w następstwie materializacji ryzyka.
2. Następnie prosimy ocenić czy względem zidentyfikowanego zagrożenia istnieją rozwiązania techniczne (np. program antywirusowy) lub organizacyjne (np. instrukcja, niesformalizowana praktyka), które mogą zapobiec wystąpieniu zagrożenia lub minimalizują możliwość wystąpienia zagrożenia.
3. Kolejnym krokiem będzie oszacowanie wartości (od 1 do 3) potencjalnego skutku oraz prawdopodobieństwa wystąpienia ryzyka.
4. Bez względu na uzyskaną wartość "poziomu ryzyka", prosimy o opisanie sugerowanych działań zaradczych. Jeżeli uzupełniający ankietę widzi szanse związane z wystąpieniem ryzyka, prosimy o uzupełnienie kolumny "Szanse".

Źródło ryzyka/Nazwa zbioru danych	Oczekiwany wynik	Zagrożenie	Działania zapobiegające	Potencjalny skutek ryzyka	Prawdopodobieństwo wystąpienia ryzyka	Poziom ryzyka	Sugerowane działania zaradcze	Szanse
				1	1	1		
				1	2	1		
				1	3	3		
				2	2	4		
				2	3	6		
				3	3	9		
				1	1	1		

Załącznik 13. Wzór planu postępowania z ryzykiem

<table>
<tr><th colspan="5">PLAN POSTĘPOWANIA z RYZYKIEM</th></tr>
<tr><td colspan="5">Część 1: szczegółowe informacje dotyczące zidentyfikowanego ryzyka</td></tr>
<tr><td colspan="2">Numer/ID ryzyka</td><td colspan="3"></td></tr>
<tr><td colspan="2">Komórka/osoba, która zidentyfikowała ryzyko:</td><td colspan="3"></td></tr>
<tr><td colspan="2">Źródło ryzyka:</td><td colspan="3"></td></tr>
<tr><td colspan="2">Oczekiwany wynik:</td><td colspan="3"></td></tr>
<tr><td colspan="2">Zidentyfikowane zagrożenia:</td><td colspan="3"></td></tr>
<tr><td colspan="2">Stosowane obecnie działania zapobiegające:</td><td colspan="3"></td></tr>
<tr><td colspan="2">Wartość ryzyka:</td><td colspan="3"></td></tr>
<tr><td rowspan="5">Plan postępowania z ryzykiem</td><td>Proponowana strategia podejścia do ryzyka:</td><td colspan="3"></td></tr>
<tr><td>Działania zaradcze zasugerowane przez uzupełniającego ankietę identyfikacji ryzyk:</td><td colspan="3"></td></tr>
<tr><td>Określenie kosztów wdrożenia sugerowanych działań zaradczych:</td><td colspan="3"></td></tr>
<tr><td>Termin realizacji:</td><td colspan="3"></td></tr>
<tr><td>Osoba odpowiedzialna:</td><td colspan="3"></td></tr>
<tr><td colspan="5">Część 2: Postępowanie z ryzykiem</td></tr>
<tr><td rowspan="3">Pracownicy IT</td><td rowspan="2">Ocena planu postępowania z ryzykiem przez pracowników IT:</td><td>Akceptacja*</td><td>Akceptacja z uwagami*</td><td>Odrzucenie (konstruktywne)*</td></tr>
<tr><td colspan="3">*skreślić niewłaściwe</td></tr>
<tr><td>Podpis osoby odpowiedzialnej:</td><td colspan="3">Treść oceny/opinii:</td></tr>
<tr><td rowspan="3">Główny Księgowy</td><td rowspan="2">Ocena planu postępowania z ryzykiem przez Głównego Księgowego:</td><td>Akceptacja*</td><td>Akceptacja z uwagami*</td><td>Odrzucenie (konstruktywne)*</td></tr>
<tr><td colspan="3">*skreślić niewłaściwe</td></tr>
<tr><td colspan="3">Treść oceny/opinii:</td></tr>
</table>

	Podpis osoby odpowiedzialnej:			
Zarząd Związku	Decyzja	Akceptacja*	Modyfikacja*	Odrzucenie (konstruktywne)*
		*skreślić niewłaściwe		
		Treść oceny/opinii:		
	Podpis osoby odpowiedzialnej:			
Część 3: Realizacja planu postępowania z ryzykiem/monitorowanie				
Numer/ID ryzyka:				
Działania zrealizowane:				
Analiza ryzyka – po wdrożeniu zaplanowanych działań/korekcjach	Źródło ryzyka:			
	Oczekiwany wynik:			
	Zidentyfikowane zagrożenia:			
	Stosowane obecnie działania zapobiegające:			
	Wartość ryzyka:			
	Podpis osoby odpowiedzialnej:			

Załącznik 14. Wzór rejestru ryzyk bezpieczeństwa informacji

Lp.	Źródło ryzyka/ Czynnik sprzyjający/wymuszający	Oczekiwany wynik	Zagrożenie	Działanie zapobiegające	Prawdopodobieństwo zajścia ryzyka	Prawdopodobieństwo wystąpienia ryzyka	POZIOM RYZYKA	POSTĘPOWANIE z RYZYKIEM/PLANY ZARZĄDZANIA RYZYKIEM	POZIOM RYZYKA PO REALIZACJI PLANU POSTĘPOWANIA	SZANSE
1										
2										
3										
4										
5										

Załącznik 15. Wzór karty oceny naruszenia – podejrzenia wystąpienia naruszenia

Karta oceny naruszenia/podejrzenia wystąpienia naruszenia bezpieczeństwa danych osobowych				
Osoba zgłaszająca lub pracownik:				
Data i godzina powzięcia informacji o incydencie:				
Data i godzina zgłoszenia:				
Dział, którego dotyczy incydent:				
Opis naruszenia:				
Charakter naruszenia danych osobowych:				
Kategoria osób objętych incydentem:				
Ilość osób, na które incydent wpływa:				
Zakres danych, których dotyczy incydent:				
Przybliżona liczba wpisów na temat osób:				
Osoba obsługująca incydent:				
Możliwe konsekwencje zaistniałego incydentu:				
Zastosowane środki zaradcze:				
Proponowane środki zaradcze:				
Prawdopodobieństwo naruszenia praw i wolności osób fizycznych:	Legenda: • dla wartości 1 przyjmuje się, że jest mało prawdopodobne, by naruszenie skutkowało ryzykiem naruszenia praw lub wolności osób fizycznych; • dla wartości 2 przyjmuje się, że jest prawdopodobne, by naruszenie skutkowało ryzykiem naruszenia praw lub wolności osób fizycznych; • dla wartości 3 przyjmuje się, że jest wręcz pewne, że naruszenie skutkuje ryzykiem naruszenia praw lub wolności osób fizycznych.			
	w skali od 2 do 3			
Uzasadnienie przypisanej wartości prawdopodobieństwa:				
Data i godzina dokonania oceny:				
Imiona i nazwiska osób, dokonujących oceny prawdopodobieństwa:				
Podpisy:				

Załącznik 16. Wzór rejestru naruszeń bezpieczeństwa danych osobowych

Lp.	Rodzaj incydentu	Osoba zgłaszająca incydent	Osoba obsługująca incydent	Data i czas wystąpienia zdarzenia	Data i czas zgłoszenia	Wartość prawdopodobieństwa naruszenia praw i wolności osób fizycznych	Możliwe konsekwencje zaistniałego incydentu	Zastosowane środki zaradcze	Konieczność informowania organu nadzorczego	Czas przekazania komunikatu do organu nadzorczego	Konieczność informowania osób, których dane dotyczą	Ilość osób, których dotyczył incydent	Sposób komunikacji z osobami fizycznymi

Załącznik 17. Wzór zawiadomienia osoby fizycznej o naruszeniu

Uwaga: Celowy Związek Gmin „Eko-Logiczni" powinien jasnym i prostym językiem opisać charakter naruszenia

Zawiadomienie osoby fizycznej o naruszeniu

Szanowny Panie/Szanowna Pani

Niniejszym na podstawie art. 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) Celowy Związek Gmin „Eko-Logiczni" informuje o:

1. Opisany prostym i jasnym językiem charakter naruszenia;
2. Imię i nazwisko osoby lub wskazanie punktu kontaktowego, od którego można uzyskać więcej informacji;
3. Opis możliwych konsekwencji naruszenia ochrony danych;
4. Opis środków zastosowanych/proponowanych w celu zaradzenia naruszeniu ochrony danych osobowych;
5. *(w szczególnych wypadkach)* Opis środków zastosowanych/proponowanych w celu zminimalizowania ewentualnych negatywnych skutków naruszenia.

Z poważaniem

Imię i nazwisko osoby wskazanej w pkt. 2

Podpis

Ja niżej podpisany/podpisana, wyrażam zgodę na przetwarzanie moich danych osobowych:

1. Celowy Związek Gmin „Eko-Logiczni" z siedzibą pod adresem 36-030 Błażowa, ul. Armii Krajowej 42a;
2. W celu *PROSZĘ OKREŚLIĆ CEL PRZETWARZANIA*;
3. W zakresie *PROSZĘ PODAĆ DANE, KTÓRE PRZEKAZUJE OSOBA*;

Jestem świadomy/świadoma, że podanie danych osobowych jest całkowicie dobrowolne.

Jestem świadomy/świadoma, że udzieloną zgodę mogę wycofać w dowolnym momencie.

Jestem świadomy/świadoma, że wycofanie udzielonej przeze mnie zgody nie wypłynie na zgodność przetwarzania z prawem, jakie miało miejsce przed wycofaniem zgody (wycofanie zgody nie powoduje skutków prawnych wstecz).

(jeżeli dotyczy) Jestem świadomy/świadoma, że moje dane osobowe mogą zostać udostępnione odbiorcom danych, tj. (proszę podać nazwy firm lub kategorie firm, którym mogą zostać udostępnione dane osobowe).

Podpis osoby składającej oświadczenie oraz data

.....

Klauzula informacyjna:

Na podstawie art. 13 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), niniejszym informujemy, że:

1. Administratorem Pana/Pani danych osobowych jest Celowy Związek Gmin „Eko-Logiczni" z siedzibą pod adresem 36-030 Błażowa, ul. Armii Krajowej 42a w imieniu którego obowiązki Administratora wypełnia Zarząd Związku;
2. Administrator danych osobowych wyznaczył inspektora ochrony danych, z którym kontakt jest możliwy pod adresem: **iod@czgrkologiczni.pl;**
3. Pana/Pani dane będą przetwarzane w celu *PROSZĘ PODAĆ CEL*, a podstawę prawną przetwarzania Pana/Pani danych osobowych stanowi *PROSZĘ OKREŚLIĆ PODSTAWY PRAWNE (RODO+ PRZEPIS PRAWA KRAJOWEGO)*;
4. Pana/Pani dane osobowe nie będą przekazywane innym podmiotom;
5. Pana/Pani dane osobowe będą przechowywane przez okres PROSZĘ PODAĆ ILOŚĆ LAT lub do momentu wcześniejszego usunięcia danych;

6. Posiada Pan/Pani prawo żądania dostępu do danych, które Pana/Pani dotyczą, ich sprostowania, usunięcia lub ograniczenia przetwarzania. Posiada Pan/Pani prawo do wniesienia sprzeciwu wobec przetwarzania oraz prawo do przenoszenia danych;
7. Posiada Pan/Pani uprawnienie do cofnięcia zgody udzielonej na przetwarzanie danych w dowolnym momencie;
8. Posiada Pan/Pani prawo do wniesienia skargi do organu nadzorczego (tj. do Prezesa Urzędu Ochrony Danych Osobowych);
9. Podanie przez Pana/Panią danych osobowych jest dobrowolne, brak ich podania nie powoduje żadnych skutków.
10. Pana/Pani dane osobowe nie będą przedmiotem procesów, w ramach których miałoby dojść do zautomatyzowanego podejmowania decyzji, w tym profilowania.

Załącznik 18. – Lista osób zapoznanych z Polityką bezpieczeństwa danych osobowych

Lp.	imię i nazwisko	data	podpis
1.			
2.			
3.			
4.			
5.			
6.			
7.			
8.			
9.			
10.			
11.			
12.			
13.			
14.			
15.			