Zał. nr 6 do Polityki ochrony danych	**Procedura: prawo do sprostowania danych osobowych**

1. Cel procedury

Celem procedury jest realizacja uprawnienia osoby fizycznej do sprostowania/uzupełnienia swoich danych przetwarzanych przez Administratora.

2. Prawa osoby fizycznej, której dane są przetwarzane

Każdej osobie fizycznej przysługuje jednakowe prawo do niezwłocznego sprostowania/uzupełnienia dotyczących go danych osobowych, które są nieprawidłowe lub nieaktualne. Uwzględniając cele przetwarzania, osoba, której dane dotyczą ma prawo do żądania od Administratora uzupełnienia niekompletnych danych osobowych, poprzez przedstawienie odpowiedniego oświadczenia Administratorowi.

Jeżeli osoba fizyczna zażąda uzupełnienia katalogu dotyczących go danych osobowych o te, które nie są niezbędne Administratorowi do działania, to taki wniosek nie musi zostać pozytywnie rozpatrzony przez Administratora dla osoby, której dane dotyczą.

3. Procedura rozpatrywania żądań o sprostowanie danych osobowych

Komunikacja z osobą, której dane dotyczą powinna być prowadzona w zwięzłej, przejrzystej, zrozumiałej i dostępnej formie.

Osoba składająca wniosek o sprostowanie/uzupełnienie danych osobowych oświadcza, że jest osobą możliwą do zidentyfikowania, na podstawie dobrowolnie podanych danych osobowych, umożliwiających jej jednoznaczną identyfikację.

W przypadku, gdy Administrator nie jest w stanie zidentyfikować osoby składającej wniosek o sprostowanie/uzupełnienie danych osobowych, ma prawo na podstawie obowiązujących przepisów prawa odmówić rozpatrzenia żądania, uprzednio podejmując wszelkie możliwe środki w celu zidentyfikowania osoby, która z nim wystąpiła.

Działania podejmowane na podstawie żądania o sprostowanie lub uzupełnienie danych są zwolnione z opłat (art. 12 ust. 5 RODO), lecz jeżeli żądania osoby, której dane dotyczą są ewidentnie nieuzasadnione lub nadmierne (np. ze względu na swój ustawiczny charakter) Administratorowi przysługują dwa uprawnienia:

1) pobranie rozsądnej opłaty, która uwzględnia administracyjne koszty prowadzenia komunikacji i podjętych działań (według stawek obowiązujących u Administratora),

2) odmowa podejmowania działań.

Administrator, w przypadku podjęcia decyzji, o nieuzasadnionym lub nadmiernym charakterze żądania ma obowiązek wykazania takich cech żądania (wniosku) w ewentualnym postępowaniu przed organem nadzorczym.

Administrator jest zobowiązany po dokonaniu sprostowania/ uzupełnienia danych osobowych poinformować wszystkich odbiorców którym ujawniono dane podlegające uzupełnieniu/sprostowaniu o fakcieich uzupełnienia/sprostowania.

W przypadku braku możliwości wykonania powyższego, lub gdy działanie takie wymagałoby niewspółmiernie dużego wysiłku ze strony Administratora, może on podjąć decyzję o nieudzieleniu stosownej informacji odbiorcom, jednakże ma obowiązek wykazania braku tej możliwości lub niewspółmiernie dużego wysiłku w ewentualnym postępowaniu przed organem nadzorczym.

4. Terminy rozpatrywania żądań o sprostowanie/uzupełnienie danych osobowych.

Na podstawie art. 12 ust. 3 RODO, Administrator podejmuje decyzję o przyjęciu/odrzuceniu oświadczenia/wniosku o sprostowanie/uzupełnienie danych osobowych bez zbędnej zwłoki.

Terminy na udzielenie odpowiedzi na żądanie:

1) Administrator zobowiązany jest do udzielenia odpowiedzi na żądanie osoby fizycznej w terminie **miesiąca** od otrzymania tego żądania;
2) jeżeli żądanie ma charakter skomplikowany, lub skierowano dużą liczbę żądań, administrator może wydłużyć czas udzielenia odpowiedzi o kolejne **2 miesiące**, jednakże w takim wypadku jest zobowiązany do przekazania takiej informacji osobie fizycznej w terminie pierwszego miesiąca licząc od momentu wpłynięcia żądania. Musi również w takim wypadku podać przyczyny wydłużenia terminu na udzielenie odpowiedzi (art. 12 ust. 3 RODO).

W przypadku, gdy Administrator nie zamierza udzielić odpowiedzi i działań wobec żądania osoby fizycznej jest zobowiązany do poinformowania tej osoby o powodach niepodjęcia działań, a także możliwości wniesienia skargi do organu nadzorczego oraz skorzystania przez podmiot danych z możliwości wniesienia sprawy do sądu.

Zał. nr 7 do Polityki ochrony danych	**Procedura: prawo do usunięcia danych osobowych („prawo do bycia zapomnianym")**

1. Cel procedury

Celem procedury jest realizacja uprawnienia osoby fizycznej prawa usunięcia swoich danych osobowych („prawo do bycia zapomnianym") przetwarzanych przez Administratora.

2. Prawa osoby fizycznej, której dane są przetwarzane

Każdej osobie fizycznej przysługuje prawo żądania usunięcia jej danych osobowych przetwarzanych przez Administratora. Prawo to składa się z następujących uprawnień:

1) możliwości żądania przez osobę, której dane dotyczą, usunięcia jej danych osobowych przez Administratora danych,
2) możliwości żądania, aby Administrator danych poinformował innych Administratorów, którym upublicznił dane osobowe, że osoba, której dane dotyczą, żąda, by ci administratorzy usunęli wszelkie łącza do tych danych lub ich kopie, czy ich replikacje.

Obowiązek poinformowania innych Administratorów może być ograniczony poprzez: dostępną technologię, koszy, konieczność ograniczenia się Administratora do „rozsądnych działań".

Administrator, w przypadku podjęcia decyzji, o ograniczeniu poinformowania innych Administratorów danych ma obowiązek wykazania takich ograniczeń w ewentualnym postępowaniu przed organem nadzorczym.

Każdej osobie fizycznej przysługuje prawo do „bycia zapomnianym."Prawo to można wykonać, jeżeli spełniona jest choć jedna z następujących przesłanek:

1) dane osobowe nie są już niezbędne do celów, w których zostały zebrane lub w inny sposób przetwarzane;
2) osoba, której dane dotyczą, wycofała zgodę na przetwarzanie danych osobowych i nie istnieje inna podstawa przetwarzania danych;
3) osoba, której dane dotyczą, zgłosiła sprzeciw wobec przetwarzania swoich danych w związku ze swoją szczególną sytuacją albo wobec przetwarzania danych dla celów marketingowych;
4) dane osobowe były przetwarzane w sposób „niezgodny z prawem";
5) dane osobowe „muszą zostać usunięte w celu wywiązania się z obowiązku prawnego przewidzianego w prawie Unii lub prawie państwa członkowskiego, któremu podlega Administrator";

6) dane osobowe zostały zebrane w związku z oferowaniem usług społeczeństwa informacyjnego bezpośrednio dziecku.

W przypadku wykonania prawa do bycia zapomnianym, Administrator zaprzestaje przetwarzania danych osobowych i usuwa dane osoby, która złożyła stosowne oświadczenie/ wniosek, chyba że zachodzą szczególne przypadki ograniczające prawo do bycia zapomnianym:

1) istnieje przepis prawa, który nakazuje przetwarzanie danych osobowych,

2) istnieje sytuacja, w której przetwarzanie jest niezbędne do ustalenia dochodzenia lub obrony roszczeń.

Zał. nr 8 do Polityki ochrony danych	**Procedura: prawo do przenoszenia danych**

1. Cel procedury

Celem procedury jest realizacja uprawnienia osoby fizycznej prawa do przeniesienia swoich danych osobowych przetwarzanych przez Administratora.

2. Prawa osoby fizycznej, której dane są przetwarzane

Prawo do przenoszenia danych może być wykonane wyłącznie wtedy, gdy osoba, której dane dotyczą uprzednio dostarczyła Administratorowi dane jej dotyczące, lub wyraziła zgodę na pozyskanie przez Administratora tych danych, w inny sposób,określony uprzednio odpowiednim oświadczeniem.

Prawo do przenoszenia danych to, w szczególności prawo do:

1) otrzymania przez osobę, której dane dotyczą, w ustrukturyzowanym, powszechnie używanym formacie nadającym się do odczytu maszynowego, danych osobowych jej dotyczących, które dostarczyła administratorowi;
2) prawo przesłania przez osobę, której dane dotyczą, danych osobowych jej dotyczących, które dostarczyła administratorowi, innemu administratorowi, bez przeszkód ze strony administratora danych, o ile jest to technicznie możliwe.

Prawo do przeniesienia danych może zostać wykonane, gdy:

1) przetwarzanie danych odbywa się na podstawie zgody osoby, lub w celu wykonania umowy;
2) przetwarzanie danych odbywa się w sposób zautomatyzowany - prawo do przenoszenia danych obejmuje tylko te dane osobowe, które są przetwarzane przy użyciu systemów informatycznych i nie obejmuje ono tradycyjnych, manualnych papierowych zbiorów danych.

Prawo do przenoszenia danych obejmuje dane osobowe dotyczące osoby, która wykonuje to prawo i które to dane ta osoba dostarczyła Administratorowi. Wykonywanie tego prawa nie może ono niekorzystnie wpływać na praw i wolności innych osób.

Prawo do przenoszenia danych nie ma zastosowania do przetwarzania, które jest niezbędne do wykonania zadania realizowanego w interesie publicznym lub w ramach sprawowania władzy publicznej powierzonej Administratorowi.

Zał.nr 9 do Polityki ochrony danych	**Procedura: prawo do sprzeciwu**

1. Cel procedury

Celem procedury jest realizacja uprawnienia osoby fizycznej prawa do sprzeciwu do przetwarzania swoich danych osobowych przez Administratora.

2. Prawa osoby fizycznej, której dane są przetwarzane

Osoba, której dane dotyczą, ma prawo w dowolnym momencie wnieść sprzeciw z przyczyn związanych z jej szczególną sytuacją wobec przetwarzania dotyczących jej danych osobowych opartego na art. 6 ust. 1 lit. e) lub f) RODO, (w tym profilowania na podstawie tych przepisów), tj. sytuacji, w której:

1) przetwarzanie jest niezbędne do wykonania zadania realizowanego w interesie publicznym lub w ramach sprawowania władzy publicznej powierzonej Administratorowi;
2) przetwarzanie jest niezbędne do celów, wynikających z prawnie uzasadnionych interesów realizowanych przez Administratora lub stronę trzecią, z wyjątkiem sytuacji, w których nadrzędny charakter wobec tych interesów mają interesy lub podstawowe prawa i wolności osoby, której dane dotyczą, wymagające ochrony danych osobowych, w szczególności, gdy osoba, której dane dotyczą jest dzieckiem.

Najpóźniej przy okazji pierwszej komunikacji z osobą, której dane dotyczą, wyraźnie informuje się ją o prawie, do złożenia sprzeciwu wobec powyższego przetwarzania jej danych osobowych, oraz przedstawia się je jasno i odrębnie od wszelkich innych informacji.

W sytuacji, gdy Administrator przetwarza dane osobowe na potrzeby marketingu bezpośredniego, osoba, której dane dotyczą, ma prawo w dowolnym momencie wnieść sprzeciw wobec przetwarzania dotyczących jej danych osobowych na potrzeby takiego marketingu, w tym również profilowania, w zakresie, w jakim przetwarzanie jest związane z takim marketingiem bezpośrednim.

Jeżeli osoba, której dane dotyczą, wniesie sprzeciw wobec przetwarzania do celów marketingu bezpośredniego, to Administratorowi nie wolno już przetwarzać tych danych osobowych do takich celów.

Jeżeli dane osobowe są przetwarzane do celów badań naukowych lub historycznych lub do celów statystycznych na mocy art. 89 ust. 1, osoba, której dane dotyczą, ma prawo wnieść sprzeciw – z przyczyn związanych z jej szczególną sytuacją – wobec przetwarzania

dotyczących jej danych osobowych, chyba że przetwarzanie jest niezbędne do wykonania zadania realizowanego w interesie publicznym.

Jeżeli dane osobowe są przetwarzane do celów marketingu bezpośredniego, osoba, której dane dotyczą, ma prawo wnieść bezpłatnie sprzeciw do Administratora, w dowolnym momencie, wobec tego konkretnego przetwarzania, pierwotnego lub dalszego (w tym profilowania), o ile jest ono powiązane z marketingiem bezpośrednim.

Prawo do sprzeciwu musi zostać przez Administratora wyraźnie podane do wiadomości osobie, której dane dotyczą, jak również musi być przedstawione jasno i oddzielnie od wszelkich innych informacji.

3. Szczególne uprawnienia związane z procesami zautomatyzowanego przetwarzania danych - w tym z profilowaniem

Profilowanie to szczególny rodzaj przetwarzania danych osobowych, który odbywa się w sposób automatyczny, ma na celu ocenę osoby fizycznej lub przewidywanie jejzachowania. Profilowanie zawsze wymaga poinformowania (w sposób możliwy do zweryfikowania) o nim osób, które są profilowane. Profilowanie może być wykorzystywane jako narzędzie dla tzw. automatycznego podejmowania decyzji Administratora wobec osób, których dane dotyczą.

Jeżeli automatyczne podejmowanie decyzji wywołuje skutki prawne wobec osób, których dane dotyczą, lub w podobny istotny sposób wpływa na te osoby, Administrator może mechanizm ten stosować wyłącznie wtedy, gdy spełniony jest jeden z następujących warunków:

1) osoba profilowana wyrazi na to wyraźną zgodę,
2) profilowanie jest niezbędne do zawarcia lub wykonywania umowy z tą osobą,
3) profilowanie jest dopuszczalne przez szczególne przepisy prawa.

Jeżeli profilowanie miałoby się odbywać w oparciu o szczególne kategorie danych osobowych, wówczas jedyną podstawą prawną, która mogłaby takie profilowanie zalegalizować, może być szczególny przepis prawa. W przypadku gdy zgoda na profilowanie została pobrana przy pomocy dedykowanej strony internetowej, odwołanie zgody musi być możliwe w ten sam sposób.

Odwołanie zgody wywołuje wyłącznie skutki na przyszłość – oznacza to, że od chwili otrzymania oświadczenia o odwołaniu zgody, nie można już opierać na zgodzie przetwarzania danych.

4. Realizacja prawa do sprzeciwu

Administrator, po wniesieniu sprzeciwu przez osobę, której dane przetwarzał, powinien zaprzestać przetwarzania tych danych osobowych, chyba że wykaże on istnienie ważnych prawnie uzasadnionych podstaw do przetwarzania, nadrzędnych wobec interesów, praw i wolności osoby, której dane dotyczą, lub podstaw do ustalenia, dochodzenia lub obrony roszczeń.

Nawet jeżeli dane osobowe mogą być przetwarzane zgodnie z prawem, gdy przetwarzanie jest niezbędne do wykonania zadania realizowanego w interesie publicznym lub w ramach sprawowania władzy publicznej powierzonej Administratorowi lub ze względu na prawnie uzasadnione interesy administratora lub strony trzeciej, każdej osobie, której dane dotyczą, przysługuje prawo sprzeciwu wobec przetwarzania danych osobowych dotyczących jej szczególnej sytuacji.

Wykazanie zaistnienia ważnych prawnie uzasadnionych podstaw do przetwarzania, nadrzędnych wobec interesów, praw i wolności osoby, której dane dotyczą, lub podstaw do ustalenia, dochodzenia lub obrony roszczeń, jest obowiązkiem leżącym po stronie Administratora, i ma on obowiązek wykazania powyższego, w ewentualnym postępowaniu przed organem nadzorczym.

Wykorzystanie prawa do sprzeciwu nie prowadzi do automatycznego usunięcia wszystkich danych osobowych przez Administratora. Oznacza ono, że Administrator, z chwilą otrzymania sprzeciwu wobec przetwarzania danych osobowych, zaprzestaje z nich korzystać.

Zał. nr 10do Polityki ochrony danych	**Wzór wniosku o nadanie upoważnienia do przetwarzania danych osobowych/uprawnienia do pracy w systemie informatycznym**

Wnioskuję o nadanie/zmianę/ upoważnienia do przetwarzania danych lub/i uprawnień w systemach informatycznych*

Panu/Pani.....

Zatrudnionemu/onej w .....

Na stanowisku.....

☐ do przetwarzania danych osobowy w następujących celach:

1. .....

2. .....

3. .....

☐ do pracy w systemach informatycznych:

lp.	systemy informatyczne*	uprawnienia*
1.		
2.		
3.		
4.		
5.		
6.		

* niepotrzebne skreślić
*Systemy informatyczne, do których użytkownik ma dostęp
* Uprawnienia:
O-odczyt
W-wydruk
M-modyfikacja (zmiana, wprowadzanie danych)

.....
(podpis osoby składającej wniosek)

Zał.nr 10 do Polityki ochrony danych	**Wzór upoważnienia do przetwarzania danych osobowych**

.....dnia.....roku

UPOWAŻNIENIE DO PRZETWARZANIA DANYCH OSOBOWYCH

Na podstawie art. 29 Rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE upoważniam:

Pana/ Panią .....

zatrudnionego/zatrudnioną w ..... na stanowisku:.....do przetwarzania danych osobowych w następujących celach:

Ponadto pracownik posiada dostęp do następujących systemów informatycznych przetwarzających dane osobowe:

lp.	systemy informatyczne	uprawnienia*
1.		
2.		
3.		
4.		

*Uprawnienia:
O-odczyt
W-wydruk
M-modyfikacja (zmiana, wprowadzanie danych)

Rozwiązanie stosunku pracy/ umowy w przypadku zleceniobiorców/ skutkuje odwołaniem upoważnienia.

(pieczęć i podpis Administratora)

Niniejszym uprzednio wydane upoważnienie traci moc. *(*niniejsza klauzula ma zastosowanie tylko dla osób którym wcześniej wydano upoważnienie)*

Zał. nr12do Polityki ochrony danych	**Wzór ewidencji osób upoważnionych do przetwarzania danych**

EWIDENCJA OSÓB UPOWAŻNIONYCH DO PRZETWARZANIA DANYCH OSOBOWYCH

Lp.	Imię i nazwisko	Stanowisko	Data nadania	Data ustania	Zakres upoważnienia

Zał.nr 13do Polityki ochrony danych	**Opis środków technicznych i organizacyjnych**

Obszar przetwarzania danych osobowych zawiera się w budynku Urzędu Gminy Osięciny, który usytuowany jest przy ulicy Wojska Polskiego 14, 88-220 Osięciny.

Budynek jest 3 kondygnacyjny: parter, I-piętro i II-piętro, podzielony na pokoje, w których przetwarzane są dane osobowe: Pokoje nr: 2, 4, 8, 9, 17, 18, 20, 21, 22, 23, 24, 25, 26, 29, 31 oraz Archiwum i Serwerownia współdzielona z pokojem nr 8. Budynek Urzędu Gminy jest współdzielony z Gminnym Ośrodkiem Pomocy Społecznej, ponadto swoją siedzibę ma Punkt Policji oraz Gminna Spółka Wodno-Melioracyjna.

Wewnątrz i na zewnątrz budynku usytuowany jest monitoring. Monitoring zewnętrzny obejmuje 8 kamer usytuowanych w m. Osięciny Serwer od monitoringu znajduje się w budynku Urzędu Gminy – pokój nr 32 , dostęp do nagrań posiada Wójt Gminy oraz Policja. Zapis z monitoringu jest przechowywany 14 dni i jest automatycznie kasowany. Ponadto w budynku Urzędu Gminy na każdej kondygnacji zamontowany jest monitoring (3 kamery) podgląd do nagrań posiada Wójt Gminy. Zapis jest przechowywany do 14 dni i jest automatycznie kasowany. Dodatkowo budynek zabezpieczony jest alarmem z powiadomieniem zewnętrznej firmy ochroniarskiej.

Na parterze w oknach są rolety antywłamaniowe.

Wykaz systemów informatycznych służących do przetwarzania danych osobowych:

INFO SYSTEM GROSZEK – (podatki, budżetowy, auta, e-

podatki, e-czynsze, środki trwałe, rejestr VAT)

Płatnik – ZUS,

AKCYZA -

SMIECI,

BESTIA,

Kopie zapasowe

Dane osobowe przetwarzane w formie elektronicznej, w szczególności w systemach informatycznych podlegają zabezpieczeniu poprzez tworzenie kopii zapasowych. Za proces tworzenia kopii zapasowych odpowiada *Firma Wenex zajmująca się obsługą informatyczną jednostki.*

Kopią zapasową objęte są:

	Częstotliwość wykonywania kopii zapasowej	Rodzaj nośnika na jakim wykonano kopię zapasową	Sposób wykonywania kopii	Miejsce przechowywania nośnika na którym zapisano kopię
Bazy danych	codziennie	Serwer FTP	automatycznie	Nazwa.pl.u

				dostawcy
Serwery	codziennie	Serwer lokalny	automatycznie	serwerownia
Pliki				

Sposób postępowania z kluczami do pomieszczeń biurowych

Administrator wyznaczył pracowników, którzy są upoważnieni do otwierania głównych drzwi wejściowych do budynku oraz do rozkodowywania systemu alarmowego przed rozpoczęciem pracy jednostki. Pracownik, któremu zostały powierzone klucze oraz kod cyfrowy do systemu alarmowego zobowiązany jest do nie udostępniania kluczy oraz kodu cyfrowego do systemu alarmowego osobom trzecim.

Administrator wyznaczył osoby odpowiedzialne za otwieranie głównych drzwi wejściowych. Administrator przekazał tym osobom kody do instalacji alarmowej. Klucze pobierane i zdawane są po zakończonym dniu do: **pokoju socjalnego** do szafki na klucze. Osobą odpowiedzialną za otwieranie/zamykanie budynku jest osoba sprzątająca.

Od momentu pobrania kluczy do momentu zakończenia dnia pracy na pracownikach spoczywa pełna odpowiedzialność za ich zabezpieczenie. Po otwarciu pomieszczeń biurowych, przed przystąpieniem do pracy, pracownicy sprawdzają stan zastosowanych zabezpieczeń. W przypadku stwierdzenia nieprawidłowości należy postępować zgodnie z procedurą naruszeń stanowiącą **załącznik nr 18 do niniejszej Polityki.**

Zabrania się pozostawiania kluczy do pomieszczeń obszaru przetwarzania danych w drzwiach lub w miejscach ogólnie dostępnych, pomieszczenia zamyka się na czas nieobecności wszystkich pracowników w sposób uniemożliwiający dostęp osobom nieupoważnionym.

Pracownicy po godzinach pracy jednostki mogą w nim przebywać jedynie za zgodą Administratora. W przypadkach przebywania pracowników w pomieszczeniach obszaru przetwarzania danych po wyznaczonych godzinach pracy, godzinach pełnienia obowiązków, wykonywania zadań na rzecz Administratora należy upewnić się czy zamknięto drzwi wejściowe do obszaru przetwarzania danych osobowych. Dodatkowo opuszczając obszar przetwarzania danych należy sprawdzić czy zamknięto wszystkie okna oraz drzwi wejściowe do pomieszczeń.

Zał. nr 14 do Polityki ochrony danych	**Wzór oświadczenia o zachowaniu w poufności danych**

.....dnia .....roku

Ja niżej podpisany ..... zobowiązuję się do zachowania w tajemnicy danych osobowych, do których mam lub będę miała/miał* dostęp w związku z wykonywaniem przeze mnie zadań służbowych i obowiązków pracowniczych, zarówno w trakcie obowiązującego stosunku pracy, jak i bezterminowo po ustaniu zatrudnienia.

.....

(podpis pracownika)

Zał.nr 15 do Polityki ochrony danych	**Oświadczenie o monitorowaniu komputerów służbowych**

Oświadczam, iż zostałam/zostałem zaznajomiona/zaznajomiony z faktem, iż systemy informatyczne, do których mam dostęp na komputerach służbowych i na których wykonuję obowiązki pracownicze, są monitorowane, w zakresie ilościowego i jakościowego wykorzystania tych systemów.

Oświadczam, że monitoring obejmuje również sposób wykorzystania służbowej poczty elektronicznej. Zobowiązuję się do wykorzystywania jej jedynie w celu realizacji zadań pracowniczych, wynikających ze stosunku pracy.

(podpis osoby składającej oświadczenie)

* - niepotrzebne skreślić

Zał.nr 16do Polityki ochrony danych	**Wzór umowy powierzenia**

UMOWA

POWIERZENIA DANYCH OSOBOWYCH DO PRZETWARZANIA

zawarta w dniu _____ r. w _____

pomiędzy:

_____ _____ _____

z siedzibą w _____. (___ - _____),
ul. _____ ,
NIP _____, reprezentowaną przez:
_____ – *(funkcja)*
_____ – *(funkcja)*
zwaną w treści Umowy „**Administratorem**",

a

_____ _____ _____

z siedzibą w _____. (___ - _____),
ul. _____ , NIP
_____, reprezentowaną przez:
_____ – *(funkcja)*
_____ – *(funkcja)*
zwaną w treści Umowy **„Procesorem"** lub „**Przetwarzającym",**

w dalszej części Umowy Administrator i Procesor są nazywani łącznie „**Stronami**" lub każde oddzielnie „**Stroną**".

§ 1

Przedmiot Umowy, rodzaj danych osobowych oraz kategorie osób, których dane dotyczą

1. Umowa ma charakter umowy powierzenia danych osobowych w rozumieniu art. 28 ust. 1 i 3 Rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych; Dz. U. UE. L. 2016, poz. 119.1), zwanego w dalszej części Umowy jako: „Rozporządzenie".
2. Procesor uprawniony jest do przetwarzania danych osobowych wyłącznie w celu wykonania umowy głównej, tj. umowy z dnia _____ , której

przedmiotem jest _____, które będzie zwane w dalszej części Umowy jako „przetwarzanie" .

3. Przetwarzanie dotyczyć będzie (*wskazać kategorie osób oraz rodzaj danych,)*

§ 2

Czas trwania Umowy

1. Umowa zostaje zawarta na czas określony od dnia _____ do dnia _____ (*ewentualnie: na czas trwania umowy, o której mowa w § 1 ust. 3*).
2. Procesor nie ma prawa do wykorzystania zgromadzonych na podstawie niniejszej Umowy danych osobowych w jakimkolwiek celu po jej rozwiązaniu, niezależnie od podstawy takiego rozwiązania.

§ 3

Warunki powierzenia danych osobowych do przetwarzania

1. Procesor przetwarza dane osobowe wyłącznie na udokumentowane polecenie Administratora oraz:
   a) zapewnia, by osoby upoważnione do przetwarzania danych osobowych zobowiązały się do zachowania tajemnicy lub by podlegały odpowiedniemu ustawowemu obowiązkowi zachowania tajemnicy;
   b) podejmuje odpowiednie środki techniczne oraz organizacyjne, mające na celu zapewnienia bezpieczeństwa danych osobowych;
   c) nie korzysta z usług innego podmiotu przetwarzającego, bez uprzedniej pisemnej zgody Administratora;
   d) w miarę możliwości pomaga Administratorowi, poprzez odpowiednie środki techniczne i organizacyjne, wywiązać się z obowiązku odpowiadania na żądania osoby, której dane dotyczą, w zakresie wykonywania jej praw określonych w art. 12-23 Rozporządzenia;
   e) uwzględniając charakter przetwarzania oraz dostępne mu informacje, pomaga administratorowi wywiązać się z obowiązków określonych w art. 32-36 Rozporządzenia;
   f) po zakończeniu świadczenia usług związanych z przetwarzaniem zależnie od decyzji Administratora usuwa lub zwraca mu wszelkie dane osobowe oraz usuwa wszelkie ich

istniejące kopie, w tym również te, zawarte na nośnikach danych, chyba że prawo Unii Europejskiej lub prawo państwa członkowskiego nakazują przechowywanie danych osobowych;

g) udostępnia Administratorowi wszelkie informacje niezbędne do wykazania spełnienia obowiązków określonych w art. 28 Rozporządzenia oraz umożliwia Administratorowi (lub upoważnionemu przez niego audytorowi) przeprowadzanie audytów, w tym inspekcji, i przyczynia się do nich.

2. Jeżeli powierzone dane osobowe są przetwarzane w formie elektronicznej na serwerach i nośnikach danych Procesora, te serwery i nośniki nie mogą znajdować się poza obszarem Unii Europejskiej i Europejskiego Obszaru Gospodarczego.
3. Procesor zobowiązuje się do każdorazowego i niezwłocznego informowania Administratora o przypadkach naruszenia przepisów prawa dotyczących ochrony powierzonych danych osobowych, w tym w szczególności przepisów Rozporządzenia, zaistniałych w okresie obowiązywania niniejszej Umowy.
4. W przypadku stwierdzenia naruszenia ochrony danych osobowych, o którym mowa w art. 33 Rozporządzenia, Procesor zgłasza je Administratorowi bez zbędnej zwłoki. Zgłoszenie naruszenia ochrony danych osobowych Administratorowi powinno nastąpić w formie pisemnej lub elektronicznej.
5. Na wypadek zawinionego naruszenia przez Procesora zasad przetwarzania danych osobowych (określonych w przepisach powszechnie obowiązującego prawa, Rozporządzenia oraz niniejszej Umowy), skutkującego zobowiązaniem Administratorana mocy prawomocnego orzeczenia sądu, ugody sądowej bądź porozumienia mediacyjnego do wypłaty odszkodowania, zadośćuczynienia lub kary pieniężnej, Procesor zobowiązuje się zrekompensować Administratorowi udokumentowane straty z tego tytułu w pełnej wysokości. Zobowiązanie Procesora, o którym mowa powyżej, powstanie pod warunkiem pisemnego powiadomienia go o każdym przypadku wystąpienia przez osoby trzecie z roszczeniem wobec Administratora z podaniem podstaw prawnych i faktycznych, w terminie 3 dni od datydowiedzenia się Administratora o takim roszczeniu.
6. Procesor jest zwolniony z odpowiedzialności za szkody spowodowane przetwarzaniem przez niego danych naruszającym przepisy prawa, jeżeli nie można mu przypisać winy za zdarzenie, które doprowadziło do powstania szkody.
7. Procesor zapewnia, że dane osobowe nie będą udostępniane jego pracownikom i zleceniobiorcom przed podpisaniem przez nich oświadczeń lub umów o zachowaniu poufności. Zachowanie poufności nie ustaje po rozwiązaniu lub wygaśnięciu stosunku

pracy lub umowy cywilnoprawnej, niezależnie od przyczyny tego rozwiązania lub wygaśnięcia.

8. Procesor zobowiązuje się do monitorowania i stosowania przepisów prawa, powszechnie dostępnych wskazówek i zaleceń organu nadzorczego oraz unijnych organów doradczych, zajmujących się ochroną danych osobowych, w zakresie przetwarzania powierzonych mu danych, po uprzednim uzgodnieniu wpływu tych regulacji na przetwarzanie danych z Administratorem.

§ 4

Kontrola przetwarzania danych powierzonych

1. Administrator przez cały okres obowiązywania Umowy jest uprawniony do kontroli poprawności zabezpieczenia i przetwarzania danych powierzonych Procesorowi. Kontrola może zostać przeprowadzona m.in. w formie bezpośredniej inspekcji polegającej na dopuszczeniu przedstawicieli Administratora do wszystkich obszarów przetwarzania danych osobowych objętych niniejszą Umową we wszystkich lokalizacjach Procesora, w sposób nieutrudniający nadmiernie jego bieżącej działalności. Procesor zobowiązany jest do przedstawienia odpowiednich dokumentów do kontroli oraz wyjaśnień na piśmie na każde wezwanie Administratora,.
2. W przypadku, gdy kontrola, o której mowa w ust. 1, wykaże jakiekolwiek nieprawidłowości Administrator ma prawo żądać od Procesora niezwłocznego wdrożenia zaleceń Administratora wynikających z ustaleń pokontrolnych. Zalecenia te przedstawiane będą w formie ustnej, pisemnej lub elektronicznej.

§ 5

Podpowierzenie danych

1. Procesor może powierzać przetwarzanie powierzonych mu danych osobowych objętych Umową innym podmiotom na stałe współpracującym z Procesorem (tzw. podpowierzenie)wyłącznie po uprzedniej pisemnej zgodzie Administratora.
2. Podpowierzając przetwarzanie danych osobowych innym podmiotom, Procesor jest obowiązany zapewnić w dalszej umowie powierzenia spełnienie przez ten podmiot wszelkich wymogów w zakresie ochrony danych osobowych na poziomie, co najmniej takim samym jak przewidziany w niniejszej Umowie.

§ 6

Poufność

1. Procesor zobowiązuje się do zachowania w tajemnicy wszelkich danych osobowych, informacji i materiałów przekazanych lub udostępnionych mu lub o których wiedzę powziął w związku z realizacją Umowy, a także powstałych w wyniku jej wykonania informacji i materiałów w formie pisemnej, graficznej lub jakiejkolwiek innej formie. Informacje
   i materiały są objęte tajemnicą nie mogą być bez uprzedniej pisemnej zgody Administratora udostępniane jakiejkolwiek osobie trzeciej, ani też ujawnione w inny sposób, chyba że w dniu ich ujawnienia były powszechnie znane albo muszą być ujawnione zgodnie z powszechnie obowiązującymi przepisami prawa, orzeczeniem sądu lub organu państwowego.
2. Procesor zapewnia, że osoby upoważnione do przetwarzania danych osobowych będą obowiązane zachować w tajemnicy te dane osobowe oraz sposoby ich zabezpieczenia. Obowiązek zachowania tajemnicy nie ustaje po zaprzestaniu przetwarzania danych z jakiejkolwiek podstawy. Przepis § 3 ust. 6 Umowy stosuje się odpowiednio.

§ 7

Współpraca Stron

1. Strony ustalają, że podczas realizacji Umowy powierzenia będą ze sobą ściśle współpracować, informując się wzajemnie o wszystkich okolicznościach mających lub mogących mieć wpływ na wykonanie powierzenia danych osobowych.
2. Strony będą dokonywały uzgodnień i podejmowały decyzje operacyjne poprzez swoich przedstawicieli odpowiedzialnych za realizację Umowyw formie ustnej, pisemnej lub elektronicznej,.
3. Strony zobowiązują się, że wszelkie decyzje dotyczące polubownego zakończenia sporu z osobą fizyczną na skutek naruszenia ochrony jej danych osobowych, w szczególności fakt i wysokość wypłaty ewentualnego odszkodowania, podejmą wspólnie.

§ 8

Wypowiedzenie umowy

1. Każdej ze Stron przysługuje uprawnienie do rozwiązania Umowy z zachowaniem miesięcznego terminu wypowiedzenia ze skutkiem na koniec miesiąca kalendarzowego, w którym oświadczenie o wypowiedzeniu zostało doręczone drugiej stronie=.

2. Administrator ma prawo wypowiedzieć Umowę w trybie natychmiastowym, w przypadku rażącego naruszenia postanowień Umowy przez Procesora, który:
   a) wykorzystał dane osobowe w sposób niezgodny z Umową, w szczególności przetwarzał je dla własnych celów lub celów innych podmiotów, a także celów niezgodnych z powszechnie obowiązującymi przepisami prawa lub postanowieniami niniejszej Umowy;
   b) wykonuje Umowę niezgodnie z obowiązującymi w tym zakresie przepisami prawa lub instrukcjami Administratora w tym zakresie;
   c) nie zaprzestał niewłaściwego przetwarzania danych osobowych mimo uprzedniego wezwania Administratora do usunięcia naruszeń i bezskutecznego upływu wyznaczonego terminu 14 dni na zaniechanie naruszeń.

§ 9
Postanowienia Końcowe

1. Z tytułu wykonywania niniejszej Umowy Procesorowi *przysługuje/nie przysługuje* dodatkowe wynagrodzenie.
2. Wszelkie zmiany niniejszej Umowy wymagają formy pisemnej pod rygorem nieważności.
3. Spory wynikłe z tytułu Umowy będzie rozstrzygał Sąd właściwy dla miejsca siedziby Administratora.
4. Umowę sporządzono w dwóch jednobrzmiących egzemplarzach, po jednym dla każdej ze Stron.

_____ _____

(Administrator) (Procesor)

Zał. nr 17 do Polityki ochrony danych	**Wzór rejestru umów powierzenia przetwarzania danych osobowych**

Lp.	**Numer umowy**	**Data zawarcia umowy**	**Strona umowy**	**Zakres powierzenia**
1.				
2.				

Zał. nr 18 do Polityki ochrony danych	**Procedura zgłaszania naruszeń ochrony danych osobowych**

1. Cel procedury

Celem procedury jest zminimalizowanie mogących wystąpić nieprawidłowości w funkcjonowaniu Zakładu, spowodowanych nieuprawnionym ujawnieniem danych osobowych, udostępnieniem lub umożliwieniem dostępu do nich osobom nieupoważnionym, zabraniem danych przez osobę nieupoważnioną, uszkodzeniem lub usunięciem, a w szczególności:

1. nieautoryzowany dostęp do danych,
1. nieautoryzowane modyfikacje lub zniszczenie danych,
2. udostępnienie danych nieautoryzowanym podmiotom,
3. nielegalne ujawnienie danych,
4. pozyskiwanie danych z nielegalnych źródeł.

2. Klasyfikacja naruszeń

Naruszenia ze względu na ich występowanie możemy podzielić na:

1. zdarzenia losowe **zewnętrzne**, których występowanie może doprowadzić do utraty integralności danych, ich zniszczenia i uszkodzenia infrastruktury technicznej, zakłócenia ciągłości pracy systemów (np. klęski żywiołowe, przerwy w zasilaniu);
2. zdarzenia losowe **wewnętrzne**, których występowanie może doprowadzić do zniszczenia danych, zakłócenia ciągłości pracy systemu, może nastąpić naruszenie poufności danych (np. niezamierzone pomyłki operatorów, administratorów, awarie sprzętowe, błędy w oprogramowaniu);
3. zdarzenia zamierzone, celowe i świadome, niepowodujące uszkodzenia infrastruktury technicznej i zakłóceń ciągłości pracy możemy podzielić na:
    a) nieuprawniony dostęp do bazy danych z zewnątrz
    b) nieuprawniony dostęp do bazy danych z sieci wewnętrznej
    c) nieuprawniony transfer danych
    d) pogorszenie funkcjonowania sprzętu i oprogramowania np.działania wirusów
    e) bezpośrednie zagrożenie materialnych składników systemu np. kradzież sprzętu.

3. Zgłaszanie naruszeń związanych z bezpieczeństwem informacji

W przypadku stwierdzenia naruszenia zabezpieczeń lub zaistnienia sytuacji, które mogą wskazywać na naruszenie zabezpieczenia danych osobowych, każdy pracownik przetwarzający dane osobowe zobowiązany jest przerwać czynności i niezwłocznie zgłosić ten fakt bezpośredniemu przełożonemu, a następnie postępować stosownie do podjętej przez niego decyzji.

Pracownicy jednostki mają obowiązek zgłaszać zauważone przez siebie naruszenia oraz notować wszystkie szczegóły związane z naruszeniami.

Zgłoszenie powinno zawierać:

a) imię i nazwisko zgłaszającego,
b) określenie sytuacji i czasu w jakim stwierdzono naruszenie zabezpieczeń danych osobowych;
c) określenie wszelkich istotnych informacji mogących wskazywać na przyczynę naruszenia;
d) określenie znanych zgłaszającemu sposobów zabezpieczenia systemu oraz wszelkich kroków podjętych po ujawnieniu zdarzenia.

Osoba zgłaszająca naruszenie w miarę możliwości powinna zabezpieczyć materiał dowodowy np.: zrobić zdjęcie ekranu komputera, co do którego zaistniało podejrzenie, że jego działanie odbiega od normy. Osobą odpowiedzialną za przyjmowanie zgłoszeń naruszeń w jednostce jest inspektor Ewelina Ceglarek.

4. Postępowanie z naruszeniami

Osoba, która otrzymała zgłoszenie dokonuje wstępnej identyfikacji zdarzenia i po konsultacji z Inspektorem Ochrony Danych Osobowych dokonuje jego kwalifikacji jako naruszenie niskie lub wysokie. W przypadku kwalifikacji naruszenia jako niskie należy dokonać wpisu do rejestru naruszeń, którego wzór stanowi ***załącznik nr 1***do niniejszej Procedury. Naruszenia zakwalifikowane jako wysokie podlegają zgłoszeniu do organu nadzorczego niezwłocznie, jednak nie później niż po upływie 72 godzin po stwierdzeniu naruszenia.

a) charakter incydentu i jego znaczenie związane z naruszeniem bezpieczeństwa fizycznego lub teleinformatycznego,
b) miejsce wystąpienia incydentu - identyfikacja punktu, w którym nastąpiło zdarzenie (lokalizacja, serwer, stacja robocza itp.),
c) liczba referatów/komórek organizacyjnych dotkniętych incydentem,
d) identyfikację zasobów potrzebnych przy dalszych działaniach w ramach postępowania z incydentem związanym z bezpieczeństwem informacji,
e) możliwości rozszerzania się incydentu i sposoby jego ograniczania,
f) szacowany poziom szkód,
g) szacunkowy czas, po którym skutki naruszenia zostaną zlikwidowane, jeżeli nie ma możliwości natychmiastowego usunięcia stanu naruszenia bezpieczeństwa informacji,
h) skutki organizacyjne i prawne (wstępny szacunek).

Po dokonanej analizie Administrator zgłasza naruszenie do organu nadzorczego(wzór zgłoszenia stanowi ***załącznik nr 2***do niniejszej Procedury), oraz jeżeli naruszenie może powodować wysokie ryzyko naruszenia praw lub wolności osób fizycznych, administrator bez zbędnej zwłoki zawiadamia osobę, której dane dotyczą, o takim naruszeniu(wzór zawiadomienia stanowi ***załącznik nr 3***do niniejszej Procedury). Zawiadomienie osoby nie jest wymagane jeśli Administrator wdrożył odpowiednie techniczne i organizacyjne środki, które uniemożliwią osobom nieuprawnionym dostęp do danych, zastosował następnie środki eliminujące prawdopodobieństwo wysokiego ryzyka naruszenia praw lub wolności osoby, której dane dotyczą. Z zawiadomienia, o którym mowa nie należy stosować gdy wymagałoby to niewspółmiernie dużego wysiłku. W takim jednak wypadku należy opublikować ogłoszenie, zastosować inny, równie skuteczny środek.

Jeżeli z jakiegokolwiek powodu nie uda się przekazać zgłoszenia w tym terminie, do zgłoszenia należy dołączyć wyjaśnienie przyczyn opóźnienia. Jeżeli Administrator nie zawiadomił jeszcze o naruszeniu osób, których ono dotyczy, organ nadzorczy może mu to nakazać.

Dodatkowo naruszenia mogą być wykorzystywane przez Inspektora Ochrony Danych podczas szkoleń pracowniczych jako przykład tego, co może się wydarzyć, jak unikać ich w przyszłości i jak reagować jak się wydarzą. Podczas wykorzystywania powyższych informacji należy wykazać się daleko idącą ostrożnością w aspekcie zachowywania poufności.

Zał. nr 18 do Polityki ochrony danych	**Procedura zgłaszania naruszeń ochrony danych osobowych**

Załącznik nr 1:

Lp.	Data naruszenia	Kategoria osób, których dane zostały naruszone	Kwalifikacja naruszenia (niskie lub wysokie)	Zastosowane środki zaradcze	Zgłoszenie do organu nadzorczego (dotyczy lub nie dotyczy)	Zawiadomienie osoby której dane dotyczą (dotyczy lub nie dotyczy)
1.						
2.						
3.						
4.						

Załącznik nr: 2

.....dnia.....

Urząd Ochrony Danych Osobowych

.....

Zgłoszenie o naruszeniu ochrony danych osobowych organowi nadzorczemu

Na podstawie obowiązku wynikającego z art. 33 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)

Data Naruszenia	
Liczba osób których dane dotyczą	
Liczba wpisów danych osobowych i kategoria tych danych	
Dane Inspektora Danych osobowych	
Dane Organu Nadzorczego	
Charakter Naruszenia:	
Konsekwencje naruszenia:	
Zastosowane i proponowane środki zaradcze:	

.....

(Podpis Administratora)

Załącznik nr: 3

.....dnia .....roku

Pan/Pani .....

.....

.....

ZAWIADOMIENIE O NARUSZENIU DANYCH OSOBOWYCH

Na podstawie obowiązku wynikającego z 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) w związku z naruszeniem Pana/Pani danych osobowych w zakresie ..... Zawiadamiamy co następuje:

Konsekwencją wyżej wymienionej sytuacji jest podjęcie przez osoby nieupoważnione informacji w zakresie.....

Urząd podjął wszelkie możliwe środki celem minimalizacji skutków naruszenia między innymi: zawiadomienie do organu nadzorczego, zawiadomienie organów ścigania, wcześniejsza szyfryzacja danych.

Celem uzyskania dodatkowych informacji należy kontaktować się z .....

.....

(Podpis Administratora)

Zał. nr 18 do Polityki ochrony danych	**Procedura zgłaszania naruszeń ochrony danych osobowych**

Zał.19 do Polityki ochrony danych	**Wzór notatki z kontroli uprawnień**

.....dnia.....roku

W związku z kontrolą uprawnień i kont użytkowników z dnia ..... stwierdzam co następuje:

1. Użytkownicy pracują na systemach zgodnych z ich uprawnieniami TAK/NIE
   Jeśli NIE, należy wskazać pracowników którym należy nadać lub zabrać upoważnienia:
   .....
   .....
2. Użytkownicy posiadają na stacjach roboczych oprogramowanie na które jednostka posiada licencje
   TAK/NIE
   Jeśli NIE, należy wykazać to oprogramowania oraz nazwy stacji roboczych, na których ono się znajduje.....
   .....
   .....
3. Na stacjach roboczych pracowników znajduje się oprogramowanie nie związane z pracą służbową np. komunikatory społecznościowe, aplikacje służące do wymiany lub pobierania plików, czytniki prywatnej poczty, oprogramowanie umożliwiające dostęp do prywatnej chmury z danymi itp. portalami społecznościowymi
   TAK/NIE
   Jeśli TAK należy wskazać pracowników oraz stacje robocze, na których zostało zidentyfikowane wyżej wymienione oprogramowanie:
   .....
   .....
4. Czy na stacjach roboczych pracowników znajdują się dokumenty i korespondencja nie związana z czynnościami służbowymi
   TAK/NIE
   Jeśli TAK należy wskazać pracowników oraz stacje robocze na której niezgodności występują:
   .....
   .....
5. Wnioski i zalecenia pokontrolne:
   .....
   .....

.....
(podpis Informatyka)