ZARZĄDZENIE NR 80/2023
WÓJTA GMINY MIEDŹNO

z dnia 23 listopada 2023 r.

w sprawie wprowadzenia Polityki Ochrony Danych Osobowych

Na podstawie art. 30 ust. 1 w zw. z art. 31 i art. 33 ust. 1 i 3 ustawy z dnia 8 marca 1990 roku o samorządzie gminnym (Dz. U. z 2023 poz. 40) w zw. z 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)

zarządza się, co następuje:

§ 1. Wprowadza się Politykę Ochrony Danych Osobowych, stanowiązą załącznik do zarządzenia.

§ 2. Polityka ma zastosowanie do wszystkich stanowisk pracy, gdzie przetwarzane są dane osobowe i służy zapewnieniu ich ochrony.

§ 3. Zobowiązuje się pracowników Urzędu Gminy Miedżno do zapoznania się z niniejszym zarządzeniem oraz przestrzegania zasad w nim zawartych.

§ 4. Załącznik do niniejszego Zarządzenia stanowi dokumentację wewnętrzną Urzędu Gminy Miedźno.

§ 5. Zarządzenie wchodzi w życie z dniem podpisania.

Wójt Gminy Miedźno

Piotr Derejczyk

Załącznik do zarządzenia Nr 80/2023
Wójta Gminy Miedźno
z dnia 23 listopada 2023 r.

GMINA MIEDŹNO

POLITYKA
OCHRONY DANYCH OSOBOWYCH

METRYKA DOKUMENTU	
STATUS	DOKUMENT WEWNĘTRZNY
WERSJA DOKUMENTU	1.0
DATA DOKUMENTU	31.10.2023 r.
LICZBA STRON	183
CEL DOKUMENTU	Niniejszy dokument stanowi wzór wewnętrznej Polityki ochrony danych osobowych, stanowiącej podstawowy dokument regulujący zasady przetwarzania danych w przedsiębiorstwie Administratora.
SPIS TREŚCI	1. Definicje ... 3 2. Zasady ogólne ... 3 3. Organizacja systemu ochrony danych osobowych ... 4 4. Udostępnianie i powierzanie danych osobowych ... 5 5. Naruszenia ochrony danych osobowych ... 5 6. Kontakty z Podmiotem danych ... 5 7. Zapewnienie ciągłości ... 6 8. Załączniki ... 6 9. Postanowienia końcowe ... 7

1. DEFINICJE

1.1. **Administrator** lub **ADO– Gmina Miedźno** z siedzibą w Miedźnie ul. Ułańska 25, 42-120 Miedźno, NIP: 5742055080

1.2. **IOD –** Inspektor Ochrony Danych, wyznaczony przez ADO, nadzorujący przestrzeganie przepisów o ochronie danych osobowych w ADO, wykonujący zadania określone w art. 39 RODO. W przypadku braku powołania w ADO IOD, zadania związane z zapewnieniem zgodności przetwarzania danych osobowych w ADO z obowiązującym prawem wykonuje **Koordynator ds. ochrony danych osobowych** (**KODO**).

1.3. **Polityka –** niniejsza Polityka ochrony danych.

1.4. **Pracownik –** osoba fizyczna zatrudniona przez Administratora na podstawie umowy o pracę.

1.5. **Współpracownik –** osoba fizyczna świadcząca na rzecz Administratora usługi na podstawie umowy cywilnoprawnej (np. umowa zlecenie, umowa o dzieło).

1.6. **Organ nadzorczy –** Prezes Urzędu Ochrony Danych Osobowych, lub ewentualnie właściwy organ nadzorczy w zakresie danych osobowych wyznaczony przez inne państwo członkowie Unii Europejskiej.

1.7. **Podmiot danych –** osoba fizyczna, której dotyczą dane osobowe przetwarzane przez Administratora.

1.8. **RODO –** rozporządzenie Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE.

2. ZASADY OGÓLNE

2.1. Niniejsza Polityka stanowi podstawowy dokument regulujący zasady przetwarzania danych przez Administratora.

2.2. Administrator zapewnia przestrzeganie Polityki przez wszystkich Pracowników Administratora.

2.3. W przypadku współpracy z podmiotem trzecim obejmującej przetwarzanie danych osobowych na zlecenie Administratora, ADO zapewnia, by taki podmiot trzeci zobowiązał się do zapewnienia odpowiedniego poziomu ochrony danych osobowych, z uwzględnieniem postanowień Polityki.

2.4. W przypadku współpracy z podmiotem trzecim, obejmującej przetwarzanie przez Administratora danych osobowych na zlecenie tego podmiotu, ADO zawiera umowę powierzenia przetwarzania danych osobowych oraz zapewnia stosowanie się do jej wymogów przez wszystkie osoby zaangażowane w tę współpracę.

2.5. Administrator poprzez odpowiednie środki techniczne i organizacyjne zapewnia możliwość wykazania zgodności przetwarzania danych osobowych z RODO oraz pozostałymi przepisami dotyczącymi danych osobowych („rozliczalność").

2.6. Administrator wyznacza osobę odpowiedzialną za obszar ochrony danych osobowych, powierzając jej funkcję IOD lub KODO, i zapewnia adekwatne środki oraz zasoby niezbędne do wykonywania powierzonych jej zadań. W przypadku powołania IOD Administrator zapewnia, by odpowiadał on bezpośrednio przed Administratorem, oraz dba o unikanie konfliktu interesów pomiędzy IOD a ADO. Postanowienia Polityki dotyczące IOD stosuje się odpowiednio do KODO.

2.7. Wdrożenie Polityki ma na celu zapewnienie zgodności z RODO procesów przetwarzania przez Administratora danych osobowych, bez względu na formę (elektroniczną bądź papierową), w jakiej to przetwarzanie następuje.

3. ORGANIZACJA SYSTEMU OCHRONY DANYCH OSOBOWYCH

3.1. Administrator przypisuje role i zakres odpowiedzialności w procesie przetwarzania danych każdemu z uczestników tego procesu.

3.2. Przed udzieleniem dostępu do przetwarzania danych osobowych Administrator zapoznaje każdego Pracownika, Współpracownika lub inne osoby przetwarzające dane z jego upoważnienia, z procedurami i zasadami dotyczącymi ochrony danych osobowych obowiązującymi u Administratora.

3.3. Przetwarzanie danych osobowych przez Pracowników i Współpracowników może odbywać się wyłącznie na podstawie udokumentowanego upoważnienia Administratora, którego zakres odpowiada przypisanej roli i zakresowi odpowiedzialności. Ponadto Administrator zobowiązuje osoby upoważnione do zachowania poufności danych oraz informacji dotyczących zabezpieczeń danych, a także do przestrzegania procedur i polityk dotyczących ochrony danych obowiązujących w organizacji Administratora.

3.4. Do zadań IOD należy między innymi:

3.4.1. informowanie Administratora oraz Pracowników i Współpracowników, którzy przetwarzają dane osobowe, o obowiązkach spoczywających na nich na mocy RODO i innych przepisów unijnych lub krajowych o ochronie danych osobowych, jak również doradztwo w kwestiach powiązanych;

3.4.2. monitorowanie przestrzegania przez osoby upoważnione przepisów RODO oraz innych przepisów unijnych i krajowych z zakresu ochrony danych osobowych, jak również wewnętrznych polityk i procedur wdrożonych u Administratora w tym zakresie;

3.4.3. udzielanie, na żądanie, zaleceń co do oceny skutków dla ochrony danych oraz monitorowanie jej wykonania zgodnie z art. 35 RODO;

3.4.4. współpraca z Organem nadzorczym;

3.4.5. pełnienie funkcji punktu kontaktowego dla Organu nadzorczego w kwestiach związanych z przetwarzaniem, w tym z uprzednimi konsultacjami, o których mowa

w art. 36 RODO, oraz w stosownych przypadkach prowadzenie konsultacji we wszelkich innych sprawach.

3.5. IOD wypełnia swoje zadania z należytym uwzględnieniem ryzyka związanego z operacjami przetwarzania, mając na uwadze charakter, zakres, kontekst i cele przetwarzania.

3.6. Pracownicy i Współpracownicy przetwarzający dane osobowe są zobowiązani w szczególności do:

3.6.1. przetwarzania danych zgodnie z posiadanym upoważnieniem oraz z należytą starannością;

3.6.2. w przypadku zaobserwowania zdarzenia mogącego stanowić naruszenie ochrony danych osobowych, niezwłocznego informowania o nim bezpośredniego przełożonego oraz IOD na zasadach opisanych w Procedurze oceny i notyfikacji naruszeń ochrony danych osobowych;

3.6.3. uczestnictwa w organizowanych szkoleniach z zakresu ochrony danych osobowych;

3.6.4. zachowania w poufności danych osobowych oraz informacji na temat sposobu ich zabezpieczenia, zgodnie z podpisaną klauzulą poufności.

4. UDOSTĘPNIANIE I POWIERZANIE DANYCH OSOBOWYCH

4.1. Udostępnianie danych osobowych jest dopuszczalne tylko wtedy, gdy spełniony jest jeden z warunków, o którym mowa w art. 6 ust. 1 albo w art. 9 ust. 2 RODO. W przypadku powzięcia wątpliwości, czy dane osobowe powinny zostać udostępnione, należy skonsultować się z IOD.

4.2. Powierzenie przetwarzania danych osobowych podmiotowi trzeciemu następuje w oparciu o umowę powierzenia przetwarzania danych, po weryfikacji tego podmiotu w sposób określony w Polityce wyboru dostawcy przetwarzającego dane osobowe.

5. NARUSZENIA OCHRONY DANYCH OSOBOWYCH

5.1. Administrator zapewnia zgłaszanie naruszeń ochrony danych osobowych Organowi nadzorczemu, chyba że jest mało prawdopodobne, by naruszenie skutkowało ryzykiem naruszenia praw lub wolności osób fizycznych. W tym celu Administrator w szczególności zobowiązuje wszystkie osoby przetwarzające dane osobowe do niezwłocznego informowania o każdym dostrzeżonym naruszeniu ochrony danych osobowych zgodnie z Procedurą oceny i notyfikacji naruszeń ochrony danych osobowych.

5.2. W każdym wypadku Administrator bada zaistniałe naruszenie i wdraża stosowne organizacyjne i techniczne środki naprawcze.

6. KONTAKTY Z PODMIOTEM DANYCH

6.1. Administrator wdraża odpowiednie środki, aby komunikacja z Podmiotem danych odbywała się w zwięzłej, przejrzystej i łatwo dostępnej formie.

6.2. Przyjmowanie i obsługa żądań Podmiotów danych odbywa się na zasadach określonych w Procedurze obsługi żądań Podmiotów danych dotyczących realizacji praw związanych z przetwarzaniem danych.

7. ZAPEWNIENIE CIĄGŁOŚCI

7.1. Administrator zapewnia stałe monitorowanie zgodności działania ADO z zasadami ochrony danych osobowych.

7.2. Do podejmowania czynności związanych z zapewnieniem zgodności zobowiązany jest IOD. Każdy pracownik i współpracownik ADO zobowiązany jest wspierać IOD w wykonywaniu jego zadań, w szczególności udzielać niezbędnych informacji i wyjaśnień.

8. ZAŁĄCZNIKI

8.1. W toku przetwarzania danych osobowych Administrator stosuje następujące zasady, polityki i procedury:

8.1.1. wdrażana jest **Polityka przetwarzania danych osobowych –** zawierająca ogólne informacje o zasadach przetwarzania danych przez Administratora, sposobie realizacji wniosków dotyczących praw podmiotów danych oraz informacje wymagane w art. 13 lub art. 14 RODO w zakresie dotyczącym osób, których dane są przetwarzane przez Administratora, ze względu na prowadzoną z nimi komunikację oraz w innych przypadkach realizacji przez Administratora jego uzasadnionych interesów. Polityka przetwarzania danych osobowych udostępniana jest każdej osobie zainteresowanej, a ponadto zamieszczana na stronie internetowej Administratora;

8.1.2. Pracownikom i Współpracownikom przekazywana jest **Informacja o przetwarzaniu danych osobowych pracowników i współpracowników –** zawierająca informacje wymagane w art. 13 RODO w zakresie obejmującym przetwarzanie danych osób zatrudnionych przez Administratora, niezależnie od podstawy prawnej zatrudnienia. Informacja o przetwarzaniu danych osobowych przekazywana jest każdemu Pracownikowi i Współpracownikowi, a ponadto udostępniana do wglądu każdemu zainteresowanemu Pracownikowi i Współpracownikowi w sposób przyjęty przez Administratora;

8.1.3. prowadzony jest **Rejestr czynności przetwarzania danych osobowych** oraz **Rejestr kategorii czynności przetwarzania**;

8.1.4. wdrażana jest **Polityka retencji danych osobowych –** określająca zasady usuwania danych osobowych oraz okresy ich przetwarzania w zależności od celu tego przetwarzania;

8.1.5. wdrażana jest **Procedura obsługi żądań podmiotów danych –** określająca zasady obsługi (przyjmowania i rozpoznawania) żądań osób fizycznych dotyczących

realizacji praw podmiotów danych, w związku z przetwarzaniem ich danych osobowych, określonych przepisami RODO;

8.1.6. wdrażana jest **Polityka oceny ryzyka i oceny skutków przetwarzania danych osobowych** – określająca zasady realizacji obowiązków wynikających z RODO w zakresie oceny ryzyka naruszenia praw podmiotów danych oraz oceny skutków przetwarzania danych;

8.1.7. wdrażana jest **Procedura oceny i notyfikacji naruszeń ochrony danych osobowych** – określająca zasady identyfikacji i oceny naruszeń ochrony danych oraz sposób ich notyfikacji, w zakresie określonym w RODO, oraz zasady prowadzenia Rejestru naruszeń;

8.1.8. prowadzony jest **Rejestr naruszeń ochrony danych osobowych**;

8.1.9. wdrażana jest **Polityka wyboru dostawcy przetwarzającego dane osobowe** – określająca zasady weryfikacji dostawcy w zakresie gwarancji wdrożenia odpowiednich środków technicznych i organizacyjnych oraz ochrony praw osób, których dane dotyczą, zgodnie z RODO;

8.1.10. wdrażana jest **Polityka współpracy z organem nadzorczym** – określająca zasady postępowania w zakresie wymagającym współpracy z Organem nadzorczym, w tym postępowania kontrolnego oraz sądowo-administracyjnego;

8.1.11. stosowane są **Zasady dokumentowania technicznych i organizacyjnych środków bezpieczeństwa ochrony danych** – określające zasady dokumentowania środków bezpieczeństwa ochrony danych wdrożonych u Administratora, zgodnie z art. 32 RODO;

8.1.12. realizowany jest **Plan utrzymania ciągłości wdrożenia** – określający ogólne ramy czasowe i organizacyjne działań związanych z zapewnieniem stałej zgodności z RODO i pozostałymi przepisami z zakresu danych osobowych.

9. POSTANOWIENIA KOŃCOWE

9.1. Polityka jest aktualizowana przez Administratora w zależności od potrzeb. IOD jest uprawniony do składania wniosku o aktualizację Polityki. Zasady aktualizacji poszczególnych załączników Polityki określone są w tych załącznikach.

9.2. Polityka udostępniana jest wszystkim Pracownikom i Współpracownikom Administratora poprzez umieszczenie jej w Urzędzie Gminy Miedźno pod adresem ul. Ułańska 25, 42-120 Miedźno.

9.3. Polityka obowiązuje od daty wskazanej odpowiednim zarządzeniem Wójta Gminy Miedźno.

POLITYKA
PRZETWARZANIA DANYCH OSOBOWYCH
(POLITYKA TRANSPARENTNOŚCI)

METRYKA DOKUMENTU	
STATUS	Dokument wewnętrzny
WERSJA DOKUMENTU	1.0
DATA DOKUMENTU	31.10.2023 roku
LICZBA STRON	183
CEL DOKUMENTU	Niniejszy dokument zawiera Politykę przetwarzania danych osobowych.
SPIS TREŚCI	Objaśnienia 1. Definicje ..... 10 2. Przetwarzanie danych przez Administratora ..... 10 3. Kontakt z Administratorem ..... 10 4. Bezpieczeństwo danych osobowych ..... 11 5. Cele oraz podstawy prawne przetwarzania ..... 11 6. Odbiorcy danych ..... 14 7. Przekazywanie danych poza EOG ..... 15 8. Okres przetwarzania Danych osobowych ..... 15 9. Uprawnienia związane z przetwarzaniem danych osobowych ..... 15 10. Zmiany Polityki przetwarzania danych osobowych 18

POLITYKA PRZETWARZANIA DANYCH OSOBOWYCH (POLITYKA TRANSPARENTNOŚCI)

DEFINICJE

Administrator – Gmina Miedźno z siedzibą w Miedźnie ul. Ułańska 25, 42-120 Miedźno, NIP: 5742055080

Dane osobowe – informacje o osobie fizycznej zidentyfikowanej lub możliwej do zidentyfikowania poprzez jeden bądź kilka szczególnych czynników określających fizyczną, fizjologiczną, genetyczną, psychiczną, ekonomiczną, kulturową lub społeczną tożsamość, w tym wizerunek, nagranie głosu, dane kontaktowe, dane o lokalizacji, informacje zawarte w korespondencji, informacje gromadzone za pośrednictwem sprzętu rejestrującego lub innej podobnej technologii.

Polityka – niniejsza Polityka przetwarzania danych osobowych.

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.

Podmiot danych – osoba fizyczna, której dotyczą dane osobowe przetwarzane przez Administratora.

PRZETWARZANIE DANYCH PRZEZ ADMINISTRATORA

W związku z prowadzoną działalnością gospodarczą Administrator zbiera i przetwarza Dane osobowe zgodnie z właściwymi przepisami prawa, w tym w szczególności z RODO, i przewidzianymi w nich zasadami przetwarzania danych.

Administrator zapewnia przejrzystość przetwarzania Danych osobowych, w szczególności zawsze informuje o przetwarzaniu danych w momencie ich zbierania, w tym o celu i podstawie prawnej przetwarzania (np. przy zawieraniu umowy sprzedaży towarów lub usług). Administrator dba o to, aby dane były zbierane tylko w zakresie niezbędnym do realizacji wskazanego celu i przetwarzane tylko przez okres, w jakim jest to niezbędne.

Przetwarzając Dane osobowe, Administrator zapewnia ich bezpieczeństwo i poufność oraz dostęp do informacji o przetwarzaniu osobom, których dane dotyczą. Gdyby pomimo stosowanych środków bezpieczeństwa doszło do naruszenia ochrony Danych osobowych (np. „wycieku" danych lub ich utraty), Administrator poinformuje o takim zdarzeniu Podmioty danych w sposób zgodny z przepisami.

KONTAKT Z ADMINISTRATOREM

Kontakt z Administratorem jest możliwy poprzez adres e-mail urzad@miedzno.pl.

Administrator wyznaczył Inspektora Ochrony Danych, z którym można skontaktować się poprzez adres e-mail marcin.pilch@aviso.pl w każdej sprawie dotyczącej przetwarzania Danych osobowych przez Administratora.

BEZPIECZEŃSTWO DANYCH OSOBOWYCH

W celu zapewnienia integralności i poufności danych Administrator wdrożył procedury umożliwiające dostęp do Danych osobowych jedynie osobom upoważnionym i wyłącznie w zakresie, w jakim jest to niezbędne ze względu na wykonywane przez nie zadania. Administrator stosuje rozwiązania organizacyjne i techniczne w celu zapewnienia, że wszystkie operacje na danych osobowych są rejestrowane i dokonywane tylko przez osoby uprawnione.

Administrator podejmuje ponadto wszelkie niezbędne działania, by także jego podwykonawcy i inne podmioty współpracujące dawały gwarancję stosowania odpowiednich środków bezpieczeństwa w każdym przypadku, gdy przetwarzają Dane osobowe na zlecenie Administratora.

Administrator prowadzi na bieżąco analizę ryzyka związanego z przetwarzaniem Danych osobowych i monitoruje adekwatność stosowanych zabezpieczeń danych do identyfikowanych zagrożeń. W razie konieczności Administrator wdraża dodatkowe środki służące zwiększeniu bezpieczeństwa danych.

CELE ORAZ PODSTAWY PRAWNE PRZETWARZANIA

KORESPONDENCJA E-MAILOWA I TRADYCYJNA

W przypadku kierowania do Administratora za pośrednictwem poczty e-mail lub tradycyjnej korespondencji niezwiązanej z usługami świadczonymi na rzecz nadawcy, inną zawartą z nim umową lub w inny sposób niepowiązanej z jakąkolwiek relacją z Administratorem, dane osobowe zawarte w tej korespondencji są przetwarzane wyłącznie w celu komunikacji i rozwiązania sprawy, której dotyczy korespondencja.

Podstawą prawną przetwarzania jest prawnie uzasadniony interes Administratora (art. 6 ust. 1 lit. f RODO), polegający na prowadzeniu korespondencji kierowanej do niego w związku z jego działalnością gospodarczą.

Administrator przetwarza jedynie Dane osobowe istotne dla sprawy, której dotyczy korespondencja. Całość korespondencji jest przechowywana w sposób zapewniający bezpieczeństwo zawartych w niej Danych osobowych (oraz innych informacji) i ujawniana jedynie osobom upoważnionym.

KONTAKT TELEFONICZNY

W przypadku kontaktowania się z Administratorem drogą telefoniczną, w sprawach niezwiązanych z zawartą umową lub świadczonymi usługami, Administrator może żądać podania Danych osobowych tylko wówczas, gdy będzie to niezbędne do obsługi sprawy, której dotyczy kontakt. Podstawą prawną jest w takim wypadku prawnie uzasadniony interes

Administratora (art. 6 ust. 1 lit. f RODO), polegający na konieczności rozwiązania zgłoszonej sprawy związanej z prowadzoną przez niego działalnością gospodarczą.

Rozmowy telefoniczne mogą być także nagrywane – w takim wypadku na początku rozmowy przekazywana jest osobie fizycznej stosowna informacja. Rozmowy są rejestrowane w celu monitorowania jakości świadczonej usługi oraz weryfikacji pracy konsultantów, a także w celach statystycznych. Nagrania są dostępne wyłącznie dla pracowników Administratora oraz osób obsługujących infolinię Administratora.

Dane osobowe w postaci nagrania rozmowy są przetwarzane:

w celach związanych z obsługą klientów i interesantów za pośrednictwem infolinii, jeśli Administrator udostępnia taką usługę – podstawą prawną przetwarzania jest niezbędność przetwarzania do świadczenia usługi (art. 6 ust. 1 lit. b RODO);

w celu monitorowania jakości obsługi i weryfikacji pracy konsultantów obsługujących infolinię, jak również w celach analitycznych i statystycznych – podstawą prawną przetwarzania jest uzasadniony interes Administratora (art. 6 ust. 1 lit. f RODO), polegający na dbaniu o jak najwyższą jakość obsługi na rzecz klientów i interesantów, a także najwyższą jakość pracy konsultantów oraz prowadzenie analiz statystycznych dotyczących komunikacji telefonicznej.

MONITORING WIZYJNY ORAZ KONTROLA WSTĘPU

W związku z koniecznością zapewnienia bezpieczeństwa osób i mienia Administrator stosuje monitoring wizyjny oraz kontroluje wstęp do lokali i na teren przez niego zarządzany. Zebrane w ten sposób dane nie są wykorzystywane do żadnych innych celów opisanych poniżej.

Dane osobowe w postaci nagrań z monitoringu oraz dane zbierane w rejestrze wejść i wyjść są przetwarzane w celu zapewnienia bezpieczeństwa osób i mienia oraz utrzymania porządku na terenie obiektu, oraz ewentualnie w celu obrony przed roszczeniami wysuwanymi wobec Administratora lub ustalenia i dochodzenia roszczeń przez Administratora. Podstawą prawną przetwarzania danych osobowych jest prawnie uzasadniony interes Administratora (art. 6 ust. 1 lit. f RODO), polegający na zapewnieniu bezpieczeństwa osób i mienia znajdujących się na terenie zarządzanym przez Administratora oraz ochrony jego praw.

Obszar objęty przez Administratora monitoringiem jest oznakowany za pomocą odpowiednich znaków graficznych.

REKRUTACJA

W ramach procesów rekrutacyjnych Administrator oczekuje przekazywania Danych osobowych (np. w CV lub życiorysie) jedynie w zakresie określonym w przepisach prawa pracy. W związku z tym nie należy przekazywać informacji w szerszym zakresie. W razie, gdy przesłane aplikacje będą zawierać dodatkowe dane, wykraczające poza zakres wskazany przepisami prawa pracy, ich przetwarzanie będzie oparte na zgodzie kandydata (art. 6 ust. 1 lit. a RODO), wyrażonej poprzez jednoznaczną czynność potwierdzającą, jaką jest przesłanie przez kandydata dokumentów aplikacyjnych. W przypadku, gdy przesłane aplikacje będą

zawierać informacje nieadekwatne do celu, jakim jest rekrutacja, nie będą one wykorzystywane ani uwzględniane w procesie rekrutacyjnym.

Dane osobowe są przetwarzane:

- w przypadku, gdy preferowaną formą zatrudnienia jest umowa o pracę – w celu wykonania obowiązków wynikających z przepisów prawa, związanych z procesem zatrudnienia, w tym przede wszystkim Kodeksu pracy – podstawą prawną przetwarzania jest obowiązek prawny ciążący na Administratorze (art. 6 ust. 1 lit. c RODO w związku z przepisami prawa pracy);

- w przypadku, gdy preferowaną formą zatrudnienia jest umowa cywilnoprawna – w celu prowadzenia procesu rekrutacyjnego – podstawą prawną przetwarzania danych zawartych w dokumentach aplikacyjnych jest podjęcie działań przed zawarciem umowy na żądanie osoby, której dane dotyczą (art. 6 ust. 1 lit b RODO);

- w celu przeprowadzenia procesu rekrutacji w zakresie danych niewymaganych przepisami prawa ani przez Administratora, a także dla celów przyszłych procesów rekrutacyjnych – podstawą prawną przetwarzania jest zgoda (art. 6 ust. 1 lit. a RODO);

- w celu weryfikacji kwalifikacji i umiejętności kandydata lub kandydatki oraz ustalenia warunków współpracy – podstawą prawną przetwarzania danych jest prawnie uzasadniony interes Administratora (art. 6 ust. 1 lit. f RODO). Prawnie uzasadnionym interesem Administratora jest weryfikacja kandydatów do pracy oraz określenie warunków ewentualnej współpracy;

- w celu ustalenia lub dochodzenia przez Administratora ewentualnych roszczeń lub obrony przed roszczeniami wysuwanymi wobec Administratora – podstawą prawną przetwarzania danych jest prawnie uzasadniony interes Administratora (art. 6 ust. 1 lit. f RODO).

W zakresie, w jakim Dane osobowe są przetwarzane na podstawie wyrażonej zgody, można tę zgodę wycofać w każdym czasie, bez wpływu na zgodność z prawem przetwarzania dokonanego przed jej wycofaniem. W przypadku wyrażenia zgody dla celów przyszłych procesów rekrutacyjnych, dane osobowe usuwane są po upływie dwóch lat – o ile wcześniej zgoda nie została wycofana.

Podanie danych w zakresie określonym w art. 22(1) Kodeksu pracy jest wymagane – w przypadku preferowania przez kandydata zatrudnienia w oparciu o umowę o pracę – przez przepisy prawa, w tym przede wszystkim przez Kodeks pracy, zaś w przypadku preferowania zatrudnienia w oparciu o umowę cywilnoprawną – przez Administratora. Konsekwencją niepodania tych danych jest brak możliwości rozpatrzenia danej kandydatury w procesie rekrutacyjnym. Podanie innych danych jest dobrowolne.

ZBIERANIE DANYCH W ZWIĄZKU ZE ŚWIADCZENIEM USŁUG LUB WYKONYWANIEM INNYCH UMÓW

W razie zbierania danych dla celów związanych z wykonaniem konkretnej umowy, Administrator przekazuje Podmiotowi danych szczegółowe informacje dotyczące przetwarzania jego danych osobowych w momencie zawierania umowy lub w momencie pozyskania danych osobowych w przypadku, gdy przetwarzanie jest niezbędne w celu podjęcia przez Administratora działań na żądanie Podmiotu danych, przed zawarciem umowy.

PRZETWARZANIE DANYCH OSOBOWYCH CZŁONKÓW PERSONELU KONTRAHENTÓW LUB KLIENTÓW WSPÓŁPRACUJĄCYCH Z ADMINISTRATOREM

W związku z zawieraniem umów handlowych w ramach prowadzonej działalności gospodarczej, Administrator pozyskuje od kontrahentów / klientów dane osób zaangażowanych w realizację takich umów (np. osób uprawnionych do kontaktu, składających zamówienia, wykonujących zlecenia itp.). Zakres przekazywanych danych jest w każdym wypadku ograniczony do stopnia niezbędnego dla wykonania umowy i zazwyczaj nie obejmuje innych informacji niż imię i nazwisko oraz służbowe dane kontaktowe.

Takie dane osobowe są przetwarzane w celu realizacji prawnie uzasadnionego interesu Administratora oraz jego kontrahenta (art. 6 ust. 1 lit. f RODO), polegającego na umożliwieniu prawidłowego i efektywnego wykonywania umowy. Takie dane mogą być ujawniane osobom trzecim zaangażowanym w realizację umowy, a także podmiotom uzyskującym dostęp do danych w oparciu o przepisy z zakresu jawności informacji publicznej oraz postępowań prowadzonych w oparciu o prawo zamówień publicznych, w zakresie przewidzianym przez te przepisy.

Dane przetwarzane są przez okres niezbędny do realizacji powyższych interesów oraz wykonania obowiązków wynikających z przepisów.

ZBIERANIE DANYCH W INNYCH PRZYPADKACH

W związku z prowadzoną działalnością Administrator zbiera Dane osobowe także w innych przypadkach – np. poprzez budowanie i wykorzystywanie trwałych wzajemnych kontaktów biznesowych (*networking*) podczas spotkań biznesowych, na wydarzeniach branżowych czy też poprzez wymianę wizytówek – w celach związanych z inicjowaniem i utrzymywaniem kontaktów biznesowych. Podstawą prawną przetwarzania jest w tym wypadku prawnie uzasadniony interes Administratora (art. 6 ust. 1 lit. f RODO), polegający na tworzeniu sieci kontaktów w związku z prowadzoną działalnością.

Dane osobowe zebrane w takich przypadkach przetwarzane są wyłącznie w celu, dla jakiego zostały zebrane, a Administrator zapewnia ich odpowiednią ochronę.

ODBIORCY DANYCH

W związku z prowadzeniem działalności wymagającej przetwarzania Dane osobowe są ujawniane zewnętrznym podmiotom, w tym w szczególności dostawcom odpowiedzialnym za obsługę systemów informatycznych i sprzętu (np. wyposażenia CCTV w zakresie monitoringu wizyjnego), podmiotom świadczącym usługi prawne lub księgowe, kurierom, agencjom marketingowym czy rekrutacyjnym. Dane są też ujawniane podmiotom powiązanym z Administratorem.

Administrator zastrzega sobie prawo ujawnienia wybranych informacji dotyczących Podmiotu danych właściwym organom bądź osobom trzecim, które zgłoszą żądanie udzielenia takich informacji, opierając się na odpowiedniej podstawie prawnej oraz zgodnie z przepisami obowiązującego prawa.

PRZEKAZYWANIE DANYCH POZA EOG

Poziom ochrony Danych osobowych poza Europejskim Obszarem Gospodarczym („**EOG**") różni się od tego zapewnianego przez prawo europejskie. Z tego powodu Administrator przekazuje Dane osobowe poza EOG tylko wtedy, gdy jest to konieczne, i z zapewnieniem odpowiedniego stopnia ochrony, przede wszystkim poprzez:

współpracę z podmiotami przetwarzającymi Dane osobowe w państwach, w odniesieniu do których została wydana stosowna decyzja Komisji Europejskiej dotycząca stwierdzenia zapewnienia odpowiedniego stopnia ochrony Danych osobowych;

stosowanie standardowych klauzul umownych wydanych przez Komisję Europejską;

stosowanie wiążących reguł korporacyjnych zatwierdzonych przez właściwy organ nadzorczy;

Administrator zawsze informuje o zamiarze przekazania Danych osobowych poza EOG na etapie ich zbierania.

OKRES PRZETWARZANIA DANYCH OSOBOWYCH

Okres przetwarzania danych przez Administratora zależy od rodzaju świadczonej usługi i celu przetwarzania. Okres przetwarzania danych może także wynikać z przepisów, gdy stanowią one podstawę przetwarzania. W przypadku przetwarzania danych na podstawie uzasadnionego interesu Administratora (np. ze względów bezpieczeństwa), dane przetwarzane są przez okres umożliwiający realizację tego interesu lub do zgłoszenia skutecznego sprzeciwu względem przetwarzania danych. Jeśli przetwarzanie odbywa się na podstawie zgody, dane przetwarzane są do jej wycofania. Gdy podstawę przetwarzania stanowi niezbędność do zawarcia i wykonania umowy, dane są przetwarzane do momentu jej rozwiązania.

Okres przetwarzania danych może zostać przedłużony w przypadku, gdy przetwarzanie jest niezbędne do ustalenia lub dochodzenia roszczeń lub obrony przed roszczeniami, a po tym okresie – jedynie w przypadku i w zakresie, w jakim będą wymagać tego przepisy prawa.

UPRAWNIENIA ZWIĄZANE Z PRZETWARZANIEM DANYCH OSOBOWYCH

PRAWA PODMIOTÓW DANYCH

Podmiotom danych przysługują następujące prawa:

prawo do informacji o przetwarzaniu danych osobowych – na tej podstawie Administrator przekazuje osobie fizycznej zgłaszającej żądanie informację o przetwarzaniu danych, w tym przede wszystkim o celach i podstawach prawnych przetwarzania,

zakresie posiadanych danych, podmiotach, którym są ujawniane, i planowanym terminie usunięcia danych;

prawo uzyskania kopii danych – na tej podstawie Administrator przekazuje kopię przetwarzanych danych dotyczących osoby fizycznej zgłaszającej żądanie;

prawo do sprostowania – Administrator zobowiązany jest usuwać ewentualne niezgodności lub błędy przetwarzanych Danych osobowych oraz uzupełniać je, jeśli są niekompletne;

prawo do usunięcia danych – na tej podstawie można żądać usunięcia danych, których przetwarzanie nie jest już niezbędne do realizowania żadnego z celów, dla których zostały zebrane;

prawo do ograniczenia przetwarzania – w razie zgłoszenia takiego żądania Administrator zaprzestaje wykonywania operacji na Danych osobowych – z wyjątkiem operacji, na które wyraziła zgodę osoba, której dane dotyczą, oraz przechowywania danych, zgodnie z przyjętymi zasadami retencji – lub dopóki nie ustaną przyczyny ograniczenia przetwarzania danych (np. zostanie wydana decyzja organu nadzorczego zezwalająca na dalsze przetwarzanie danych);

prawo do przenoszenia danych – na tej podstawie – w zakresie, w jakim dane są przetwarzane w sposób zautomatyzowany w związku z zawartą umową lub wyrażoną zgodą – Administrator wydaje dane dostarczone przez osobę, której one dotyczą, w formacie pozwalającym na odczyt danych przez komputer. Możliwe jest także zażądanie przesłania tych danych innemu podmiotowi, jednakże pod warunkiem, że istnieją w tym zakresie techniczne możliwości zarówno po stronie Administratora, jak również wskazanego podmiotu;

prawo sprzeciwu wobec przetwarzania danych w celach marketingowych – Podmiot danych może w każdym momencie sprzeciwić się przetwarzaniu Danych osobowych w celach marketingowych, bez konieczności uzasadnienia takiego sprzeciwu;

prawo sprzeciwu wobec innych celów przetwarzania danych – Podmiot danych może w każdym momencie sprzeciwić się – z przyczyn związanych z jego szczególną sytuacją – przetwarzaniu Danych osobowych, które odbywa się na podstawie prawnie uzasadnionego interesu Administratora (np. dla celów analitycznych lub statystycznych albo ze względów związanych z ochroną mienia); sprzeciw w tym zakresie powinien zawierać uzasadnienie;

prawo wycofania zgody – jeśli dane przetwarzane są na podstawie wyrażonej zgody, Podmiot danych ma prawo wycofać ją w dowolnym momencie, co jednak nie wpływa na zgodność z prawem przetwarzania dokonanego przed jej wycofaniem;

prawo do skargi – w przypadku uznania, że przetwarzanie Danych osobowych narusza przepisy RODO lub inne przepisy dotyczące ochrony Danych osobowych, Podmiot danych może złożyć skargę do organu nadzorującego przetwarzanie Danych osobowych, właściwego ze względu na miejsce zwykłego pobytu Podmiotu danych, jego miejsce pracy lub miejsce popełnienia domniemanego naruszenia. W Polsce organem nadzorczym jest Prezes Urzędu Ochrony Danych Osobowych.

ZGŁASZANIE ŻĄDAŃ ZWIĄZANYCH Z REALIZACJĄ PRAW

Żądanie dotyczące realizacji praw Podmiotów danych można zgłosić:

w formie pisemnej na adres: ul. Ułańska 25, Miedźno.

drogą elektroniczną na adres e-mail: marcin.pilch@aviso.pl

Jeżeli Administrator nie będzie w stanie zidentyfikować osoby fizycznej na podstawie zgłoszonego żądania, zwróci się do wnioskodawcy o dodatkowe informacje. Podanie takich danych nie jest obowiązkowe, jednak brak ich podania będzie skutkować odmową realizacji żądania.

Żądanie może zostać zgłoszone osobiście lub za pośrednictwem pełnomocnika (np. członka rodziny). Ze względu na bezpieczeństwo danych Administrator zachęca do posługiwania się pełnomocnictwem w formie poświadczonej przez notariusza lub upoważnionego radcę prawnego bądź adwokata, co istotnie przyspieszy weryfikację autentyczności żądania.

Odpowiedź na zgłoszenie powinna zostać udzielona w ciągu miesiąca od jego otrzymania. W razie konieczności przedłużenia tego terminu Administrator informuje wnioskodawcę o przyczynach tego działania.

W przypadku, w którym żądanie zostało skierowane do ADO elektronicznie, odpowiedzi udziela się w tej samej formie, chyba że wnioskodawca zażądał udzielenia odpowiedzi w innej formie. W innych przypadkach odpowiedzi udziela się pisemnie. W przypadku, gdy termin realizacji żądania uniemożliwia udzielenie odpowiedzi drogą pisemną, a zakres danych wnioskodawcy przetwarzanych przez Administratora umożliwia kontakt drogą elektroniczną, odpowiedzi udziela się drogą elektroniczną.

ADO przechowuje informacje dotyczące zgłoszonego żądania oraz osoby, która żądanie zgłosiła, w celu zapewnienia możliwości wykazania zgodności oraz w celu ustalenia, obrony lub dochodzenia ewentualnych roszczeń podmiotów danych. Rejestr żądań przechowywany jest w sposób zapewniający integralność i poufność zawartych w nim danych.

ZASADY POBIERANIA OPŁAT

Postępowanie w sprawie składanych wniosków jest nieodpłatne. Opłaty mogą zostać pobrane jedynie w przypadku:

zgłoszenia żądania wydania drugiej i każdej kolejnej kopii danych (pierwsza kopia danych jest bezpłatna); w takim wypadku Administrator może zażądać uiszczenia opłaty w wysokości 100 zł. Powyższa opłata zawiera koszty administracyjne związane z realizacją żądania;

zgłaszania przez tę samą osobę żądań nadmiernych (np. niezwykle częstych) lub ewidentnie nieuzasadnionych; w takim wypadku Administrator może zażądać uiszczenia opłaty w wysokości 500 zł. Powyższa opłata zawiera koszty prowadzenia komunikacji oraz koszty związane z podjęciem żądanych działań;

W razie kwestionowania decyzji o nałożeniu opłaty osoba, której dane dotyczą, może złożyć skargę do organu nadzorującego przetwarzanie Danych osobowych, właściwego ze względu na miejsce zwykłego pobytu tej osoby, jej miejsce pracy lub miejsce

popełnienia domniemanego naruszenia. W Polsce organem nadzorczym jest Prezes Urzędu Ochrony Danych Osobowych.

ZMIANY POLITYKI PRZETWARZANIA DANYCH OSOBOWYCH

Polityka jest na bieżąco weryfikowana i w razie potrzeby aktualizowana.

Aktualna wersja Polityki obowiązuje w dniu wskazanym w zarządzenia kierownika jednostki.

Informacja dotycząca przetwarzania danych pracowników oraz współpracowników Gminy Miedźno

1. **Administratorem** Pani/Pana* danych osobowych jest *Gmina Miedźno z siedzibą w Miedźnie ul. Ułańska 25, 42-120 Miedźno, NIP: 5742055080,* zwana dalej Administratorem.
2. **Inspektorem Ochrony Danych Osobowych** jest Marcin Pilch e-mail: marcin.pilch@aviso.pl, tel: 34 317 81 00.
3. **Pani/Pana* dane osobowe będą przetwarzane w celach** związanych z zawarciem oraz realizacją stosunku pracy, a mianowicie:
   a) *zawarcia i realizacji umowy o pracę, w szczególności wystawienia skierowania na badania wstępne, okresowe oraz kontrolne, prowadzenia akt pracowniczych, rozliczania listy płac i wypłaty wynagrodzeń, rozliczania zwolnień lekarskich i przyznanych zasiłków, przygotowania oraz realizacji aneksów zmieniających warunki zatrudnienia, przygotowywania wypowiedzenia umowy o pracę, przygotowania oraz nałożenia kar porządkowych, realizacji zajęcia wynagrodzenia za pracę, wystawiania oraz doręczenia świadectwa pracy, wystawiania oraz wysyłki dokumentacji PIT, przygotowania i doręczenia innych niż wymienione powyżej dokumentów związanych ze stosunkiem pracy;*

   b) *opieki medycznej lub ochrony ubezpieczeniowej dla pracowników i członków rodzin pracowników;*

   c) *świadczeń dodatkowych dla pracowników oraz członków rodzin pracowników*

   d) *uczestnictwa w szkoleniach prowadzonych przez osoby trzecie;*

   e) *bezpieczeństwa i higieny pracy (szkolenia BHP, przygotowanie dokumentacji zaistniałych wypadków).*

4. **Podstawę prawną przetwarzania Pani/Pana* danych osobowych stanowią**):
   a) *wykonanie umowy, której jest Pani/Pan Stroną;*

   b) *konieczność wypełnienia obowiązków prawnych ciążących na Administratorze, szczególności wynikających z: ustawy z 26.06.1974 r. – Kodeks pracy, ustawy z 13.10.1998 r. o systemie ubezpieczeń społecznych oraz ustawy z 26.07.1991 r. o podatku dochodowym od osób fizycznych;*

   c) *prawnie uzasadniony interes realizowany przez Administratora, np. udzielanie odpowiedzi na Pani/Pana pisma i wnioski;*

   d) *udzielona przez Panią/Pana zgoda.*

5. **Pani/Pana* dane osobowe Administrator może przekazać odpowiednim odbiorcom**, w szczególności podmiotom zewnętrznym, takim jak:
   a) Zakład Ubezpieczeń Społecznych;
   b) urzędy skarbowe;
   c) banki;
   d) podmioty współpracujące w celu zapewnienia świadczeń z Zakładowego Funduszu Świadczeń Socjalnych;
   e) podmioty współpracujące w zakresie obsługi prawnej;
   f) podmioty współpracujące w zakresie obsługi BHP, organizacji szkoleń i konferencji, wyjazdów, usług transportowych oraz kurierskich;
   g) podmioty współpracujące w zakresie ewentualnej ochrony ubezpieczeniowej;

   h) podmioty współpracujące w zakresie ewentualnej opieki medycznej;

   i) podmioty współpracujące w zakresie ewentualnych świadczeń dodatkowych

j) podmioty przetwarzające dane osobowe w imieniu i na rzecz Administratora (np. podmiot sprawujący nadzór nad siecią informatyczną.);

k) kontrahenci Administratora (w celu realizacji zawartych umów);

l)podmioty lub organy uprawnione do uzyskania danych osobowych na podstawie przepisów prawa (w tym sądy, prokuratorzy, komornicy, organy regulacyjne i nadzorcze).

6. **Administrator nie zamierza przekazywać Pani/Pana* danych osobowych do państw trzecich** (tj. państw spoza Europejskiego Obszaru Gospodarczego obejmującego Unię Europejską, Norwegię, Liechtenstein i Islandię) oraz do organizacji międzynarodowych. Jeśli jednak zaistnieje powyższa potrzeba, Administrator będzie przekazywać dane osobowe, zapewniając odpowiedni poziom ich ochrony oraz stosując odpowiednie przepisy prawa.
7. **Posiada Pani/Pan* prawo dostępu** do treści swoich danych osobowych, ich sprostowania, usunięcia, ograniczenia przetwarzania oraz prawo do przenoszenia danych osobowych i wniesienia sprzeciwu wobec ich przetwarzania – w przypadkach i na zasadach określonych w przepisach RODO.
8. **Przysługuje Pani/Panu* także prawo wniesienia skargi do organu nadzorczego –** Prezesa Urzędu Ochrony Danych Osobowych z siedzibą w Warszawie przy ul. Stawki 2, 00-193 Warszawa, gdy uznają Państwo, iż przetwarzanie ich danych osobowych narusza przepisy RODO.
9. **W każdym czasie ma Pani/Pan* prawo cofnięcia wyrażonej zgody**. Wycofanie zgody nie ma wpływu na zgodność z prawem przetwarzania danych osobowych, którego dokonano na podstawie zgody udzielonej przed jej cofnięciem.
10. **Pani/Pana* dane osobowe będą przechowywane przez okres** trwania stosunku pracy oraz w obowiązkowym okresie przechowywania dokumentacji związanej ze stosunkiem pracy i akt osobowych po jego ustaniu, ustalonym zgodnie z odrębnymi przepisami. Przykładowe okresy, przez jakie Pani/Pana dane osobowe mogą być przechowywane po ustaniu stosunku pracy:
akta pracownicze – 10 lat, licząc od końca roku kalendarzowego, w którym stosunek pracy uległ rozwiązaniu lub wygasł *[uwaga: z dniem 1.01.2019 r. weszła w życie ustawa z 10.01.2018 r. o zmianie niektórych ustaw w związku ze skróceniem okresu przechowywania akt pracowniczych oraz ich elektronizacją (Dz.U. poz. 357). Skrócony (z 50 do 10 lat) okres przechowywania akt pracowniczych, co do zasady z modyfikacjami określonymi w ww. ustawie z 10.01.2018 r., obowiązuje w stosunku do nowych pracowników, czyli zatrudnionych po dniu wejścia w życie ww. ustawy, tj. po 1.01.2019 r. Okres przechowywania dokumentacji w sprawach związanych ze stosunkiem pracy oraz akt osobowych pracownika i byłego pracownika dotyczących stosunków pracy nawiązanych przed 1.01.2019 r. ustala się na podstawie przepisów obowiązujących przed 1.01.2019 r. (tj. według starych zasad)]*;

11. **Pani/Pana* dane osobowe nie będą podlegać zautomatyzowanemu podejmowaniu decyzji, w tym profilowaniu** *(jeżeli omawiany proces ma miejsce, należy wskazać istotne informacje o zasadach ich podejmowania, a także informacje o znaczeniu i przewidywanych konsekwencjach takiego przetwarzania dla osoby, której dane dotyczą).*

.

.....

(podpis – imię i nazwisko administratora

lub osoby uprawnionej do składania

oświadczeń w imieniu administratora)

Rejestr czynności przetwarzania danych osobowych

Administrator Danych Osobowych: Gmina Miedźno

Inspektor Ochrony Danych: Marcin Pilch e-mail: marcin.pilch@aviso.pl

Ogólny opis technicznych i organizacyjnych środków bezpieczeństwa zastosowanych do ochrony danych osobowych określa

Polityka Ochrony Danych Osobowych wdrożona do stosowania u Administratora Danych Osobowych

Dane osobowe nie są przekazywane do żadnych odbiorców w państwach trzecich i w organizacjach międzynarodowych

L.p.	**NAZWA CZYNNOŚCI /PROCESU** **(aktywności) przetwarzania danych osobowych** **(zbiory, zestawy danych osobowych)**	**CELE PRZETWARZANIA** **Podstawa prawna przetwarzania**	**OPIS KATEGORII OSÓB, KTÓRYCH DANE DOTYCZĄ, ORAZ KATEGORII DANYCH OSOBOWYCH**	**KATEGORIE ODBIORCÓW, KTÓRYM DANE OSOBOWE ZOSTAŁY LUB ZOSTANĄ UJAWNIONE** ("odbiorca" oznacza osobę fizyczną lub prawną, organ publiczny, jednostkę lub inny podmiot, któremu ujawnia się dane osobowe, niezależnie od tego, czy jest stroną trzecią. Organy publiczne, które mogą otrzymywać dane, osobowe w ramach konkretnego postępowania zgodnie z prawem, nie są jednak uznawane za odbiorców)	**PLANOWANE TERMINY USUNIĘCIA POSZCZEGÓLNYCH KATEGORII DANYCH** (Jeżeli jest to możliwe. a gdy nie jest to możliwe, kryteria ustalania tego okresu)

1.	PRZETWARZANIE DANYCH OSOBOWYCH W ZWIĄZKU Z ZATRUDNIENIEM	Cel: Wypełnienie obowiązku prawnego związanego z zatrudnieniem, obsługa kadrowo-płacowa pracowników Podstawy prawne - Realizacja Umowy o pracę - Przepisy prawa pracy, o ubezpieczeniu społecznym i ordynacji podatkowej (art. 6 ust. 1 lit. c RODO), - Zgoda pracownika na przetwarzanie danych wykraczających poza wymagane przepisami prawa (art. 6 ust. 1 lit. a RODO) - Wypełnienie obowiązków w dziedzinie prawa pracy, zabezpieczenia społecznego i ochrony socjalnej (art. 9 ust. 2 lit. b RODO)	Pracownicy, a także dane osobowe dzieci pracownika i innych członków jego najbliższej rodziny, jeżeli podanie takich danych jest konieczne ze względu na korzystanie przez pracownika ze szczególnych uprawnień przewidzianych w prawie pracy. Dane identyfikacyjne, PESEL, a w przypadku jego braku - rodzaj i numer dokumentu potwierdzającego tożsamość; data urodzenia; dane adresowe i kontaktowe, dane o wykształceniu; dane o przebiegu pracy i stażu pracy, o absencji (zwolnienia chorobowe, urlopy, urlopy rehabilitacyjne, szkoleniowe i inne), dane o zakresie obowiązków, stawce wynagrodzenia, karach i nagrodach oraz inne dane wymagane zgodnie z Kodeksem pracy, przepisami o ubezpieczeniu społecznym i ordynacji podatkowej.	*Należy wskazać dane podmiotów przetwarzających dane w imieniu ADO, np. firmy informatyczne, dostawcę systemu kadrowego, archiwizującą dokumenty, niszczącą dokumenty, itd.* Odbiorcami będą także podmioty upoważnione do tego na podstawie przepisów prawa (ZUS, US), banki, ubezpieczyciele, kurierzy.	Dane są przechowywane przez okres określony w szczegółowych przepisach prawa Akta osobowe są przechowywane zgodnie z zasadami określonymi w art. 51u ust 1 ustawy z dnia 14.07.1983 r. o narodowym zasobie archiwalnym i archiwach - 10 lub 50 lat w zależności od daty rozpoczęcia pracy przez pracownika. W przypadku danych przetwarzanych na podstawie zgody, do czasu wycofania zgody lub ustania celu, w szczególności rozwiązania umowy o pracę.
2.	PROWADZENIE ZAKŁADOWEGO FUNDUSZU ŚWIADCZEŃ SOCJALNYCH	Wypełnienie obowiązku prawnego - Pomoc materialna i rzeczowa dla pracowników	Pracownicy oraz osoby, których dane są wskazywane we wnioskach o przyznanie świadczenia.	*Należy wskazać dane podmiotów przetwarzających dane w imieniu ADO, np. firmy informatyczne, firmę archiwizującą dokumenty,*	Pracodawca przetwarza dane osobowe przez okres niezbędny do przyznania ulgowej usługi i świadczenia,

		Przepisy prawa: * Ustawa o ZFŚS oraz przepisy ordynacji podatkowej * Wypełnienie obowiązków i wykonywanie szczególnych praw w dziedzinie prawa pracy, zabezpieczenia społecznego i ochrony socjalnej	Dane wnioskodawcy w zakresie danych identyfikacyjnych, kontaktowych, adresowych, miejsce pracy, stanowisko, stan cywilny, liczba osób w rodzinie, liczba osób pozostających na wyłącznym utrzymaniu, roczny, dochód oraz inne informacje i dane dołączone do wniosku, jeżeli mają znaczenie dla sprawy.	*niszczącą dokumenty, kancelarię prawną, itd.* Odbiorcami będą także podmioty upoważnione do tego na podstawie przepisów prawa (ZUS, US), banki, ubezpieczyciele, kurierzy.	dopłaty z Funduszu oraz ustalenia ich wysokości, a także przez okres niezbędny do dochodzenia praw lub roszczeń, ale nie dłużej niż do czasu przedawnienia tych roszczeń, tzn. 3 lata. W przypadku wystąpienia obowiązku podatkowego w związku z przyznanym świadczeniem dane będą przechowywane przez okres 5 lat kalendarzowych licząc od kolejnego roku, po którym nastąpił obowiązek podatkowy.
3.	PROWADZENIE SPRAW ZWIĄZANYCH Z EWIDENCJĄ GRUNTÓW I BUDYNKÓW	Wypełnienie obowiązku prawnego - ustawa z dnia 17 maja 1989 r. Prawo geodezyjne i kartograficzne. W zakresie kontaktu drogą elektroniczną zgoda osoby, której dane dotyczą.	Osoby fizyczne - nazwiska i imiona, imiona rodziców, adres zamieszkania lub pobytu, numer ewidencyjny PESEL, informacje o własności, tytule nabycia lub zbycia nieruchomości, dane zawarte w dokumentach przekazywanych przez zobligowane organy i podmioty, jak sądy, notariusze, organy administracji publicznej.	Odbiorcy danych mających dostęp do ewidencji gruntów i budynków,	*Należy wskazać okresy przechowywania danych wskazane w JRWA jednostki.*

4.	PROWADZENIE SPRAW BUDOWLANYCH	Wypełnienie obowiązku prawnego - ustawa z dnia 7 lipca 1994 r. Prawo budowlane; Ustawa z dnia 24 czerwca 1994 r. o własności lokali. W zakresie kontaktu drogą elektroniczną zgoda osoby, której dane dotyczą.	Dane inwestorów: nazwy podmiotów, dane adresowe i kontaktowe, informacje o pozwoleniu na budowę, dane osób działających w imieniu inwestora, dane dotyczące nieruchomości Dane kierownika budowy: dane identyfikacyjne, oświadczenia dotyczące budowy, nr uprawnień, nazwiska i imiona, adres zamieszkania lub pobytu.	Podmioty i organy uprawnione do uzyskania danych na podstawie przepisów prawa, operatorzy pocztowi.	*Należy wskazać okresy przechowywania danych wskazane w JRWA jednostki.*
5.	REJESTROWANIE STOWARZYSZEŃ	Ustawa z dnia 7 kwietnia 1989 r. Prawo o stowarzyszeniach. W zakresie kontaktu drogą elektroniczną zgoda osoby, której dane dotyczą.	Przedstawiciele Stowarzyszenia - nazwiska i imiona, nazwa stowarzyszenia, pełniona funkcja, dane adresowe i kontaktowe.	Podmioty i organy uprawnione do uzyskania danych na podstawie przepisów prawa, operatorzy pocztowi.	*Należy wskazać okresy przechowywania danych wskazane w JRWA jednostki.*
6.	PRZYJMOWANIE SKARG I PROWADZENIE POSTĘPOWAŃ WYNIKAJĄCYCH Z OTRZYMANYCH SKARG	Ustawa z dnia 14 czerwca 1960 r. Kodeks postępowania administracyjnego. Rozporządzenie Rady Ministrów z dnia 8 stycznia 2002r. w sprawie organizacji, przyjmowania i rozpatrywania skarg i wniosków	Osoby fizyczne, Interesanci, sygnaliści - nazwiska i imiona, adres zamieszkania, informacje zawarte w skargach.	Podmioty i organy uprawnione do uzyskania danych na podstawie przepisów prawa. W stosownych przypadkach strony postępowania, operatorzy pocztowi.	*Należy wskazać okresy przechowywania danych wskazane w JRWA jednostki.*
7.	REALIZACJA ZAMÓWIEŃ PUBLICZNYCH	Udzielenie zamówienia publicznego Ustawa z dnia 29 stycznia 2004 r.- Prawo zamówień publicznych.	Oferenci i Wykonawcy postępowań o udzielenie zamówienia publicznego - nazwiska i imiona, imiona rodziców, data urodzenia, miejsce urodzenia, adres	Podmioty i organy uprawnione do uzyskania danych na podstawie przepisów prawa.	*Należy wskazać okresy przechowywania danych wskazane w JRWA jednostki.*

			zamieszkania, PESEL, miejsce pracy, zawód, wykształcenie, seria i nr dowodu osobistego, nr telefonu, REGON, nazwisko rodowe, nazwisko rodowe matki, zaświadczenie z KRK, e-mail, adres prowadzonej działalności gospodarczej, informacje o niezaleganiu z opłatami składek na ubezpieczenie zdrowotne i społeczne, informacje o niezaleganiu z podatkiem, a także inne informacje wymagane przepisami prawa.	Osoby zainteresowane postępowaniem, w zakresie danych, które będą podlegały ujawnieniu w ramach informacji publicznej. W stosownych przypadkach strony postępowania, operatorzy pocztowi.	
8.	ZAPEWNIENIE BEZPIECZEŃSTWA POPRZEZ MONITORING WIZYJNY	Zapewnienie porządku publicznego i bezpieczeństwa obywateli oraz ochrony przeciwpożarowej i przeciwpowodziowej Obowiązek wynikający z przepisów prawa - Ustawa z dnia 8 marca 1990 r. o samorządzie gminnym.	Osoby objęte monitoringiem (pracownicy, interesanci). Wizerunek, data i czas nagrania, dane pojazdów.	Organy ścigania, jeżeli nagranie jest dowodem w sprawie.	*Należy wskazać faktyczny czas przechowywania, nie dłuższy niż 3 miesiące.*
9.	DZIAŁANIA PODEJMOWANE NA RZECZ RADY GMINY	Obowiązek wynikający z przepisów prawa - Ustawa z dnia 8 marca 1990 r. o samorządzie	Radni - nazwiska i imiona, adres zamieszkania, nr telefonu, Inne informacje dotyczące wykonywania przez radnego zadań mających związek z wykonywaniem przez	Podmioty i organy uprawnione do uzyskania danych na podstawie przepisów prawa. Osoby uzyskujące dane w ramach dostępu do	*Należy wskazać okresy przechowywania danych wskazane w JRWA jednostki.*

		gminnym. W zakresie kontaktu drogą elektroniczną zgoda osoby, której dane dotyczą.	niego mandatu, informacje dotyczące stanu majątkowego.	informacji publicznej, operatorzy pocztowi.	
10.	PROWADZENIE REJESTRU KORESPONDENCJI	Ewidencjowanie wszelkich dokumentów wychodzących i przychodzących, a także danych odbiorców i nadawców. Działanie realizowane w interesie publicznym.	Nadawcy i odbiorcy korespondencji - nazwiska i imiona, adres zamieszkania, nr sprawy.	Osoby uzyskujące dane w ramach dostępu do informacji publicznej.	*Należy wskazać okresy przechowywania danych wskazane w JRWA jednostki.*
11.	UDOSTĘPNIANIE INFORMACJI PUBLICZNEJ	Ustawa z dnia 6 września 2001 r. o dostępie do informacji publicznej.	Wnioskodawcy - nazwiska i imiona, adres zamieszkania lub pobytu, nr telefonu, adres poczty elektronicznej. Dane upubliczniane w BIP w zakresie kandydatów na stanowiska (imiona, nazwiska, postępowanie), dane pracowników (stanowisko, wydział, dane kontaktowe), oświadczenia majątkowe (dane identyfikacyjne, dane związane z majątkiem).	Osoby uzyskujące dane w ramach dostępu do informacji publicznej.	*Należy wskazać okresy przechowywania danych wskazane w JRWA jednostki, a także wynikające z przepisów prawa, np. dla oświadczeń majątkowych, czy danych kandydatów.*
12.	ARCHIWIZACJA DOKUMENTÓW	Ustawa z dnia 14 lipca 1983 r. o narodowym zasobie archiwalnym i archiwach.	Dane osób znajdujących się w dokumentach podlegających archiwizacji - nazwiska i imiona, data urodzenia, miejsce urodzenia, adres zamieszkania lub pobytu, nr telefonu,adres poczty elektronicznej, PESEL, miejsce	Podmioty i organy uprawnione do uzyskania danych na podstawie przepisów prawa. Osoby uzyskujące dane w ramach dostępu do	Dane są przechowywane zgodnie z przyjętymi kategoriami archiwalnymi wskazanymi w JRWA.

			pracy, zawód, nr dowodu, adres email, imiona rodziców, NIP, wykształcenie, miejsce pracy, zawód.	informacji publicznej, operatorzy pocztowi.	

DOKUMENTACJA PRZETWARZANIA DANYCH OSOBOWYCH [FIRMA ADMINISTRATORA]

1. REJESTR CZYNNOŚCI PRZETWARZANIA DANYCH OSOBOWYCH
2. REJESTR KATEGORII CZYNNOŚCI PRZETWARZANIA

Administrator danych osobowych:

[nazwa Administratora]
[adres]
[NIP]

Inspektor ochrony danych:

Marcin Pilch
marcin.pilch@aviso.pl
600379700

REJESTR CZYNNOŚCI PRZETWARZANIA DANYCH OSOBOWYCH

Lp.	Czynność przetwarzania	Współadministrator	Cele przetwarzania	Opis kategorii osób, których dane dotyczą	Opis kategorii danych osobowych	Kategorie odbiorców	Przekazanie danych osobowych do państwa trzeciego lub organizacji międzynarodowej	Planowane terminy usunięcia poszczególnych kategorii danych	Chwila, od której liczony jest termin usunięcia danych	Ogólny opis technicznych i organizacyjnych środków bezpieczeństwa	Dane wprowadził/a	Data wprowadzenia informacji do rejestru	Dane zmienił/a	Data zmiany informacji w rejestrze	Treść zmiany	Powód zmiany
	Należy wskazać czynność przetwarzania, tzn. czynność obejmującą wiele operacji przetwarzania podejmowanych dla realizacji jednolitych celów przetwarzania danych osobowych.	Należy wypełnić tylko w przypadku, gdy w procesie występuje współadministrator; w pozostałych przypadkach wskazać: n/d	Należy wskazać, w punktach, wszystkie cele przetwarzania w ramach opisywanej czynności.	Należy wymienić wszystkie kategorie osób, których dane przetwarzane są w ramach opisywanej czynności.	Należy wskazać kategorie danych przetwarzanych w odniesieniu do kategorii osób wskazanych w kolumnie E. Przez kategorie danych należy rozumieć dane o analogicznym charakterze (np. dane kontaktowe - obejmujące numer telefonu i adres e-mail, historię zamówień, dane zawarte w CV itd.). W przypadku, gdy zakresy danych osobowych przetwarzanych w poszczególnych celach wskazanych w kolumnie D różnią się od siebie, należy określić kategorie danych w punktach, odrębnie dla poszczególnych celów.	Należy wskazać kategorie podmiotów, którym dane zostały lub zostaną ujawnione, w tym odbiorców w państwach trzecich lub w organizacjach międzynarodowych. Nie należy wskazywać organów publicznych, którym ujawniono dane osobowe w ramach konkretnego postępowania.	Należy wskazać: a) nazwę państwa trzeciego lub organizacji międzynarodowej, którym przekazywane są dane osobowe; b) instrument prawny, na podstawie którego przekazywane są dane osobowe (np. wiążące reguły korporacyjne, zatwierdzone przez organ nadzorczy).	Należy wskazać terminy usunięcia danych. W przypadku, gdy terminy usunięcia danych dla poszczególnych celów wskazanych w kolumnie D różnią się od siebie, należy wskazać w punktach terminy odpowiadające poszczególnym celom przetwarzania danych osobowych.	Należy wskazać zdarzenie, od którego zajścia liczony jest termin usunięcia danych.	Należy w sposób ogólny opisać stosowane środki bezpieczeństwa, wdrożone na podstawie art. 32 RODO.						
1																
2																
3																
4																
5																
6																
7																

REJESTR KATEGORII CZYNNOŚCI PRZETWARZANIA DANYCH OSOBOWYCH

Lp.	Nazwa administratora	Dane kontaktowe administratora	Dane Inspektora Ochrony Danych Administratora	Kategorie przetwarzań	Przekazanie danych osobowych do państwa trzeciego lub organizacji międzynarodowej	Ogólny opis technicznych i organizacyjnych środków bezpieczeństwa	Dane wprowadził/a	Data wprowadzenia informacji do rejestru	Dane zmienił/a	Data zmiany informacji w rejestrze	Treść zmiany	Powód zmiany
	Należy wskazać firmę lub nazwę administratora danych, w imieniu którego działa podmiot przetwarzający.	Należy wskazać adres siedziby administratora danych, w którego imieniu realizowane jest przetwarzania. W każdym przypadku gdy to możliwe, należy wskazać ponadto adres e-mail oraz nr telefonu. administratora danych.	Jeśli administrator powołał Inspektora Ochrony Danych, należy podać jego: a) imię i nazwisko b) adres e-mail c) nr telefonu	Należy wymienić kategorie przetwarzań realizowanych w imieniu administratora. Przez przetwarzania należące do jednej kategorii należy rozumieć przetwarzania posiadające tożsamy charakter (wymagające od procesora analogicznych czynności), np. hosting danych.	Należy wskazać: a) nazwę państwa trzeciego lub organizacji międzynarodowej, którym przekazywane są dane osobowe; b) instrument prawny, na podstawie którego przekazywane są dane osobowe (np. wiążące reguły korporacyjne, zatwierdzone przez organ nadzorczy).	Należy w sposób ogólny opisać stosowane środki bezpieczeństwa, wdrożone na podstawie art. 32 RODO, przy czym dopuszczalne jest odwołanie się do stosownych postanowień umowy powierzenia.						
1												
2												
3												
4												
5												
6												
7												
8												
9												
10												

GMINA MIEDŹNO

POLITYKA RETENCJI DANYCH OSOBOWYCH

METRYKA DOKUMENTU	
WERSJA DOKUMENTU	1.0
DATA DOKUMENTU	31.10.2023 r.
LICZBA STRON	183
CEL DOKUMENTU	Niniejszy dokument opisuje zasady usuwania danych osobowych po upływie okresu retencji oraz wskazuje okresy retencji dla poszczególnych procesów przetwarzania danych **w zakresie nieuregulowanym powszechnie obowiązującymi przepisami prawa przez okres z nich wynikający, w szczególności ustawy z dnia 14 lipca 1983 r. o narodowym zasobie archiwalnym i archiwach oraz rozporządzenia Prezesa Rady Ministrów z dnia 18 stycznia 2011 r. w sprawie instrukcji kancelaryjnej, jednolitych rzeczowych wykazów akt oraz instrukcji w sprawie organizacji i zakresu działania archiwów zakładowych.**
SPIS TREŚCI	1. Definicje ..... 34 2. Zasady ogólne ..... 34 3. Okresy retencji Danych osobowych ..... 35 4. Usuwanie danych ..... 35 5. Postanowienia końcowe ..... 36 Załącznik A – Tabela okresów retencji 37

10. DEFINICJE

10.1. **Administrator– Gmina Miedźno** z siedzibą w Miedźnie ul. Ułańska 25, 42-120 Miedźno, NIP: 5742055080

10.2. **Dane osobowe –** informacje o osobie fizycznej zidentyfikowanej lub możliwej do zidentyfikowania poprzez jeden bądź kilka szczególnych czynników określających fizyczną, fizjologiczną, genetyczną, psychiczną, ekonomiczną, kulturową lub społeczną tożsamość, w tym IP urządzenia, dane o lokalizacji, identyfikator internetowy oraz informacje gromadzone za pośrednictwem plików cookie czy innej podobnej technologii.

10.3. **IOD –** Inspektor Ochrony Danych, wyznaczony przez Gminę, nadzorujący przestrzeganie przepisów o ochronie danych osobowych w Gminie, wykonujący zadania określone w art. 39 RODO.

10.4. **Osoba dedykowana –** pracownik lub współpracownik zobowiązany do wykonania czynności technicznych związanych z usunięciem danych osobowych z systemów informatycznych lub zasobów papierowych Gminie; Osoby dedykowane w Gminie wyznaczane są na zasadach określonych w odrębnej procedurze.

10.5. **Polityka –** niniejsza polityka retencji danych osobowych.

10.6. **RCP –** rejestr czynności przetwarzania, o którym mowa w art. 30 RODO, prowadzony przez Gminę.

10.7. **RODO –** rozporządzenie Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE.

10.8. **Tabela –** tabela okresów retencji stanowiąca załącznik A do Polityki.

11. ZASADY OGÓLNE

11.1. Gmina przetwarza Dane osobowe z uwzględnieniem zasady ograniczenia przechowywania i zapewnia, że Dane osobowe przetwarzane są tylko tak długo, jak długo jest to uzasadnione oraz zgodne z przepisami prawa (okres retencji).

11.2. W przypadkach, gdy okresy retencji Danych osobowych nie wynikają wyraźnie z przepisów prawa, Gmina ustala te okresy samodzielnie. W przypadku, gdy okres retencji wynika z przepisów prawa, ma on pierwszeństwo przed postanowieniami Polityki i RCP.

11.3. Gmina zapewnia, że w przypadku dezaktualizacji wszystkich celów przetwarzania Danych osobowych nie są realizowane jakiekolwiek operacje na tych danych z wyjątkiem ich usunięcia (przy czym przez usunięcie należy również rozumieć nieodwracalną anonimizację danych).

12. OKRESY RETENCJI DANYCH OSOBOWYCH

12.1. Okresy retencji danych zostały określone w RCP.

12.2. Okresy retencji, znajdujące zastosowanie w najbardziej powszechnych procesach realizowanych w Gminie, zostały wskazane ponadto w Tabeli, która stanowi załącznik A do Polityki. Tabela ma charakter wyłącznie informacyjny. Wiążące okresy retencji wskazane zostały w RCP.

12.3. Ustalając okresy retencji, uwzględniono w szczególności:

12.3.1. obowiązki prawne ciążące na Gminie w zakresie przechowywania określonych Danych osobowych lub dokumentów zawierających Dane osobowe, wynikające z przepisów prawa;

12.3.2. potencjalną niezbędność przetwarzania danych dla celów związanych z ustalaniem lub dochodzeniem roszczeń oraz obroną przed takimi roszczeniami i związane z tym okresy przedawnienia roszczeń wynikające z Kodeksu cywilnego.

12.4. Okresy retencji określone w RCP mogą ulegać zmianie w związku ze zmianą obowiązujących przepisów prawa mających wpływ na okres retencji lub w związku z decyzją IOD, o czym osoby zatrudnione w Gminie oraz z nią współpracujące zostaną poinformowane. Przyczyny decyzji IOD o zmianie okresu retencji powinny być odnotowane w RCP.

13. USUWANIE DANYCH

13.1. Za usuwanie Danych osobowych zgodnie z obowiązującymi okresami retencji odpowiedzialna jest Osoba dedykowana.

13.2. Przed usunięciem danych należy zweryfikować, czy nie zachodzą przesłanki wydłużenia okresu retencji, w szczególności poprzez sprawdzenie, czy:

13.2.1. nie występuje obowiązek prawny ciążący na Gminie, którego wykonanie wymaga przetwarzania Danych osobowych, a który nie został uwzględniony w Tabeli lub RCP;

13.2.2. nie nastąpiło przerwanie lub zawieszenie okresu przedawnienia roszczeń, zgodnie z właściwymi przepisami, skutkujące koniecznością dalszego przetwarzania Danych osobowych;

13.2.3. dalsze przechowywanie nie jest konieczne w związku z biegnącym okresem przedawnienia zobowiązań podatkowych.

13.3. W razie wątpliwości przed usunięciem danych Osoba dedykowana zasięga opinii IOD.

13.4. Usunięcie danych powinno nastąpić niezwłocznie po upływie okresu retencji, z uwzględnieniem okresu koniecznego do podjęcia niezbędnych czynności technicznych i organizacyjnych związanych z usunięciem Danych osobowych, jednak nie później niż ostatniego dnia roku kalendarzowego, w którym upłynął okres retencji.

14. POSTANOWIENIA KOŃCOWE

14.1. IOD zobowiązany jest do bieżącego monitorowania wykonywania Polityki, a w razie potrzeby zawiadomienia Gminie o konieczności jej aktualizacji. IOD uprawniony jest do samodzielnej aktualizacji Tabeli. W razie takiej aktualizacji IOD zobowiązany jest poinformować o wprowadzonych zmianach Osoby dedykowane oraz Kierownika jednostki..

14.2. Postanowienia Polityki dotyczące IOD stosuje się odpowiednio wobec KODO.

14.3. Polityka wchodzi w życie z dniem wskazanym w zarządzeniu Wójta Gminy Miedźno.

14.4. Integralną część Polityki stanowi:

14.4.1. Załącznik A – Tabela okresów retencji.

Załącznik A – Tabela okresów retencji

Lp.	Cel przetwarzania Danych osobowych	Typowe dokumenty oraz nośniki, z których należy usunąć dane	Maksymalny termin usunięcia danych	Moment, od którego liczony jest termin usunięcia danych
1.	**Prowadzenie procesów rekrutacyjnych**	CV życiorys list motywacyjny treść e-maila, w którym przesłano dokumenty aplikacyjne	Niezwłocznie / 3 lata[1]	Zakończenie postępowania rekrutacyjnego, które nie zakończyło się zatrudnieniem postępowania i nie wyrażono zgody na przetwarzanie danych w celu przyszłych rekrutacji.
2.	**Prowadzenie bazy danych potencjalnych kandydatów na potrzeby przyszłych rekrutacji**	CV życiorys list motywacyjny treść e-maila, w którym przesłano dokumenty aplikacyjne	2 lata lub moment wycofania zgody, jeśli nastąpił wcześniej	Zakończenie postępowania rekrutacyjnego lub otrzymanie aplikacji (jeżeli rekrutacja nie była prowadzona).
3.	**Wykonywanie umowy pracowniczej**	CV życiorys list motywacyjny	50 lat / 10 lat[2] (z wyjątkiem dokumentów, wobec których konieczność dłuższego przechowywania wynika	Zakończenie stosunku pracy.

[1] Termin przedawnienia roszczeń ze stosunku pracy (art. 291 § 1 Kodeksu pracy).

[2] Okres przechowywania dokumentacji pracowniczej został skrócony do 10 lat dla stosunków pracy zawartych po 1 stycznia 2019 r. Okres przechowywania dokumentacji w sprawach związanych ze stosunkiem pracy oraz akt osobowych pracownika dotyczących stosunków pracy nawiązanych po 31 grudnia 1998 r., a przed 1 stycznia 2019 r. ulega skróceniu w przypadku złożenia raportu informacyjnego, o którym mowa w art. 7 ustawy z dnia 10 stycznia 2018 r. o zmianie niektórych ustaw w związku ze skróceniem okresu przechowywania akt pracowniczych oraz ich elektronizacją.

Lp.	Cel przetwarzania Danych osobowych	Typowe dokumenty oraz nośniki, z których należy usunąć dane	Maksymalny termin usunięcia danych	Moment, od którego liczony jest termin usunięcia danych
		treść e-maila, w którym przesłano dokumenty aplikacyjne dokumentacja pracownicza	z właściwych przepisów prawa, oraz przypadków, gdy przechowywanie jest niezbędne z uwagi na bieg przedawnienia dla zobowiązań podatkowych). Powyższe okresy nie obejmują danych dotyczących wymierzenia kar porządkowych, które powinny być przechowywane przez **1 rok** (okres nienagannej pracy pracownika od momentu wymierzenia kary, po którym kara uważana jest za niebyłą).	
3.	**Wykonywanie umowy pracowniczej**	dokumentacja związana z oceną pracowniczą dokumentacja wytworzona w związku z utrzymywaniem ZFŚS umowy dotyczące dofinansowania szkoleń oraz inne umowy cywilnoprawne z pracownikami dokumentacja związana z obsługą świadczeń dodatkowych (pakiety sportowe, medyczne, ubezpieczenia grupowe) dokumentacja związana z powierzaniem mienia	3 lata (z wyjątkiem dokumentów księgowych)	

Lp.	Cel przetwarzania Danych osobowych	Typowe dokumenty oraz nośniki, z których należy usunąć dane	Maksymalny termin usunięcia danych	Moment, od którego liczony jest termin usunięcia danych
		pracownikom (w tym zarządzanie flotą samochodową, telefonami służbowymi) dokumentacja dotycząca chorób zawodowych karta ewidencji czasu pracy		
4.	**Wykonywanie umowy ze współpracownikami**	CV życiorys list motywacyjny treść e-maila, w którym przesłano dokumenty aplikacyjne umowa o świadczenie usług, zlecenia, umowa o dzieło itp. dokumentacja związana z oceną współpracy umowy dotyczące dofinansowania szkoleń oraz inne umowy cywilnoprawne ze współpracownikami dokumentacja związana z obsługą świadczeń dodatkowych (pakiety sportowe, medyczne, ubezpieczenia grupowe)	3 lata (z wyjątkiem dokumentów, wobec których konieczność dłuższego przechowywania wynika z właściwych przepisów prawa, oraz przypadków, gdy przechowywanie jest niezbędne z uwagi na bieg przedawnienia dla zobowiązań podatkowych). 50 lat / 10[3] lat w odniesieniu do przechowywania dokumentów zgodnie z wymogami przepisów z zakresu ubezpieczeń społecznych.	Zakończenie współpracy.

[3] Okres przechowywania dokumentacji został skrócony do 10 lat dla ubezpieczonych zgłoszonych po 1 stycznia 2019 r. Okres przechowywania dokumentacji dotyczącej ubezpieczonych zgłoszonych po 31 grudnia 1998 r., a przed 1 stycznia 2019 r. ulega skróceniu w przypadku złożenia raportu informacyjnego, o którym mowa w art. 7 ustawy z dnia 10 stycznia 2018 r. o zmianie niektórych ustaw w związku ze skróceniem okresu przechowywania akt pracowniczych oraz ich elektronizacją.

Lp.	Cel przetwarzania Danych osobowych	Typowe dokumenty oraz nośniki, z których należy usunąć dane	Maksymalny termin usunięcia danych	Moment, od którego liczony jest termin usunięcia danych
		dokumentacja związana z powierzaniem mienia pracownikom (w tym zarządzanie flotą samochodową, telefonami służbowymi)		
5.	**Obsługiwanie praktyk / stażów**	CV życiorys list motywacyjny treść e-maila, w którym przesłano dokumenty aplikacyjne dokumentacja związana z obsługą świadczeń dodatkowych (pakiety sportowe, medyczne, ubezpieczenia grupowe)	10 lat – w przypadku umów zawartych przed 9 lipca 2018 r. 6 lat – w przypadku umów zawartych po 9 lipca 2018 r.	Zakończenie praktyk / stażu.
6.	**Obsługiwanie wypadków przy pracy**	dokumentacja powypadkowa	10 lat	Data wypadku przy pracy.
7.	**Prowadzenie działań promocyjnych polegających na przesyłaniu informacji handlowych drogą elektroniczną (newsletter)**	system informatyczny, w którym przechowywane są informacje (wszystkie lokalizacje) formularze, za pośrednictwem których zbierana była zgoda	Niezwłocznie (pod warunkiem, że dane nie mogą być przetwarzane w innym celu).	Moment wycofania zgody na przesyłanie informacji handlowych drogą elektroniczna (tzw. zgoda na newsletter).

Lp.	Cel przetwarzania Danych osobowych	Typowe dokumenty oraz nośniki, z których należy usunąć dane	Maksymalny termin usunięcia danych	Moment, od którego liczony jest termin usunięcia danych
8.	**Prowadzenie działań telemarketingowych**	system informatyczny, w którym przechowywane są informacje (wszystkie lokalizacje) formularze, za pośrednictwem których zbierana była zgoda	Niezwłocznie (pod warunkiem, że dane nie mogą być przetwarzane w innym celu).	Moment wycofania zgody na wykorzystywanie urządzeń końcowych w celach marketingowych (tzw. zgoda na telemarketing).
9.	**Prowadzenie działań marketingowych drogą tradycyjną (wysyłka pocztowa)**	system informatyczny, w którym przechowywane są informacje (wszystkie lokalizacje) formularze, za pośrednictwem których zbierana była zgoda potwierdzenia wysłania przesyłek	Niezwłocznie (pod warunkiem, że dane nie mogą być przetwarzane w innym celu).	Moment, w którym kończy się relacja podmiotu danych ze ADO (np. rozwiązanie umowy, wycofanie wszystkich zgód marketingowych) lub gdy złożony został skuteczny sprzeciw wobec przetwarzania danych.
10.	**Organizacja konkursów i innych promocji**	system informatyczny, w którym przechowywane są informacje (wszystkie lokalizacje) formularze zgłoszeniowe zapisy dźwiękowe przeprowadzonych rozmów (w zakresie konkursów radiowych) potwierdzenia wydania nagród protokoły komisji konkursowych reklamacje	6 lat 10 lat – dla roszczeń konsumenckich powstałych i nieprzedawnionych przed 9 lipca 2018 r. (z wyjątkiem dokumentów księgowych).	Zakończenie konkursu / promocji (zgodnie z regulaminem).
11.	**Organizacja gier hazardowych, w tym**	system informatyczny, w którym przechowywane są informacje (wszystkie lokalizacje)	6 miesięcy (z wyjątkiem dokumentów księgowych).	Zakończenie loterii (zgodnie z jej regulaminem).

Lp.	Cel przetwarzania Danych osobowych	Typowe dokumenty oraz nośniki, z których należy usunąć dane	Maksymalny termin usunięcia danych	Moment, od którego liczony jest termin usunięcia danych
	loterii promocyjnych, audioteksowych	formularze zgłoszeniowe potwierdzenia wydania nagród protokoły komisji loteryjnych zapisy dźwiękowe przeprowadzonych rozmów (w zakresie loterii audioteksowych w radiu)		
12.	**Obsługiwanie umów z dostawcami (w tym negocjowane i zawieranie umów)**	zapytania ofertowe i oferty dokumenty związane z negocjacjami korespondencja w sprawie zawarcia umowy umowa z załącznikami aneksy do umowy z załącznikami wszelkie pisma i dokumenty związane z wykonaniem umowy (w tym monity, wezwania itp.) oraz jej rozwiązaniem system informatyczny, w którym przechowywane są informacje (wszystkie lokalizacje)	3 lata (z wyjątkiem dokumentów księgowych).	Rozwiązanie umowy.
13.	**Obsługiwanie umów sprzedażowych (w tym usług świadczonych drogą elektroniczną / przez**	formularz służący do zawarcia umowy zamówienie umowa z załącznikami aneksy do umowy z załącznikami	6 lat 10 lat – dla roszczeń konsumenckich powstałych i nieprzedawnionych	Rozwiązanie umowy.

Lp.	Cel przetwarzania Danych osobowych	Typowe dokumenty oraz nośniki, z których należy usunąć dane	Maksymalny termin usunięcia danych	Moment, od którego liczony jest termin usunięcia danych
	Internet) zawieranych z konsumentami	korespondencja w sprawie zawarcia umowy wszelkie pisma i dokumenty związane z wykonaniem umowy (w tym monity, wezwania itp.) oraz jej rozwiązaniem system informatyczny, w którym przechowywane są informacje (wszystkie lokalizacje)	przed 9 lipca 2018 r. (z wyjątkiem dokumentów księgowych).	
14.	**Obsługiwanie umów sprzedażowych (w tym usług świadczonych drogą elektroniczną / przez Internet) zawieranych z przedsiębiorcami**	formularz służący do zawarcia umowy zamówienie umowa z załącznikami aneksy do umowy z załącznikami korespondencja w sprawie zawarcia umowy wszelkie pisma i dokumenty związane z wykonaniem umowy (w tym monity, wezwania, itp.) oraz jej rozwiązaniem system informatyczny, w którym przechowywane są informacje (wszystkie lokalizacje)	3 lata (z wyjątkiem dokumentów księgowych).	Rozwiązanie umowy.

Lp.	Cel przetwarzania Danych osobowych	Typowe dokumenty oraz nośniki, z których należy usunąć dane	Maksymalny termin usunięcia danych	Moment, od którego liczony jest termin usunięcia danych
15.	**Prowadzenie spraw sądowych oraz postępowań przed organami administracyjnymi**	każdy rodzaj dokumentu związany z postępowaniem (pisma, orzeczenia, odpisy itp.) innego rodzaju korespondencja prowadzona z sądem / organem itp.	3 lata – dla roszczeń związanych z działalnością gospodarczą. 6 lat – dla roszczeń konsumenckich. 10 lat – dla roszczeń konsumenckich stwierdzonych prawomocnym orzeczeniem sądu lub organu, powstałych i nieprzedawnionych przed 9 lipca 2018 r. (z wyjątkiem dokumentów księgowych).	Dzień, w którym orzeczenie stało się prawomocne, chyba że w tym czasie wszczęto egzekucję (następuje przerwanie biegu przedawnienia).
16.	**Obsługiwanie monitoringu wizyjnego**	nagrania z monitoringu	3 miesiące (o ile przepisy szczególne nie stanowią inaczej)[4].	Data nagrania.
17.	**Zapewnianie ochrony mienia (obsługiwanie księgi wejść i wyjść)**	księga wejść i wyjść system informatyczny, w którym przechowywane są informacje	12 miesięcy	Data zamknięcia księgi / Data zapisania informacji w systemie.
18.	**Obsługa korespondencji przychodzącej / wychodzącej**	wiadomości e-mail w poczcie pracowniczej – służbowej	3 lata	Zakończenie stosunku pracy / współpracy danego pracownika / współpracownika.
19.	**Obsługa księgowa (rachunkowość, podatki, ubezpieczenia społeczne)**	dokumenty księgowe dokumentacja podatkowa dokumentacja ZUS	5 lat (chyba że inny okres wynika z przepisów szczególnych).	Moment liczony zgodnie z właściwymi przepisami.

[4]. W przypadku, w którym nagrania obrazu stanowią dowód w postępowaniu prowadzonym na podstawie prawa lub pracodawca powziął wiadomość, iż mogą one stanowić dowód w postępowaniu, termin 3 miesięcy ulega przedłużeniu do czasu prawomocnego zakończenia postępowania.

GMINA MIEDŹNO

PROCEDURA OBSŁUGI ŻĄDAŃ PODMIOTÓW DANYCH

dotyczących realizacji praw związanych z przetwarzaniem danych osobowych

METRYKA DOKUMENTU	
STATUS	Dokument wewnętrzny
WERSJA DOKUMENTU	1.0
DATA DOKUMENTU	31.10.2023 r.
LICZBA STRON	183
CEL DOKUMENTU	Niniejszy dokument opisuje zasady obsługi (przyjmowania i rozpoznawania) wniosków osób fizycznych, dotyczących realizacji praw podmiotów danych określonych przepisami RODO, w związku z przetwarzaniem ich danych osobowych.
SPIS TREŚCI	1. Definicje ..... 48 2. Zasady ogólne ..... 48 3. Identyfikacja Wnioskodawcy ..... 49 4. Sposób udzielenia odpowiedzi przez KOW ..... 50 5. Rola IOD ..... 51 6. Postanowienia końcowe ..... 52 Załącznik A – Realizacja żądania w zakresie dostępu do danych, w tym w zakresie poszczególnych rodzajów informacji nt. przetwarzania danych osobowych ..... 53 Załącznik B – Realizacja żądania wydania kopii danych ..... 56 Załącznik C – Realizacja żądania w zakresie sprostowania danych ..... 59 Załącznik D – Realizacja żądania w zakresie przeniesienia danych ..... 62 Załącznik E – Realizacja prawa do zgłoszenia sprzeciwu dotyczącego marketingu bezpośredniego ..... 65 Załącznik F – Realizacja prawa do zgłoszenia sprzeciwu względem przetwarzania danych w celach innych niż marketing bezpośredni ..... 68 Załącznik G – Realizacja prawa do wycofania zgody na przetwarzanie danych ..... 71 Załącznik H – Realizacja żądania w zakresie ograniczenia przetwarzania ..... 74 Załącznik I – Realizacja żądania w zakresie usunięcia danych osobowych ..... 78 Załącznik J – Procedura postępowania w przypadku zgłoszenia żądania przez pełnomocnika ..... 83 Załącznik K – Wzory pism stosowanych w Procedurze ..... 87 Załącznik L – Wzór zawiadomienia dedykowanych pracowników o wpłynięciu żądania ..... 96 Załącznik M – Wzór rejestru żądań 97

1. DEFINICJE

a. **Administrator - Gmina Miedźno** z siedzibą w Miedźnie ul. Ułańska 25, 42-120 Miedźno, NIP: 5742055080.

b. **Koordynator obsługi wniosków** lub **KOW –** osoba lub osoby, w których zakres obowiązków służbowych wchodzi przyjmowanie żądań podmiotów danych i odpowiadanie na te żądania.

c. **Dedykowany pracownik Gminy** – pracownik zobowiązany do wykonania czynności technicznych związanych z realizacją żądania Wnioskodawcy w obrębie jednej lub kilku jednostek organizacyjnych Gminy.

d. **IOD –** Inspektor Ochrony Danych, wyznaczony przez Gminę, nadzorujący przestrzeganie przepisów o ochronie danych osobowych w Gminie, wykonujący zadania określone w art. 39 RODO. W przypadku braku powołania w Gminie IOD, zadania związane z zapewnieniem zgodności przetwarzania danych osobowych w Gminie z obowiązującym prawem wykonuje **Koordynator ds. ochrony danych osobowych** (**KODO**).

e. **Pracownik –** osoba fizyczna zatrudniona na podstawie umowy o pracę lub innej umowy cywilnoprawnej.

f. **Prawa podmiotu danych –** prawa, o których mowa w art. 15–22 RODO.

g. **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.

h. **Wnioskodawca –** osoba fizyczna, której dane dotyczą, zgłaszająca żądanie realizacji jednego lub więcej Praw podmiotu danych.

2. ZASADY OGÓLNE

a. Procedura określa ogólne ramy postępowania z żądaniami osób fizycznych, kierowanymi do Administratora, a dotyczącymi Praw podmiotu danych. W każdym przypadku, w którym sposób postępowania nie wynika wprost z Procedury, niezbędna jest konsultacja z IOD.

b. Żądanie dotyczące Praw podmiotu danych może być złożone w formie pisemnej lub e-mailowej. Przyjmowanie żądań drogą telefoniczną za pośrednictwem Biura Obsługi Interesantów możliwe jest wyłącznie w przypadku, gdy dane zostały pierwotnie zebrane tą drogą. Nie jest dopuszczalne odrzucenie żądania z tego względu, że zostało ono zawarte w piśmie dotyczącym innej sprawy.

c. Żądania dotyczące Praw podmiotu danych realizuje KOW. W razie skierowania żądania do innej jednostki organizacyjnej pracownik, który otrzymał żądanie, zobowiązany jest niezwłocznie, lecz nie później niż do końca dnia roboczego, w którym żądanie wpłynęło, przekazać je do KOW.

d. Postępowanie, o którym mowa w Procedurze, jest nieodpłatne, z zastrzeżeniem pkt 4.h.

e. W przypadku braku możliwości jednoznacznej weryfikacji tożsamości Wnioskodawcy, KOW może zażądać dodatkowych informacji w celu potwierdzenia tożsamości Wnioskodawcy, zgodnie z postanowieniami rozdziału 3 poniżej.

f. Rozpoznanie żądania zgłoszonego przez pełnomocnika możliwe jest pod warunkiem, że przedstawia on pełnomocnictwo (upoważnienie), z którego jednoznacznie wynika umocowanie do zgłoszenia żądania i zakres żądania.

g. Pełnomocnictwo (upoważnienie) powinno mieć formę:

i. aktu notarialnego; albo

ii. pisemną, z poświadczeniem notarialnym; albo

iii. pisemną, z poświadczeniem radcy prawnego lub adwokata – w przypadku, gdy pełnomocnictwo zostało udzielone temu radcy prawnemu lub adwokatowi;

iv. pisemną, zwykłą tzn. niepoświadczoną. W takim wypadku KOW powinien zasięgnąć opinii IOD w przedmiocie dopuszczalności działania w oparciu o złożone pełnomocnictwo, zgodnie z instrukcją określoną w załączniku J.

h. W przypadku braku możliwości jednoznacznego określenia faktycznej treści żądania Wnioskodawcy, KOW może żądać od Wnioskodawcy dodatkowych wyjaśnień.

i. Wszystkie czynności podejmowane w związku z realizacją żądania podmiotu danych są dokumentowane w sposób określony przez Administratora lub w wytycznych, o których mowa w pkt 5.b. KOW rejestruje każde otrzymane żądanie w rejestrze, którego wzór określony został w załączniku M do Procedury.

3. IDENTYFIKACJA WNIOSKODAWCY

a. Przed udzieleniem odpowiedzi na żądanie KOW zobowiązany jest do weryfikacji tożsamości Wnioskodawcy.

b. W przypadku braku możliwości jednoznacznej weryfikacji tożsamości Wnioskodawcy, KOW może żądać dodatkowych informacji w celu potwierdzenia tożsamości Wnioskodawcy, w szczególności w przypadku złożenia żądania o pozyskanie kopii lub przeniesienie danych.

c. Tożsamość Wnioskodawcy jest potwierdzana w sposób określony w odrębnych procedurach i/lub zgodnie z wytycznymi IOD.

d. Niezależnie od przyjętych procedur, weryfikacja tożsamości Wnioskodawcy powinna każdorazowo odbywać się zgodnie z poniższymi zasadami:

i. w przypadku żądania od Wnioskodawcy podania dodatkowych danych w celu jednoznacznego potwierdzenia tożsamości Wnioskodawcy, należy pozyskiwać jedynie dane w zakresie niezbędnym dla osiągnięcia zamierzonego celu;

ii. w przypadku żądania od Wnioskodawcy podania dodatkowych danych celem jednoznacznego potwierdzenia tożsamości Wnioskodawcy, należy niezwłocznie, lecz nie później niż w ciągu miesiąca poinformować Wnioskodawcę, że termin

udzielenia odpowiedzi na żądanie będzie liczony od dnia udzielenia informacji umożliwiających jednoznaczną identyfikację;

iii. w przypadku okazania przez Wnioskodawcę dokumentu celem umożliwienia jednoznacznego potwierdzenia tożsamości, dokument powinien być pozyskiwany wyłącznie do wglądu, tzn. nie powinna być wykonywana jego kopia ani skan.

e. W przypadku, gdy w procesie identyfikacji tożsamość Wnioskodawcy nie została jednoznacznie potwierdzona, KOW udziela odpowiedzi zgodnie z wzorem nr 4 określonym w załączniku K.

4. SPOSÓB UDZIELENIA ODPOWIEDZI PRZEZ KOW

a. KOW zobowiązany jest udzielić odpowiedzi na żądanie w terminie miesiąca od dnia jego otrzymania (tzn. od dnia wpłynięcia żądania do Gminy). W przypadku zamiaru przesłania odpowiedzi drogą pocztową, KOW zapewnia, by odpowiedź została wysłania nie później niż w terminie 3 dni roboczych przed upływem miesiąca od daty otrzymania żądania.

b. Jeżeli koniec terminu przypada na dzień ustawowo wolny od pracy, za ostatni dzień terminu uważa się najbliższy następny dzień powszedni.

c. W przypadkach otrzymania żądania, w związku z którym konieczne jest:

i. ustalenie lub weryfikacja tożsamości Wnioskodawcy; lub

ii. ustalenie lub doprecyzowanie przedmiotu żądania

– miesięczny termin dotyczy podjęcia przez KOW czynności w celu uzyskania informacji niezbędnych do ustalenia powyższych okoliczności. W takim przypadku termin na udzielenie odpowiedzi na żądanie wynosi miesiąc od dnia uzyskania przez KOW wszystkich informacji niezbędnych do realizacji żądania.

d. KOW uprawniony jest do przedłużenia terminu udzielenia odpowiedzi na żądanie jedynie w przypadku, gdy dochowanie miesięcznego terminu nie jest możliwe z uwagi na skomplikowany charakter żądania lub dużą liczbę zgłoszonych żądań. W przypadku przedłużenia terminu rozpatrzenia żądania, KOW zobowiązany jest poinformować Wnioskodawcę o przedłużeniu terminu udzielenia odpowiedzi, wskazując przyczyny przedłużenia terminu zgodnie z wzorem nr 1 określonym w załączniku K do Procedury.

e. W przypadku, w którym żądanie zostało skierowane do Gminy elektronicznie, odpowiedzi udziela się w tej samej formie, chyba że Wnioskodawca zażądał udzielenia odpowiedzi w innej formie. W innych przypadkach odpowiedzi udziela się pisemnie. W przypadku, gdy termin realizacji żądania uniemożliwia udzielenie odpowiedzi drogą pisemną, a zakres danych Wnioskodawcy przetwarzanych przez Administratora umożliwia kontakt drogą elektroniczną, odpowiedzi należy udzielić drogą elektroniczną.

f. Odmowa podjęcia działań w związku ze zgłoszonym żądaniem dopuszczalna jest wyłącznie w przypadku, gdy:

i. żądanie jest ewidentnie nieuzasadnione;

ii. żądania Wnioskodawcy są nadmierne, w szczególności gdy ich zgłaszanie ma charakter ustawiczny.

g. O odmowie podjęcia działań z uwagi na powyższe okoliczności Gmina informuje Wnioskodawcę w terminie miesiąca od otrzymania żądania. Informacja udzielana jest zgodnie z wzorem nr 3 określonym w załączniku K do Procedury.

h. W przypadku określonym w pkt f powyżej Gmina może zamiast odmowy podjęcia działań rozpoznać żądanie merytorycznie po pobraniu opłaty w wysokości uprzednio ustalonej.

i. Decyzja o odmowie podjęcia działań lub pobraniu opłaty wymaga bezwzględnie uprzedniej zgody IOD w formie pisemnej lub e-mailowej. IOD może w wytycznych, o których mowa w pkt 5.b, określić przypadki, w których zgoda na odmowę podjęcia działań lub pobranie opłaty nie jest wymagana.

5. ROLA IOD

a. IOD wspiera KOW w zapewnieniu prawidłowości merytorycznej odpowiedzi udzielanych Wnioskodawcom.

b. IOD może opracować wytyczne dotyczące sposobu wykonywania Procedury, w szczególności:

i. zasad identyfikacji Wnioskodawców;

ii. przypadków uzasadniających pobrania opłaty od Wnioskodawców;

iii. odmowy uwzględnienia żądań Wnioskodawców;

iv. sposobu realizacji Wniosków zgłoszonych przez osoby trzecie w oparciu o pełnomocnictwo (upoważnienie);

v. merytorycznego sposobu rozpoznawania żądań.

c. Wytyczne udostępniane są pracownikom KOW. IOD zobowiązany jest zapewnić zgodność wytycznych z publikowanymi stanowiskami właściwych organów i w razie konieczności dokonuje ich aktualizacji.

d. IOD udziela niezbędnego wsparcia w związku z rozpatrywaniem żądań Wnioskodawców, w tym w szczególności udziela konsultacji pracownikom zaangażowanym w obsługę żądań, opracowuje niezbędne skrypty i prowadzi okresowe szkolenia pracowników KOW.

e. IOD jest odpowiedzialny za dokonywanie systematycznych przeglądów zasad realizacji żądań Wnioskodawców, zawartych w załącznikach od A do J (w tym za przedstawianie rekomendacji w zakresie ich aktualizacji), nie rzadziej niż raz na 6 miesięcy.

f. IOD jest uprawniony do aktualizacji załączników K, L i M do Procedury. W razie takiej aktualizacji IOD zobowiązany jest poinformować o wprowadzonych zmianach pracowników KOW oraz Gminy.

g. IOD w granicach swoich kompetencji może powierzyć wykonywanie obowiązków określonych w Procedurze innej osobie, przy czym nie zwalnia to IOD z odpowiedzialności za wykonanie tych obowiązków.

h. Postanowienia Procedury dotyczące IOD stosuje się odpowiednio do KODO.

6. POSTANOWIENIA KOŃCOWE

a. Każdy pracownik Gminy zobowiązany jest do zapoznania się z Procedurą i przestrzegania jej postanowień.

b. Z zastrzeżeniem pkt 5.f, zmiana Procedury wymaga zarządzenia Wójta Gminy.

c. Procedura wchodzi w życie z dniem wejścia w życie zarządzenia przez Wójta Gminy.

d. Integralną część Procedury stanowią jej załączniki:

i. Załącznik A – Realizacja żądania w zakresie dostępu do danych;

ii. Załącznik B – Realizacja żądania wydania kopii danych;

iii. Załącznik C – Realizacja żądania w zakresie sprostowania danych;

iv. Załącznik D – Realizacja żądania w zakresie przeniesienia danych;

v. Załącznik E – Realizacja prawa do zgłoszenia sprzeciwu dotyczącego marketingu bezpośredniego;

vi. Załącznik F – Realizacja prawa do zgłoszenia sprzeciwu względem przetwarzania danych w celach innych niż marketing bezpośredni;

vii. Załącznik G – Realizacja prawa do wycofania zgody na przetwarzanie danych;

viii. Załącznik H – Realizacja żądania w zakresie ograniczenia przetwarzania;

ix. Załącznik I – Realizacja żądania w zakresie usunięcia danych osobowych;

x. Załącznik J – Procedura postępowania w przypadku zgłoszenia żądania przez pełnomocnika;

xi. Załącznik K – Wzory pism stosowanych w Procedurze;

xii. Załącznik L – Wzór zawiadomienia dedykowanych pracowników o wpłynięciu żądania;

xiii. Załącznik M – Wzór rejestru żądań.

Załącznik A – Realizacja żądania w zakresie dostępu do danych, w tym w zakresie poszczególnych rodzajów informacji nt. przetwarzania danych osobowych

OSOBA ODPOWIEDZIALNA	WYMAGANE DZIAŁANIA	MAKSYMALNY TERMIN[5] (W DNIACH OD WPŁYNIĘCIA ŻĄDANIA)
I. Czynności formalne		
Pracownik KOW	Potwierdzenie przyjęcia żądania.	**1**
	Weryfikacja możliwości jednoznacznej identyfikacji Wnioskodawcy zgodnie z oddzielnymi procedurami. W braku takiej możliwości, udzielenie Wnioskodawcy odpowiedzi zgodnie z wzorem nr 4 określonym w załączniku K do Procedury obsługi żądań podmiotów danych.	**3**
II. Weryfikacja merytoryczna żądania		
Pracownik KOW	**1.** W razie konieczności, jednoznaczne potwierdzenie z Wnioskodawcą zakresu żądania. W braku jednoznacznego potwierdzenia zakresu żądania przez Wnioskodawcę, przekazanie Wnioskodawcy informacji potwierdzającej lub zaprzeczającej przetwarzaniu danych Wnioskodawcy przez Gminę. W przypadku istotnych wątpliwości co do sposobu rozstrzygnięcia żądania – konsultacja z IOD.	**7**
IOD	Rekomendacja co do sposobu rozstrzygnięcia żądania.	**9**
Pracownik KOW	Decyzja co do sposobu rozstrzygnięcia żądania.	**10**
III. Zawiadomienie o żądaniu dedykowanych pracowników Gminy		

[5] Wszystkie podane terminy mają charakter rekomendacji. W przypadku braku możliwości zrealizowania zgłoszonego żądania podmiotu danych w terminie 1 miesiąca od wpłynięcia wniosku, należy poinformować Wnioskodawcę o przedłużeniu terminu zgodnie z pkt 4.d Procedury obsługi żądań podmiotów danych.

OSOBA ODPOWIEDZIALNA	WYMAGANE DZIAŁANIA	MAKSYMALNY TERMIN[5] (W DNIACH OD WPŁYNIĘCIA ŻĄDANIA)
Pracownik KOW	**1.** Przekazanie do dedykowanych pracowników Gminy informacji o zakresie, w jakim żądanie zostało uwzględnione, zgodnie z wzorem określonym w załączniku L do Procedury obsługi żądań podmiotów danych.	**12**
IV. Realizacja czynności niezbędnych dla spełnienia żądania Wnioskodawcy		
Dedykowany pracownik Gminy	**1.** Przeszukanie systemów informatycznych w zakresie danych osobowych dotyczących Wnioskodawcy, których dotyczy żądanie. Wygenerowanie zestawienia zawierającego następujące informacje: **a.** cele przetwarzania danych osobowych Wnioskodawcy; **b.** kategorie przetwarzanych danych osobowych Wnioskodawcy; **c.** informacje o odbiorcach lub kategoriach odbiorców, którym dane osobowe Wnioskodawcy zostały ujawnione; **d.** planowany okres przechowywania danych osobowych Wnioskodawcy; **e.** informacje o prawach przysługujących Wnioskodawcy w związku z przetwarzaniem danych (w zakresie prawa do żądania sprostowania, usunięcia lub ograniczenia przetwarzania danych osobowych Wnioskodawcy oraz prawie wniesienia sprzeciwu wobec przetwarzania – w zależności od okoliczności); **f.** informację o prawie wniesienia skargi do organu nadzorczego; **g.** informację o źródle danych osobowych Wnioskodawcy, jeśli dane nie pochodzą od Wnioskodawcy; **h.** o ile ma to zastosowanie, informację o zautomatyzowanym podejmowaniu decyzji, w tym profilowaniu oraz istotne informacje o zasadach ich podejmowania, a także o znaczeniu	**24**

OSOBA ODPOWIEDZIALNA	WYMAGANE DZIAŁANIA	MAKSYMALNY TERMIN[5] (W DNIACH OD WPŁYNIĘCIA ŻĄDANIA)
	i przewidywanych konsekwencjach takiego przetwarzania dla osoby; **i.** o ile ma to zastosowanie, informacje o odpowiednich zabezpieczeniach związanych z przekazywaniem danych do państw trzecich. Wygenerowane zestawienie powinno uwzględniać wytyczne IOD w tym zakresie, wydane na podstawie pkt **Error! Reference source not found.**. Procedury.	
Dedykowany pracownik Gminy	Wyszukanie danych osobowych dotyczących Wnioskodawcy przetwarzanych w formie papierowej. Sporządzenie zestawienia w zakresie określonym w ust. 2 i 3 części IV powyżej.	**24**
Pracownik KOW	Scalenie sporządzonych zestawień w jeden dokument.	**26**
V. Udzielenie odpowiedzi na żądanie		
Pracownik KOW	**1.** Udzielenie odpowiedzi na żądanie.	**maks. 1 miesiąc**

Załącznik B – Realizacja żądania wydania kopii danych

OSOBA ODPOWIEDZIALNA	WYMAGANE DZIAŁANIA	MAKSYMALNY TERMIN[6] (W DNIACH OD WPŁYNIĘCIA ŻĄDANIA)
I. Czynności formalne		
Pracownik KOW	**1.** Potwierdzenie przyjęcia żądania.	**1**
	Weryfikacja możliwości jednoznacznej identyfikacji Wnioskodawcy zgodnie z oddzielnymi procedurami. W braku takiej możliwości, udzielenie Wnioskodawcy odpowiedzi zgodnie z wzorem nr 4 określonym w załączniku K do Procedury obsługi żądań podmiotów danych.	**3**
II. Weryfikacja merytoryczna żądania		
Pracownik KOW	**1.** W razie konieczności, jednoznaczne potwierdzenie z Wnioskodawcą zakresu żądania, w tym jednoznaczne określenie: **a.** okresu przetwarzania, którego dotyczy żądanie; **b.** usług, w związku z którymi przetwarzane są dane, których dotyczy żądanie; **c.** formy, w jakiej kopia danych ma zostać przekazana. W przypadku istotnych wątpliwości co do sposobu rozstrzygnięcia żądania – konsultacja z IOD.	**7**
IOD	Rekomendacja co do sposobu rozstrzygnięcia żądania.	**9**
Pracownik KOW	Decyzja co do sposobu rozstrzygnięcia żądania.	**10**

[6] Wszystkie podane terminy mają charakter rekomendacji. W przypadku braku możliwości zrealizowania zgłoszonego żądania podmiotu danych w terminie 1 miesiąca od wpłynięcia wniosku, należy poinformować Wnioskodawcę o przedłużeniu terminu zgodnie z pkt 4.d. Procedury obsługi wniosków podmiotów danych.

OSOBA ODPOWIEDZIALNA	WYMAGANE DZIAŁANIA	MAKSYMALNY TERMIN[6] (W DNIACH OD WPŁYNIĘCIA ŻĄDANIA)
III. Zawiadomienie o żądaniu dedykowanych pracowników Gminy		
Pracownik KOW	**1.** Przekazanie do dedykowanych pracowników Gminy informacji o zakresie, w jakim żądanie zostało uwzględnione, zgodnie z wzorem określonym w załączniku L do Procedury obsługi żądań podmiotów danych.	**12**
IV. Realizacja czynności niezbędnych dla spełnienia żądania Wnioskodawcy		
Dedykowany pracownik Gminy	**1.** Przeszukanie systemów informatycznych w zakresie danych osobowych dotyczących Wnioskodawcy, których dotyczy żądanie. Sporządzenie kopii wyszukanych danych osobowych.	**24**
Dedykowany pracownik Gminy	Wyszukanie danych osobowych dotyczących Wnioskodawcy przetwarzanych w formie papierowej. Sporządzenie kopii wyszukanych danych osobowych.	**24**
Pracownik KOW	Weryfikacja sporządzonych kopii pod kątem: **a.** ryzyka ujawnienia tajemnicy przedsiębiorstwa Gminy lub podmiotów trzecich; **b.** ryzyka naruszenia praw własności intelektualnej Gminy lub podmiotów trzecich; **c.** ryzyka naruszenia praw i wolności podmiotów danych, innych niż Wnioskodawca. Konsultacja dopuszczalności i zakresu zanonimizowania przekazywanych informacji lub zmiany ich struktury z IOD w związku ze zidentyfikowanymi ryzykami.	**26**
IOD	Rekomendacja co do dopuszczalności i zakresu zanonimizowania przekazywanych informacji lub zmiany ich	**28**

OSOBA ODPOWIEDZIALNA	WYMAGANE DZIAŁANIA	MAKSYMALNY TERMIN[6] (W DNIACH OD WPŁYNIĘCIA ŻĄDANIA)
	struktury w związku z ryzykami zidentyfikowanymi przez KOW.	
V. Udzielenie odpowiedzi na żądanie		
Pracownik KOW	**2.** Udzielenie odpowiedzi na żądanie Wnioskodawcy (wydanie kopii danych).	**maks. 1 miesiąc**

Załącznik C – Realizacja żądania w zakresie sprostowania danych

OSOBA ODPOWIEDZIALNA	WYMAGANE DZIAŁANIA	MAKSYMALNY TERMIN[7] (W DNIACH OD WPŁYNIĘCIA ŻĄDANIA)
I. Czynności formalne		
Pracownik KOW	**1.** Potwierdzenie przyjęcia żądania.	**1**
	Weryfikacja możliwości jednoznacznej identyfikacji Wnioskodawcy zgodnie z oddzielnymi procedurami. W braku takiej możliwości, udzielenie Wnioskodawcy odpowiedzi zgodnie z wzorem nr 4 określonym w załączniku K do Procedury obsługi żądań podmiotów danych.	**3**
II. Weryfikacja merytoryczna żądania		
Pracownik KOW	**1.** W razie konieczności, jednoznaczne potwierdzenie z Wnioskodawcą zakresu żądania, w tym określenie czy żądanie dotyczy sprostowania czy uzupełnienia danych osobowych. **2.** W razie konieczności, zażądanie od Wnioskodawcy stosownego dowodu potwierdzającego nieprawidłowość lub niekompletność danych – w szczególności w formie wglądu do dokumentu lub poprzez złożenie przez Wnioskodawcę oświadczenia. **3.** W przypadku żądania uzupełnienia danych, weryfikacja czy dane, których uzupełnienia żąda Wnioskodawca są niezbędne dla realizacji procesu. **4.** W razie stwierdzenia, że uzupełniane dane są zbędne lub Wnioskodawca nie wykazał, że przetwarzane dane są nieprawidłowe, udzielenie Wnioskodawcy odmownej odpowiedzi na żądanie, ze wskazaniem powyższych okoliczności.	**7**

[7] Wszystkie podane terminy mają charakter rekomendacji. W przypadku braku możliwości zrealizowania zgłoszonego żądania podmiotu danych w terminie 1 miesiąca od wpłynięcia wniosku, należy poinformować Wnioskodawcę o przedłużeniu terminu zgodnie z pkt 4.d Procedury obsługi wniosków podmiotów danych.

OSOBA ODPOWIEDZIALNA	WYMAGANE DZIAŁANIA	MAKSYMALNY TERMIN[7] (W DNIACH OD WPŁYNIĘCIA ŻĄDANIA)
	5. W przypadku istotnych wątpliwości co do sposobu rozstrzygnięcia żądania – konsultacja z IOD.	
IOD	Rekomendacja co do sposobu rozstrzygnięcia żądania.	**9**
Pracownik KOW	Decyzja co do sposobu rozstrzygnięcia żądania.	**10**
III. Zawiadomienie o żądaniu dedykowanych pracowników Gminy		
Pracownik KOW	**1.** Przekazanie do dedykowanych pracowników Gminy informacji o zakresie, w jakim żądanie zostało uwzględnione, zgodnie z wzorem określonym w załączniku K do Procedury obsługi żądań podmiotów danych.	**12**
IV. Realizacja czynności niezbędnych dla spełnienia żądania Wnioskodawcy		
Dedykowany pracownik Gminy	**1.** Przeszukanie systemów informatycznych w zakresie danych osobowych dotyczących Wnioskodawcy, których dotyczy żądanie o sprostowanie. **2.** Wprowadzenie zmian danych osobowych we wszystkich lokalizacjach, w których przetwarzane są dane osobowe Wnioskodawcy. **3.** Identyfikacja odbiorców danych osobowych Wnioskodawcy – podmiotów, którym ujawnione zostały dane osobowe Wnioskodawcy.	**24**
Dedykowany pracownik Gminy	Identyfikacja dokumentacji papierowej zawierającej dane osobowe Wnioskodawcy. Odnotowanie faktu zmiany danych w dokumentacji papierowej w formie właściwej dla tej dokumentacji, w tym w formie notatki służbowej. Adnotacja oznaczana jest dodatkowo:	**24**

OSOBA ODPOWIEDZIALNA	WYMAGANE DZIAŁANIA	MAKSYMALNY TERMIN[7] (W DNIACH OD WPŁYNIĘCIA ŻĄDANIA)
	a. podpisem osoby wprowadzającej zmianę; **b.** datą dokonania sprostowania.	
V. Udzielenie odpowiedzi na żądanie		
Pracownik KOW	**1.** Udzielenie odpowiedzi na żądanie Wnioskodawcy. **2.** Powiadomienie o realizacji żądania Wnioskodawcy zidentyfikowanych odbiorców danych. **3.** W razie zgłoszenia takiego żądania przez Wnioskodawcę, powiadomienie Wnioskodawcy o wszystkich odbiorcach jego danych osobowych poprzez wskazanie co najmniej firm tych podmiotów.	**maks. 1 miesiąc**

Załącznik D – Realizacja żądania w zakresie przeniesienia danych

OSOBA ODPOWIEDZIALNA	WYMAGANE DZIAŁANIA	MAKSYMALNY TERMIN[8] (W DNIACH OD WPŁYNIĘCIA ŻĄDANIA)
I. Czynności formalne		
Pracownik KOW	**1.** Potwierdzenie przyjęcia żądania.	**1**
	Weryfikacja możliwości jednoznacznej identyfikacji Wnioskodawcy zgodnie z oddzielnymi procedurami. W braku takiej możliwości, udzielenie Wnioskodawcy odpowiedzi zgodnie z wzorem nr 4 określonym w załączniku K do Procedury obsługi żądań podmiotów danych.	**3**
II. Weryfikacja merytoryczna żądania		
Pracownik KOW	**1.** W razie konieczności, jednoznaczne potwierdzenie z Wnioskodawcą zakresu żądania, w tym określenie: **a.** czy żądanie dotyczy przekazania danych Wnioskodawcy czy przesłania innemu podmiotowi; **b.** czy żądanie dotyczy wszystkich danych Wnioskodawcy podlegających prawu do przeniesienia, czy też jedynie danych przetwarzanych w związku ze świadczeniem przez Gminę konkretnej usługi lub usług. **2.** Weryfikacja możliwości technicznych przesłania danych bezpośredniemu administratorowi wskazanemu przez Wnioskodawcę. W braku takich możliwości – poinformowanie Wnioskodawcy o braku możliwości uwzględnienia żądania z powyższych względów.	**7**

[8] Wszystkie podane terminy mają charakter rekomendacji. W przypadku braku możliwości zrealizowania zgłoszonego żądania podmiotu danych w terminie 1 miesiąca od wpłynięcia wniosku, należy poinformować Wnioskodawcę o przedłużeniu terminu zgodnie z pkt **Error! Reference source not found.** Procedury obsługi żądań podmiotów danych.

OSOBA ODPOWIEDZIALNA	WYMAGANE DZIAŁANIA	MAKSYMALNY TERMIN[8] (W DNIACH OD WPŁYNIĘCIA ŻĄDANIA)
	W przypadku istotnych wątpliwości co do sposobu rozstrzygnięcia żądania – konsultacja z IOD.	
IOD	Rekomendacja co do sposobu rozstrzygnięcia żądania.	**9**
Pracownik KOW	Decyzja co do sposobu rozstrzygnięcia żądania.	**10**
III. Zawiadomienie o żądaniu dedykowanych pracowników Gminy		
Pracownik KOW	**1.** Przekazanie do dedykowanych pracowników Gminy informacji o zakresie, w jakim żądanie zostało uwzględnione, zgodnie z wzorem określonym w załączniku L do Procedury obsługi żądań podmiotów danych.	**12**
IV. Realizacja czynności niezbędnych dla spełnienia żądania Wnioskodawcy		
Dedykowany pracownik Gminy	**1.** Przeszukanie systemów informatycznych w zakresie danych osobowych dotyczących Wnioskodawcy. Wyselekcjonowanie wśród wyników wyszukiwania danych osobowych przetwarzanych na podstawie zgody Wnioskodawcy lub w związku z wykonywaniem umowy z Wnioskodawcą. Wyselekcjonowanie spośród danych wyodrębnionych zgodnie z pkt. 2, danych dostarczonych przez Wnioskodawcę. Jeżeli żądanie nie dotyczyło wszystkich przetwarzanych danych, usunięcie z wyników wyszukania danych nieobjętych żądaniem. Eksport wyników wyszukania do ustrukturyzowanego formatu odczytywalnego przez komputer (csv, xml).	**24**
Pracownik KOW	Scalenie otrzymanych zestawień w jeden dokument.	**24**

OSOBA ODPOWIEDZIALNA	WYMAGANE DZIAŁANIA	MAKSYMALNY TERMIN[8] (W DNIACH OD WPŁYNIĘCIA ŻĄDANIA)
	Weryfikacja otrzymanego zestawienia pod kątem: **a.** ryzyka ujawnienia tajemnicy przedsiębiorstwa Gminy lub podmiotów trzecich; **b.** ryzyka naruszenia praw własności intelektualnej Gminy lub podmiotów trzecich; **c.** ryzyka naruszenia praw i wolności podmiotów danych, innych niż Wnioskodawca. Konsultacja dopuszczalności i zakresu zanonimizowania przekazywanych informacji lub zmiany ich struktury z IOD w związku ze zidentyfikowanymi ryzykami.	
IOD	Rekomendacja co do dopuszczalności i zakresu zanonimizowania przekazywanych informacji lub zmiany ich struktury w związku z ryzykami zidentyfikowanymi przez KOW.	**26**
V. Udzielenie odpowiedzi na żądanie		
Pracownik KOW	**1.** Udzielenie odpowiedzi na żądanie. **2.** Przesłanie danych nowemu administratorowi w przypadku takiej technicznej możliwości.	**maks. 1 miesiąc**

Załącznik E – Realizacja prawa do zgłoszenia sprzeciwu dotyczącego marketingu bezpośredniego

OSOBA ODPOWIEDZIALNA	WYMAGANE DZIAŁANIA	MAKSYMALNY TERMIN[9] (W DNIACH OD WPŁYNIĘCIA ŻĄDANIA)
Wszelkie czynności wykonywane w związku z realizacją przedmiotowego prawa powinny być realizowane niezwłocznie. O ile jest to możliwe techniczne, pracownik, do którego wpłynęło żądanie, albo KOW natychmiast po otrzymaniu żądania wstrzymuje komunikację o charakterze marketingowym względem Wnioskodawcy.		
I. Czynności formalne		
Pracownik KOW	**1.** Potwierdzenie przyjęcia żądania.	**1**
	Weryfikacja możliwości jednoznacznej identyfikacji Wnioskodawcy zgodnie z oddzielnymi procedurami. W przypadku braku takiej możliwości, udzielenie Wnioskodawcy odpowiedzi zgodnie z wzorem nr 4 określonym w załączniku K do Procedury obsługi żądań podmiotów danych.	**3**
II. Weryfikacja merytoryczna żądania		
Pracownik KOW	**1.** W razie konieczności, jednoznaczne potwierdzenie z Wnioskodawcą zakresu żądania. W braku jednoznacznego potwierdzenia zakresu żądania przez Wnioskodawcę, przekazanie Wnioskodawcy informacji potwierdzającej lub zaprzeczającej przetwarzaniu danych Wnioskodawcy przez Gminę. W przypadku istotnych wątpliwości co do sposobu rozstrzygnięcia żądania – konsultacja z IOD.	**7**
IOD	Rekomendacja co do sposobu rozstrzygnięcia żądania.	**9**

[9] Wszystkie podane terminy mają charakter rekomendacji. W przypadku braku możliwości zrealizowania zgłoszonego żądania podmiotu danych w terminie 1 miesiąca od wpłynięcia wniosku, należy poinformować Wnioskodawcę o przedłużeniu terminu zgodnie z pkt 4.d. Procedury obsługi wniosków podmiotów danych.

OSOBA ODPOWIEDZIALNA	WYMAGANE DZIAŁANIA	MAKSYMALNY TERMIN[9] (W DNIACH OD WPŁYNIĘCIA ŻĄDANIA)
Pracownik KOW	Decyzja co do sposobu rozstrzygnięcia żądania.	**10**
III. Zawiadomienie o żądaniu dedykowanych pracowników Gminy		
Pracownik KOW	**1.** Przekazanie do dedykowanych pracowników Gminy informacji o zakresie, w jakim żądanie zostało uwzględnione, zgodnie z wzorem określonym w załączniku L do Procedury obsługi żądań podmiotów danych.	**12**
IV. Realizacja czynności niezbędnych dla spełnienia żądania Wnioskodawcy		
Dedykowany pracownik Gminy	**1.** Przeszukanie systemów informatycznych w zakresie danych osobowych dotyczących Wnioskodawcy. **2.** Wyselekcjonowanie danych przetwarzanych w celu marketingu bezpośredniego. **3.** Oznaczenie tak wyselekcjonowanych danych jako objętych sprzeciwem. **4.** Zaprzestanie przetwarzania oznaczonych danych w celu marketingu bezpośredniego. W przypadku, gdy dla celów objętych sprzeciwem dane przetwarzane są także w postaci papierowej: **5.** Wyszukanie danych osobowych Wnioskodawcy przetwarzanych w postaci papierowej w celu marketingu bezpośredniego. **6.** Odnotowanie faktu zgłoszenia sprzeciwu w dokumentacji papierowej w formie właściwej dla tej dokumentacji, w tym w formie notatki służbowej. Adnotacja powinna zawierać: **a.** datę zgłoszenia sprzeciwu i daty dokonania adnotacji; **b.** podpis osoby, dokonującej adnotacji. **7.** Zaprzestanie przetwarzania oznaczonych danych w celu marketingu bezpośredniego.	**24**

OSOBA ODPOWIEDZIALNA	WYMAGANE DZIAŁANIA	MAKSYMALNY TERMIN[9] (W DNIACH OD WPŁYNIĘCIA ŻĄDANIA)
	8. W razie, gdy dane osobowe przetwarzane były w postaci papierowej jedynie w celu marketingu bezpośredniego, a sprzeciw został uwzględniony, nieodwracalne usunięcie (zniszczenie) danych osobowych lub zanonimizowanie dokumentów papierowych.	
V. Udzielenie odpowiedzi na żądanie		
Pracownik KOW	**1.** Udzielenie odpowiedzi na żądanie.	**maks. 1 miesiąc**

Załącznik F – Realizacja prawa do zgłoszenia sprzeciwu względem przetwarzania danych w celach innych niż marketing bezpośredni

OSOBA ODPOWIEDZIALNA	WYMAGANE DZIAŁANIA	MAKSYMALNY TERMIN[10] (W DNIACH OD WPŁYNIĘCIA ŻĄDANIA)
I. Czynności formalne		
Pracownik KOW	**1.** Potwierdzenie przyjęcia żądania.	**1**
	Weryfikacja możliwości jednoznacznej identyfikacji Wnioskodawcy zgodnie z oddzielnymi procedurami. W braku takiej możliwości, udzielenie Wnioskodawcy odpowiedzi zgodnie z wzorem nr 4 określonym w załączniku K do Procedury obsługi żądań podmiotów danych.	**3**
II. Weryfikacja merytoryczna żądania		
Pracownik KOW	**1.** W razie konieczności, jednoznaczne potwierdzenie z Wnioskodawcą zakresu żądania. **2.** Weryfikacja merytoryczna żądania w zakresie przedstawionych przez Wnioskodawcę przyczyn związanych z jego szczególną sytuacją oraz podstaw przetwarzania danych przez Gminę. **3.** W przypadku istotnych wątpliwości co do sposobu rozstrzygnięcia żądania – konsultacja z IOD.	**7**
IOD	Rekomendacja co do sposobu rozstrzygnięcia żądania.	**9**
Pracownik KOW	Decyzja co do sposobu rozstrzygnięcia żądania.	**10**
III. Zawiadomienie o żądaniu dedykowanych pracowników Gminy		

[10] Wszystkie podane terminy mają charakter rekomendacji. W przypadku braku możliwości zrealizowania zgłoszonego żądania podmiotu danych w terminie 1 miesiąca od wpłynięcia wniosku, należy poinformować Wnioskodawcę o przedłużeniu terminu zgodnie z pkt 4.d. Procedury obsługi wniosków podmiotów danych.

OSOBA ODPOWIEDZIALNA	WYMAGANE DZIAŁANIA	MAKSYMALNY TERMIN[10] (W DNIACH OD WPŁYNIĘCIA ŻĄDANIA)
Pracownik KOW	**1.** Przekazanie do dedykowanych pracowników Gminy informacji o zakresie, w jakim żądanie zostało uwzględnione, zgodnie z wzorem określonym w załączniku L do Procedury obsługi żądań podmiotów danych.	**12**
IV. Realizacja czynności niezbędnych dla spełnienia żądania Wnioskodawcy		
Dedykowany pracownik Gminy	**1.** Przeszukanie systemów informatycznych w zakresie danych osobowych dotyczących Wnioskodawcy. **2.** Wyselekcjonowanie danych oznaczonych jako przetwarzane na podstawie art. 6 ust. 1 pkt f) RODO (uzasadniony interes). **3.** Identyfikacja celów przetwarzania wyselekcjonowanych danych. **4.** Oznaczenie wyselekcjonowanych danych jako objętych sprzeciwem w zakresie celów, dla których sprzeciw został uwzględniony. **5.** Zaprzestanie przetwarzania oznaczonych danych we wskazanych celach. <u>W przypadku, gdy dla celów objętych sprzeciwem dane przetwarzane są także w postaci papierowej:</u> Wyszukanie danych osobowych Wnioskodawcy przetwarzanych w postaci papierowej w celu realizacji uzasadnionego interesu Gminy lub innego podmiotu, innego niż marketing bezpośredni. Identyfikacja celów przetwarzania wyszukanych danych osobowych. Odnotowanie faktu zgłoszenia sprzeciwu w dokumentacji papierowej w formie właściwej dla tej dokumentacji, w tym w	**24**
Dedykowany pracownik Gminy[11]		**24**

11 W praktyce, przypadki przetwarzania danych osobowych postaci papierowej w celach związanych z uzasadnionym interesem, innych niż dochodzenie lub obrona przed ewentualnymi roszczeniami, będą występować bardzo rzadko.

OSOBA ODPOWIEDZIALNA	WYMAGANE DZIAŁANIA	MAKSYMALNY TERMIN[10] (W DNIACH OD WPŁYNIĘCIA ŻĄDANIA)
	formie notatki służbowej. Adnotacja powinna zawierać wskazanie: **a.** celów, dla których sprzeciw został uwzględniony; **b.** daty zgłoszenia sprzeciwu i daty dokonania adnotacji; **c.** podpisu osoby, dokonującej adnotacji. Zaprzestanie przetwarzania oznaczonych danych w celach objętych sprzeciwem. W razie, gdy dane osobowe przetwarzane były w postaci papierowej jedynie w celach objętych sprzeciwem, który został uwzględniony, nieodwracalne usunięcie (zniszczenie) danych osobowych lub zanonimizowanie dokumentów papierowych.	
V. Udzielenie odpowiedzi na żądanie		
Pracownik KOW	**1.** Udzielenie odpowiedzi na żądanie.	**maks. 1 miesiąc**

Załącznik G – Realizacja prawa do wycofania zgody na przetwarzanie danych

OSOBA ODPOWIEDZIALNA	WYMAGANE DZIAŁANIA	MAKSYMALNY TERMIN[12] (W DNIACH OD WPŁYNIĘCIA ŻĄDANIA)
Wszelkie czynności wykonywane w związku z realizacją przedmiotowego prawa powinny być realizowane niezwłocznie. W przypadku, gdy wycofanie zgody dotyczy działań marketingowych – o ile jest to możliwe techniczne, pracownik, do którego wpłynęło żądanie, albo KOW natychmiast po otrzymaniu żądania wstrzymuje komunikację o charakterze marketingowym względem Wnioskodawcy.		
I. Czynności formalne		
Pracownik KOW	**1.** Potwierdzenie przyjęcia żądania.	**1**
	Weryfikacja możliwości jednoznacznej identyfikacji Wnioskodawcy zgodnie z oddzielnymi procedurami. W braku takiej możliwości, udzielenie Wnioskodawcy odpowiedzi zgodnie z wzorem nr 4 określonym w załączniku K do Procedury obsługi żądań podmiotów danych.	**3**
II. Weryfikacja merytoryczna żądania		
Pracownik KOW	**1.** W razie konieczności, jednoznaczne potwierdzenie z Wnioskodawcą zakresu żądania. W braku jednoznacznego potwierdzenia zakresu żądania przez Wnioskodawcę, przekazanie Wnioskodawcy informacji potwierdzającej lub zaprzeczającej przetwarzaniu danych Wnioskodawcy przez Gminę. W przypadku istotnych wątpliwości co do sposobu rozstrzygnięcia żądania – konsultacja z IOD.	**7**
IOD	Rekomendacja co do sposobu rozstrzygnięcia żądania.	**9**
Pracownik KOW	Decyzja co do sposobu rozstrzygnięcia żądania.	**10**

[12] Wszystkie podane terminy mają charakter rekomendacji. W przypadku braku możliwości zrealizowania zgłoszonego żądania podmiotu danych w terminie 1 miesiąca od wpłynięcia wniosku, należy poinformować Wnioskodawcę o przedłużeniu terminu zgodnie z pkt 4.d Procedury obsługi wniosków podmiotów danych.

OSOBA ODPOWIEDZIALNA	WYMAGANE DZIAŁANIA	MAKSYMALNY TERMIN[12] (W DNIACH OD WPŁYNIĘCIA ŻĄDANIA)
III. Zawiadomienie o żądaniu dedykowanych pracowników Gminy		
Pracownik KOW	**1.** Przekazanie do dedykowanych pracowników Gminy informacji o zakresie, w jakim żądanie zostało uwzględnione, zgodnie z wzorem określonym w załączniku L do Procedury obsługi żądań podmiotów danych.	**12**
IV. Realizacja czynności niezbędnych dla spełnienia żądania Wnioskodawcy		
Dedykowany pracownik Gminy	**1.** Przeszukanie systemów informatycznych w zakresie danych osobowych dotyczących Wnioskodawcy. **2.** Wyselekcjonowanie danych przetwarzanych w celach wskazanych w zgłoszonym żądaniu. **3.** Wyodrębnienie w wyszukanych danych, danych przetwarzanych na podstawie art. 6 ust. 1 pkt a) RODO (zgoda podmiotu danych). **4.** W przypadku, gdy wyszukane dane przetwarzane są równocześnie dla innych celów niż objętych zgłoszonym żądaniem, zaprzestanie przetwarzania oznaczonych danych w celu objętym żądaniem. **5.** W przypadku, gdy wyszukane dane przetwarzane są wyłącznie dla celu objętego wycofanym oświadczeniem zgody, nieodwracalne usunięcie lub anonimizacja danych zgodnie z odrębnymi procedurami.	**24**
Dedykowany pracownik Gminy	<u>W przypadku, gdy dla celów objętych oświadczeniem o wycofaniu zgody dane przetwarzane są także w postaci papierowej:</u> **6.** Wyszukanie danych osobowych Wnioskodawcy przetwarzanych w postaci papierowej w celach wskazanych w zgłoszonym żądaniu. **7.** Wyodrębnienie w wyszukanych danych, danych przetwarzanych na podstawie art.	

OSOBA ODPOWIEDZIALNA	WYMAGANE DZIAŁANIA	MAKSYMALNY TERMIN[12] (W DNIACH OD WPŁYNIĘCIA ŻĄDANIA)
	6 ust. 1 pkt a) RODO (zgoda podmiotu danych). **8.** Odnotowanie faktu wycofania zgody w dokumentacji papierowej w formie właściwej dla tej dokumentacji, w tym w formie notatki służbowej. Adnotacja powinna zawierać następujące elementy: **a.** datę wycofania zgody i datę dokonania adnotacji; **b.** podpis osoby, dokonującej adnotacji. **9.** Jeżeli wyselekcjonowane dane przetwarzane są równocześnie dla innych celów niż objętych oświadczeniem zgody, zaprzestanie przetwarzania oznaczonych danych w celu objętym oświadczeniem wycofanej zgody. **10.** W razie, gdy dane osobowe przetwarzane były w postaci papierowej jedynie w celu objętym oświadczeniem zgody, nieodwracalne usunięcie (zniszczenie) danych osobowych lub zanonimizowanie dokumentów papierowych zgodnie z odrębnymi procedurami.	
V. Udzielenie odpowiedzi na żądanie		
Pracownik KOW	**1.** Udzielenie odpowiedzi na żądanie.	**maks. 1 miesiąc**

Załącznik H – Realizacja żądania w zakresie ograniczenia przetwarzania

OSOBA ODPOWIEDZIALNA	WYMAGANE DZIAŁANIA	MAKSYMALNY TERMIN[13] (W DNIACH OD WPŁYNIĘCIA ŻĄDANIA)
I. Czynności formalne		
Pracownik KOW	**1.** Potwierdzenie przyjęcia żądania.	**1**
	Weryfikacja możliwości jednoznacznej identyfikacji Wnioskodawcy zgodnie z oddzielnymi procedurami. W braku takiej możliwości, udzielenie Wnioskodawcy odpowiedzi zgodnie z wzorem nr 4 określonym w załączniku K do Procedury obsługi żądań podmiotów danych.	**3**
II. Weryfikacja merytoryczna żądania		
Pracownik KOW	**1.** W razie konieczności, jednoznaczne potwierdzenie z Wnioskodawcą zakresu żądania. **2.** W przypadkach, gdy żądanie ograniczenia przetwarzania wiąże się z: **a.** zakwestionowaniem przez podmiot danych prawidłowości jego danych; **b.** zgłoszeniem sprzeciwu dotyczącego celów innych niż marketing bezpośredni – niezwłoczne zawiadomienie o żądaniu dedykowanych pracowników Gminy zgodnie z częścią III. **3.** W przypadkach, gdy Wnioskodawca powołuje się na: **a.** przetwarzanie jego danych osobowych niezgodnie z prawem lub **b.** okoliczność, że Gmina nie potrzebuje już danych osobowych Wnioskodawcy do celów przetwarzania – weryfikacja merytoryczna żądania w zakresie jego zasadności. W razie	**7**

[13] Wszystkie podane terminy mają charakter rekomendacji. W przypadku braku możliwości zrealizowania zgłoszonego żądania podmiotu danych w terminie 1 miesiąca od wpłynięcia wniosku, należy poinformować Wnioskodawcę o przedłużeniu terminu zgodnie z pkt 4.d. Procedury obsługi wniosków podmiotów danych.

OSOBA ODPOWIEDZIALNA	WYMAGANE DZIAŁANIA	MAKSYMALNY TERMIN[13] (W DNIACH OD WPŁYNIĘCIA ŻĄDANIA)
	istotnych wątpliwości co do sposobu rozstrzygnięcia żądania – konsultacja z IOD. **4.** W przypadkach, gdy Wnioskodawca powołuje się na inne okoliczności niż określone w pkt 2 i 3 powyżej, odmowa ograniczenia przetwarzania z uwagi na brak przesłanek określonych w RODO.	
IOD	Rekomendacja co do sposobu rozstrzygnięcia żądania.	**9**
Pracownik KOW	Decyzja co do sposobu rozstrzygnięcia żądania.	**10**
III. Zawiadomienie o żądaniu dedykowanych pracowników Gminy		
Pracownik KOW	**1.** Przekazanie do dedykowanych pracowników Gminy informacji o zakresie, w jakim żądanie zostało uwzględnione, zgodnie z wzorem określonym w załączniku L do Procedury obsługi żądań podmiotów danych.	**12**
IV. Realizacja czynności niezbędnych dla spełnienia żądania Wnioskodawcy		
Dedykowany pracownik Gminy	**1.** Oznaczenie danych osobowych w systemach informatycznych objętych wnioskiem jako danych, których przetwarzanie zostało ograniczone. Zaprzestanie wykonywania operacji na tak oznaczonych danych osobowych z wyjątkiem: **a.** przechowywania; **b.** operacji niezbędnych do dochodzenia lub obrony przed roszczeniami; **c.** operacji, na które Wnioskodawca wyraził zgodę. Identyfikacja odbiorców danych osobowych Wnioskodawcy – podmiotów, którym ujawnione zostały dane osobowe Wnioskodawcy.	**24**

OSOBA ODPOWIEDZIALNA	WYMAGANE DZIAŁANIA	MAKSYMALNY TERMIN[13] (W DNIACH OD WPŁYNIĘCIA ŻĄDANIA)
Dedykowany pracownik Gminy	W przypadku, gdy dla celów objętych żądaniem ograniczenia dane przetwarzane są także w postaci papierowej: Wyszukanie danych osobowych Wnioskodawcy przetwarzanych w postaci papierowej. Odnotowanie faktu zgłoszenia żądania ograniczenia przetwarzania w dokumentacji papierowej w formie właściwej dla tej dokumentacji, w tym w formie notatki służbowej. Adnotacja powinna zawierać : **d.** datę wpłynięcia żądania ograniczenia przetwarzania i datę dokonania adnotacji; **e.** podpis osoby dokonującej adnotacji. Zaprzestanie wykonywania operacji na tak oznaczonych danych osobowych z wyjątkiem: **f.** przechowywania; **g.** operacji niezbędnych do dochodzenia lub obrony przed roszczeniami; **h.** operacji, na które Wnioskodawca wyraził zgodę. Identyfikacja odbiorców danych osobowych Wnioskodawcy – podmiotów, którym ujawnione zostały dane osobowe Wnioskodawcy.	
V. Udzielenie odpowiedzi na żądanie		
Pracownik KOW	**1.** Udzielenie odpowiedzi na żądanie. Powiadomienie o realizacji żądania Wnioskodawcy zidentyfikowanych odbiorców danych. W razie zgłoszenia takiego żądania przez Wnioskodawcę, powiadomienie Wnioskodawcy o wszystkich odbiorcach jego danych osobowych poprzez wskazanie co najmniej firm tych podmiotów.	**maks. 1 miesiąc**

OSOBA ODPOWIEDZIALNA	WYMAGANE DZIAŁANIA	MAKSYMALNY TERMIN[13] (W DNIACH OD WPŁYNIĘCIA ŻĄDANIA)
	W razie zamiaru zniesienia ograniczenia przetwarzania z uwagi na ustanie przesłanek uzasadniających ograniczenie – uprzednie poinformowanie o tym Wnioskodawcy, ze wskazaniem przyczyn zniesienia ograniczenia.	

Załącznik I – Realizacja żądania w zakresie usunięcia danych osobowych

OSOBA ODPOWIEDZIALNA	WYMAGANE DZIAŁANIA	MAKSYMALNY TERMIN[14] (W DNIACH OD WPŁYNIĘCIA ŻĄDANIA)
I. Czynności formalne		
Pracownik KOW	**1.** Potwierdzenie przyjęcia żądania.	**1**
	Weryfikacja możliwości jednoznacznej identyfikacji Wnioskodawcy zgodnie z oddzielnymi procedurami. W braku takiej możliwości, udzielenie Wnioskodawcy odpowiedzi zgodnie z wzorem nr 4 określonym w załączniku K do Procedury obsługi żądań podmiotów danych.	**3**
II. Weryfikacja merytoryczna żądania		
Pracownik KOW	**1.** W razie konieczności, jednoznaczne potwierdzenie z Wnioskodawcą zakresu żądania. **2.** W przypadku, gdy Wnioskodawca powołuje się na: **a.** zgłoszony przez siebie sprzeciw wobec przetwarzania danych w celu marketingu bezpośredniego; **b.** okoliczność, że dane osobowe Wnioskodawcy zostały zebrane w związku z oferowaniem usług społeczeństwa informacyjnego dziecku poniżej 16 roku życia – niezwłoczne zawiadomienie o żądaniu dedykowanych pracowników Gminy zgodnie z częścią III. **3.** W przypadku, gdy Wnioskodawca powołuje się na: **a.** fakt, że dane osobowe wnioskodawcy nie są już potrzebne Gminie dla osiągnięcia celów przetwarzania;	**7**

[14] Wszystkie podane terminy mają charakter rekomendacji. W przypadku braku możliwości zrealizowania zgłoszonego żądania podmiotu danych w terminie 1 miesiąca od wpłynięcia wniosku, należy poinformować Wnioskodawcę o przedłużeniu terminu zgodnie z pkt 4.4. Procedury obsługi wniosków podmiotów danych.

OSOBA ODPOWIEDZIALNA	WYMAGANE DZIAŁANIA	MAKSYMALNY TERMIN[14] (W DNIACH OD WPŁYNIĘCIA ŻĄDANIA)
	b. cofniętą zgodę na przetwarzanie danych osobowych; **c.** sprzeciw wobec przetwarzania w celach innych niż marketing bezpośredni; **d.** niezgodność z prawem przetwarzania danych osobowych lub prawny obowiązek Gminy usunięcia danych; - weryfikacja merytoryczna żądania w zakresie zasadności zgłoszonego żądania. W razie istotnych wątpliwości co do sposobu rozstrzygnięcia żądania – konsultacja z IOD. W przypadkach, gdy Wnioskodawca powołuje się na inne okoliczności niż określone w pkt 2 i 3 powyżej - weryfikacja merytoryczna żądania w zakresie faktycznego występowania przesłanek usunięcia danych osobowych. W braku takich przesłanek – odmowa usunięcia danych z uwagi na brak przesłanek określonych w RODO. W razie istotnych wątpliwości co do sposobu rozstrzygnięcia żądania – konsultacja z IOD	
IOD	Rekomendacja co do sposobu rozstrzygnięcia żądania.	**9**
Pracownik KOW	Decyzja co do sposobu rozstrzygnięcia żądania.	**10**
III. Zawiadomienie o żądaniu dedykowanych pracowników Gminy		
Pracownik KOW	**1.** Przekazanie do dedykowanych pracowników Gminy informacji o zakresie, w jakim żądanie zostało uwzględnione, zgodnie z wzorem określonym w załączniku L do Procedury obsługi żądań podmiotów danych.	**12**
IV. Realizacja czynności niezbędnych dla spełnienia żądania Wnioskodawcy		

OSOBA ODPOWIEDZIALNA	WYMAGANE DZIAŁANIA	MAKSYMALNY TERMIN[14] (W DNIACH OD WPŁYNIĘCIA ŻĄDANIA)
Dedykowany pracownik Gminy	**1.** Przeszukanie systemów informatycznych w zakresie danych osobowych dotyczących Wnioskodawcy. **2.** Oznaczenie dezaktualizacji celów przetwarzania, które stały się nieaktualne na skutek uwzględnienia żądania, wśród danych osobowych zawartych w wynikach wyszukiwania, z wyjątkiem: **a.** celu w postaci realizacji obowiązku wynikającego z przepisu prawa; **b.** celu w postaci realizacji korzystania z prawa do wolności wypowiedzi i informacji; **c.** celów archiwalnych w interesie publicznym, do celów badań naukowych lub historycznych lub do celów statystycznych; **d.** celu w postaci dochodzenia lub obrony przed roszczeniami; **e.** celu w postaci interesu publicznego wynikającego z odrębnych przepisów. **3.** Identyfikacja odbiorców danych osobowych Wnioskodawcy – podmiotów, którym ujawnione zostały dane osobowe Wnioskodawcy. **4.** Nieodwracalne usunięcie danych osobowych, w odniesieniu do których nieaktualne stały się wszystkie cele i podstawy prawne przetwarzania.	**24**
Dedykowany pracownik Gminy	<u>W przypadku, gdy dla celów objętych żądaniem usunięcia dane przetwarzane są także w postaci papierowej:</u> Wyszukanie danych osobowych Wnioskodawcy przetwarzanych w postaci papierowej. Identyfikacja celów przetwarzania wyszukanych danych osobowych, które stały się nieaktualne na skutek uwzględnienia żądania. Identyfikacja odbiorców danych osobowych Wnioskodawcy – podmiotów, którym	**24**

OSOBA ODPOWIEDZIALNA	WYMAGANE DZIAŁANIA	MAKSYMALNY TERMIN[14] (W DNIACH OD WPŁYNIĘCIA ŻĄDANIA)
	ujawnione zostały dane osobowe Wnioskodawcy. W razie, gdy dane osobowe przetwarzane były w postaci papierowej jedynie w celach, które stały się nieaktualne na skutek złożonego żądania, nieodwracalne usunięcie (zniszczenie) danych osobowych lub zanonimizowanie dokumentów papierowych. W razie, gdy dane osobowe przetwarzane były w postaci papierowej także: **a.** w celu realizacji obowiązku wynikającego z przepisu prawa; **b.** w celu realizacji korzystania z prawa do wolności wypowiedzi i informacji; **c.** w celach archiwalnych w interesie publicznym, do celów badań naukowych lub historycznych lub do celów statystycznych; **d.** w celu dochodzenia lub obrony przed roszczeniami; – oznaczenie tych danych osobowych poprzez odnotowanie: **e.** celów, dla których żądanie usunięcia danych zostało uwzględnione; **f.** daty zgłoszenia żądania i daty dokonania adnotacji; **g.** podpisu osoby, dokonującej adnotacji; – oraz zaprzestanie przetwarzania oznaczonych danych w celach, dla których żądanie usunięcia danych zostało uwzględnione.	
Pracownik KOW	**5.** W przypadku, gdy dane osobowe Wnioskodawcy zostały upublicznione przez Gminę (np. na stronie internetowej Gminy), o ile będzie to rozsądnie możliwe, poinformowanie innych administratorów danych osobowych o żądaniu usunięcia danych, w tym wszystkich kopii i łącz do tych danych osobowych.	**26**
V. Udzielenie odpowiedzi na żądanie		

OSOBA ODPOWIEDZIALNA	WYMAGANE DZIAŁANIA	MAKSYMALNY TERMIN[14] (W DNIACH OD WPŁYNIĘCIA ŻĄDANIA)
Pracownik KOW	**1.** Udzielenie odpowiedzi na żądanie. **2.** Powiadomienie o realizacji żądania Wnioskodawcy zidentyfikowanych odbiorców danych. **3.** W razie zgłoszenia takiego żądania przez Wnioskodawcę, powiadomienie Wnioskodawcy o wszystkich odbiorcach jego danych osobowych poprzez wskazanie co najmniej firm tych podmiotów.	**maks. 1 miesiąc**

Załącznik J – Procedura postępowania w przypadku zgłoszenia żądania przez pełnomocnika

OSOBA ODPOWIEDZIALNA	WYMAGANE DZIAŁANIA	MAKSYMALNY TERMIN[15] (W DNIACH OD WPŁYNIĘCIA ŻĄDANIA)
I. Czynności formalne		
Pracownik KOW	**1.** Potwierdzenie przyjęcia żądania.	**1**
	Weryfikacja złożonego pełnomocnictwa pod kątem formalnym poprzez stwierdzenie czy został spełniony jeden z poniższych warunków: **a.** pełnomocnictwo ma formę aktu notarialnego; **b.** pełnomocnictwo ma formę pisemną i zostało poświadczone przez notariusza; **c.** pełnomocnictwo ma formę pisemną, zostało udzielone adwokatowi lub radcy prawnemu i zostało poświadczone przez tego adwokata lub radcę prawnego; Weryfikacja tożsamości pełnomocnika poprzez wgląd do dokumentu tożsamości.	**1**
II-A. Czynności w przypadku złożenia pełnomocnictwa w jednej z form wymienionych w ust. 2 powyżej		
Pracownik KOW	**1.** Weryfikacja złożonego pełnomocnictwa pod kątem merytorycznym poprzez stwierdzenie, czy złożone pełnomocnictwo zawiera wszystkie następujące elementy: **a.** jednoznaczne określenie podmiotu danych (osoby, której dane dotyczą); **b.** jednoznaczne określenie pełnomocnika (imienia i nazwiska oraz dodatkowej danej identyfikującej – np. nr PESEL, nr dokumentu tożsamości, nr wpisu na listę radców prawnych lub adwokatów);	**2**

[15] Wszystkie podane terminy mają charakter rekomendacji. W przypadku braku możliwości zrealizowania zgłoszonego żądania podmiotu danych w terminie 1 miesiąca od wpłynięcia wniosku, należy poinformować Wnioskodawcę o przedłużeniu terminu zgodnie z pkt 4.4. Procedury obsługi wniosków podmiotów danych.

OSOBA ODPOWIEDZIALNA	WYMAGANE DZIAŁANIA	MAKSYMALNY TERMIN[15] (W DNIACH OD WPŁYNIĘCIA ŻĄDANIA)
	c. jednoznaczne określenie zakresu żądania poprzez wskazanie podmiotu będącego administratorem danych osobowych oraz prawa lub praw, których realizacji dotyczy żądanie. **2.** W przypadku, gdy któryś z elementów wskazanych w pkt. od a. do c. budzi uzasadnione wątpliwości – konsultacja z IOD.	
IOD	Rekomendacja w zakresie uznania czy pełnomocnictwo spełnia minimalne wymogi określone w Procedurze.	**3**
Pracownik KOW	Decyzja co do uznania pełnomocnictwa za spełniające minimalne wymogi określone w Procedurze. *W przypadku uznania pełnomocnictwa za spełniające minimalne wymogi określone Procedurą, dalsze czynności realizowane są zgodnie z cz.II–V załączników od A do H.*	**3**
II-B. Czynności w przypadku złożenia pełnomocnictwa w formie innej niż wskazane w ust 2 powyżej		
Pracownik KOW	**1.** Zwrócenie się o opinię IOD w przedmiocie dopuszczalności przyjęcia żądania zgłoszonego na podstawie pełnomocnictwa. **2.** Ocena, czy przedstawione pełnomocnictwo budzi jakiekolwiek wątpliwości co do swojej wiarygodności. W razie stwierdzenia, że pełnomocnictwo budzi wątpliwości co do swojej wiarygodności, udzielenie odpowiedzi zgodnie z wzorem nr 4 załącznika J do Procedury. **3.** W razie stwierdzenia, że przedstawione pełnomocnictwo nie budzi wątpliwości co do swojej wiarygodności, zwrócenie się do IOD o wyrażenie zgody na rozpoznanie żądania.	**2**

OSOBA ODPOWIEDZIALNA	WYMAGANE DZIAŁANIA	MAKSYMALNY TERMIN[15] (W DNIACH OD WPŁYNIĘCIA ŻĄDANIA)
IOD	Wydanie opinii w przedmiocie dopuszczalności przyjęcia żądania zgłoszonego na podstawie pełnomocnictwa. Wyrażenie lub odmowa zgody na rozpoznanie żądania w oparciu o przedstawione pełnomocnictwo w formie innej niż określone w ust. 2. *Wyrażając opinię, IOD może jednocześnie udzielić rekomendacji w zakresie, o jakim mowa w pkt. 0 poniżej.*	**4**
Pracownik KOW	W razie negatywnej oceny dopuszczalności przyjęcia żądania zgłoszonego na podstawie pełnomocnictwa, udzielenie odpowiedzi zgodnie z wzorem nr 4 załącznika K do Procedury. W razie pozytywnej oceny dopuszczalności przyjęcia żądania zgłoszonego na podstawie pełnomocnictwa, weryfikacja złożonego pełnomocnictwa pod kątem merytorycznym poprzez stwierdzenie, czy złożone pełnomocnictwo zawiera wszystkie następujące elementy: **a.** jednoznaczne określenie podmiotu danych (osoby, której dane dotyczą); **b.** jednoznaczne określenie pełnomocnika (imienia i nazwiska oraz dodatkowej danej identyfikującej – np. nr PESEL, nr dokumentu tożsamości, nr wpisu na listę radców prawnych lub adwokatów); **c.** jednoznaczne określenie zakresu żądania poprzez wskazanie podmiotu będącego administratorem danych osobowych oraz prawa lub praw, których realizacji dotyczy żądanie. W przypadku, gdy któryś z elementów wskazanych w pkt od a. do c. budzi uzasadnione wątpliwości – konsultacja z IOD.	**5**

OSOBA ODPOWIEDZIALNA	WYMAGANE DZIAŁANIA	MAKSYMALNY TERMIN[15] (W DNIACH OD WPŁYNIĘCIA ŻĄDANIA)
IOD	Rekomendacja w zakresie uznania, czy pełnomocnictwo spełnia minimalne wymogi określone w Procedurze.	**6**
Pracownik KOW	Decyzja co do uznania pełnomocnictwa za spełniające minimalne wymogi określone w Procedurze. *W przypadku uznania pełnomocnictwa za spełniające minimalne wymogi określone Procedurą, Dalsze czynności realizowane są zgodnie z częściami II–V załączników od A do I.*	**maks. 7 dni od wpłynięcia żądania**

Załącznik K – Wzory pism stosowanych w Procedurze

Wzór informacji o przedłużeniu terminu rozpoznania żądania 88
Wzór odpowiedzi na żądanie w przypadku konieczności pobrania opłaty 89
Wzór odpowiedzi na żądanie w przypadku odmowy podjęcia czynności w związku z wnioskiem 89
Wzór odpowiedzi na żądanie w przypadku braku możliwości jednoznacznej identyfikacji wnioskodawcy, w tym z uwagi na nieprawidłowe pełnomocnictwo 91
Wzór wezwania do doprecyzowania żądania 92
Wzór odpowiedzi w wypadku uwzględnienia w całości żądania podmiotu danych 92
Wzór odpowiedzi w wypadku częściowego uwzględnienia żądania 94
Wzór odpowiedzi w wypadku, gdy Gmina nie przetwarza danych osobowych wnioskodawcy 95

WZÓR INFORMACJI O PRZEDŁUŻENIU TERMINU ROZPOZNANIA ŻĄDANIA

[**data**]

[**dane Wnioskodawcy**]

Dot. żądania nr

Szanowna Pani / Szanowny Panie,

Uprzejmie informujemy, że zgłoszone przez Panią / Pana żądanie w przedmiocie realizacji praw związanych z przetwarzaniem Pani / Pana danych osobowych przez nie mogło zostać rozpoznane w standardowym 1-miesięcznym terminie z uwagi na .

Z uwagi na powyższe okoliczności termin rozpoznania Pani / Pana żądania został przedłużony do dnia .

Informujemy, że na przetwarzanie Pani / Pana danych osobowych niezgodnie z przepisami Rozporządzenia ogólnego o ochronie danych osobowych[16] przysługuje Pani / Panu prawo wniesienia skargi do organu nadzorczego – Prezesa Urzędu Ochrony Danych Osobowych – oraz skorzystania ze środków ochrony prawnej przed sądem, zgodnie z właściwymi przepisami.

Przypominamy, że ogólne informacje dotyczące przetwarzania danych osobowych przez można uzyskać:

a) na stronie internetowej w zakładce Prywatność;
b) pod adresem e-mailowym Inspektora Ochrony Danych : .

Z poważaniem

Załączniki:

1) [jeśli dotyczy]
2) [jeśli dotyczy]

[16] Rozporządzenie Parlamentu Europejskiego i Rady UE 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (Dz. Urz. UE. L. 2016 Nr 119 str. 1).

WZÓR ODPOWIEDZI NA ŻĄDANIE W PRZYPADKU KONIECZNOŚCI POBRANIA OPŁATY

[**data**]

[**dane Wnioskodawcy**]

Dot. żądania nr

Szanowna Pani / Szanowny Panie,

Uprzejmie informujemy, że w ocenie zgłoszone przez Panią / Pana żądanie w przedmiocie realizacji praw związanych z przetwarzaniem Pani / Pana danych osobowych przez należy uznać za nadmierne z uwagi na .

Z uwagi na wyżej wskazane okoliczności żądanie zostanie rozpoznane pod warunkiem uiszczenia przez Panią / Pana opłaty w wysokości . Opłatę należy uiścić na rachunek bankowy :

W tytule przelewu należy wskazać numer żądania znajdujący się w nagłówku pisma. Prosimy o przesłanie dowodu uiszczenia opłaty na adres e-mailowy lub za pośrednictwem faksu na nr .

W razie uiszczenia opłaty w terminie późniejszym niż 7 dni od dnia otrzymania niniejszego pisma, uprzejmie prosimy o poinformowanie Gminy o dokonaniu opłaty drogą telefoniczną pod nr lub e-mailową na adres: .

Informujemy, że na przetwarzanie Pani / Pana danych osobowych niezgodnie z przepisami Rozporządzenia ogólnego o ochronie danych osobowych[17] przysługuje Pani / Panu prawo wniesienia skargi do organu nadzorczego – Prezesa Urzędu Ochrony Danych Osobowych – oraz skorzystania ze środków ochrony prawnej przed sądem, zgodnie z właściwymi przepisami.

Przypominamy jednocześnie, że ogólne informacje dotyczące przetwarzania danych osobowych przez można uzyskać:

a) na stronie internetowej w zakładce Prywatność;
b) pod adresem e-mailowym Inspektora Ochrony Danych : .

Z poważaniem

Załączniki:

1) [jeśli dotyczy]

WZÓR ODPOWIEDZI NA ŻĄDANIE W PRZYPADKU ODMOWY PODJĘCIA CZYNNOŚCI W ZWIĄZKU Z WNIOSKIEM

[17] Rozporządzenie Parlamentu Europejskiego i Rady UE 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (Dz. Urz. UE. L. 2016 Nr 119 str. 1).

[**data**]

[**dane Wnioskodawcy**]

Dot. wniosku nr

Szanowna Pani / Szanowny Panie,

Uprzejmie informujemy, że w ocenie zgłoszone przez Panią / Pana żądanie w przedmiocie realizacji praw związanych z przetwarzaniem Pani / Pana danych osobowych przez należy uznać za nadmierne z uwagi na .

Z uwagi na wskazane wyżej okoliczności żądanie nie zostanie rozpoznane.

Informujemy, że na przetwarzanie Pani / Pana danych osobowych niezgodnie z przepisami Rozporządzenia ogólnego o ochronie danych osobowych[18] przysługuje Pani / Panu prawo wniesienia skargi do organu nadzorczego – Prezesa Urzędu Ochrony Danych Osobowych – oraz skorzystania ze środków ochrony prawnej przed sądem, zgodnie z właściwymi przepisami.

Przypominamy jednocześnie, że ogólne informacje dotyczące przetwarzania danych osobowych przez można uzyskać:

c) na stronie internetowej w zakładce Prywatność;
d) pod adresem e-mailowym Inspektora Ochrony Danych : .

Z poważaniem

Załączniki:

1) [jeśli dotyczy]
2) [jeśli dotyczy]

[18] Rozporządzenie Parlamentu Europejskiego i Rady UE 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (Dz. Urz. UE. L. 2016 Nr 119 str. 1).

WZÓR ODPOWIEDZI NA ŻĄDANIE W PRZYPADKU BRAKU MOŻLIWOŚCI JEDNOZNACZNEJ IDENTYFIKACJI WNIOSKODAWCY, W TYM Z UWAGI NA NIEPRAWIDŁOWE PEŁNOMOCNICTWO

[**data**]

[**dane Wnioskodawcy**]

Dot. żądania nr

Szanowna Pani / Szanowny Panie,

Uprzejmie informujemy, że złożone przez Panią / Pana żądanie w przedmiocie realizacji praw związanych z przetwarzaniem Pani / Pana danych osobowych przez nie mogło zostać rozpoznane z uwagi na brak możliwości jednoznacznego potwierdzenia tożsamości wnioskodawcy, pomimo wezwania Pani / Pana do potwierdzenia tożsamości zgodnie z odrębnymi procedurami.

nie ma możliwości udzielenia odpowiedzi na żądanie z uwagi na ryzyko naruszenia bezpieczeństwa i poufności danych poprzez ich przekazanie osobie nieuprawnionej. Zapewniamy, że niezwłocznie po potwierdzeniu przez Panią / Pana tożsamości, zgodnie z przedstawionymi wymogami, zgłoszone żądanie zostanie rozpoznane.

W przypadku, gdy żądanie składane jest przez pełnomocnika, zachęcamy do przedstawienia pełnomocnictwa poświadczonego przez notariusza lub radcę prawnego / adwokata występującego w sprawie, co przyspieszy weryfikację zgłaszanego żądania.

Informujemy, że na przetwarzanie Pani / Pana danych osobowych niezgodnie z przepisami Rozporządzenia ogólnego o ochronie danych osobowych[19] przysługuje Pani / Panu prawo wniesienia skargi do organu nadzorczego – Prezesa Urzędu Ochrony Danych Osobowych – oraz skorzystania ze środków ochrony prawnej przed sądem, zgodnie z właściwymi przepisami.

Przypominamy jednocześnie, że ogólne informacje dotyczące przetwarzania danych osobowych przez można uzyskać:

a) Na stronie internetowej w zakładce Prywatność;
b) pod adresem e-mailowym Inspektora Ochrony Danych : .

Z poważaniem

[19] Rozporządzenie Parlamentu Europejskiego i Rady UE 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (Dz. Urz. UE. L. 2016 Nr 119 str. 1).

WZÓR WEZWANIA DO DOPRECYZOWANIA ŻĄDANIA

[**data**]

[**dane Wnioskodawcy**]

Dot. żądania nr

Szanowna Pani / Szanowny Panie,

W nawiązaniu do złożonego przez Panią / Pana żądania w przedmiocie realizacji praw związanych z przetwarzaniem Pani / Pana danych osobowych przez uprzejmie prosimy o doprecyzowanie zgłaszanego żądania poprzez wskazanie .

Brak podania informacji we wskazanym wyżej zakresie uniemożliwia merytoryczne rozpoznanie złożonego żądania.

Informujemy, że na przetwarzanie Pani / Pana danych osobowych niezgodnie z przepisami Rozporządzenia ogólnego o ochronie danych osobowych[20] przysługuje Pani / Panu prawo wniesienia skargi do organu nadzorczego – Prezesa Urzędu Ochrony Danych Osobowych – oraz skorzystania ze środków ochrony prawnej przed sądem, zgodnie z właściwymi przepisami.

Przypominamy, że ogólne informacje dotyczące przetwarzania danych osobowych przez można uzyskać:

a) na stronie internetowej w zakładce Prywatność;
b) pod adresem e-mailowym Inspektora Ochrony Danych : .

Z poważaniem

Załączniki:

1) [jeśli dotyczy]
2) [jeśli dotyczy]

WZÓR ODPOWIEDZI W WYPADKU
UWZGLĘDNIENIA W CAŁOŚCI ŻĄDANIA PODMIOTU DANYCH

[20] Rozporządzenie Parlamentu Europejskiego i Rady UE 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (Dz. Urz. UE. L. 2016 Nr 119 str. 1).

[**data**]

[**dane Wnioskodawcy**]

Dot. żądania nr

Szanowna Pani / Szanowny Panie,

Uprzejmie informujemy, że zgłoszone przez Panią / Pana żądanie w przedmiocie realizacji praw związanych z przetwarzaniem Pani / Pana danych osobowych zostało uwzględnione w całości i zrealizowane w dniu .

Przypominamy, że ogólne informacje dotyczące przetwarzania danych osobowych przez można uzyskać:

a) na stronie internetowej w zakładce Prywatność;
b) pod adresem e-mailowym Inspektora Ochrony Danych : .

Z poważaniem

Załączniki:

1) [jeśli dotyczy]
2) [jeśli dotyczy]

WZÓR ODPOWIEDZI W WYPADKU CZĘŚCIOWEGO UWZGLĘDNIENIA ŻĄDANIA

[**data**]

[**dane Wnioskodawcy**]

Dot. żądania nr

Szanowna Pani / Szanowny Panie,

W nawiązaniu do Pani / Pana żądania w przedmiocie realizacji praw związanych z przetwarzaniem Pani / Pana danych osobowych przez , uprzemie informujemy, że Pani / Pana żądanie zostało uwzględnione w zakresie .

W zakresie, w jakim żądanie nie mogło zostać uwzględnione, wyjaśniamy, że

[Należy wskazać uzasadnienie częściowej odmowy realizacji żądania – np. posiadanie ważnej podstawy prawnej przetwarzania, brak wystąpienia przesłanek żądania określonych w przepisach itd.]

Informujemy, że na przetwarzanie Pani / Pana danych osobowych niezgodnie z przepisami Rozporządzenia ogólnego o ochronie danych osobowych[21] przysługuje Pani / Panu prawo wniesienia skargi do organu nadzorczego – Prezesa Urzędu Ochrony Danych Osobowych – oraz skorzystania ze środków ochrony prawnej przed sądem, zgodnie z właściwymi przepisami.

Przypominamy jednocześnie, że ogólne informacje dotyczące przetwarzania danych osobowych przez można uzyskać:

a) na stronie internetowej w zakładce Prywatność;
b) pod adresem e-mailowym Inspektora Ochrony Danych : .

Z poważaniem

Załączniki:

1) [jeśli dotyczy]
2) [jeśli dotyczy]

[21] Rozporządzenie Parlamentu Europejskiego i Rady UE 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (Dz. Urz. UE. L. 2016 Nr 119 str. 1).

WZÓR ODPOWIEDZI W WYPADKU,
GDY GMINA NIE PRZETWARZA DANYCH OSOBOWYCH WNIOSKODAWCY

[**data**]

[**dane Wnioskodawcy**]

Dot. żądania nr

Szanowna Pani / Szanowny Panie,

W nawiązaniu do Pani / Pana żądania w przedmiocie realizacji praw związanych z przetwarzaniem Pani / Pana danych osobowych przez , uprzemie informujemy, że nie przetwarza aktualnie żadnych danych osobowych Pani / Pana dotyczących.

Informujemy, że na przetwarzanie Pani / Pana danych osobowych niezgodnie z przepisami Rozporządzenia ogólnego o ochronie danych osobowych[22] przysługuje Pani / Panu prawo wniesienia skargi do organu nadzorczego – Prezesa Urzędu Ochrony Danych Osobowych – oraz skorzystania z środków ochrony prawnej przed sądem, zgodnie z właściwymi przepisami.

Przypominamy jednocześnie, że ogólne informacje dotyczące przetwarzania danych osobowych przez można uzyskać:

a) na stronie internetowej w zakładce Prywatność;
b) pod adresem e-mailowym Inspektora Ochrony Danych : .

Z poważaniem

Załączniki:

1) [jeśli dotyczy]
2) [jeśli dotyczy]

22 Rozporządzenie Parlamentu Europejskiego i Rady UE 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (Dz. Urz. UE. L. 2016 Nr 119 str. 1).

Załącznik L – Wzór zawiadomienia dedykowanych pracowników o wpłynięciu żądania

ZAWIADOMIENIE O WPŁYNIĘCIU ŻĄDANIA O REALIZACJĘ PRAW PODMIOTU DANYCH					
4. P.	**5. DATA WPŁYWU ŻĄDANIA**	**6. WNIOSKODAWCA**	**7. ZAKRES ŻĄDANIA PODLEGAJĄCY WYKONANIU**	**8. TERMIN REALIZACJI ŻĄDANIA**	**9. DODATKOWE UWAGI**
	Należy wskazać dokładną datę otrzymania żądania przez Gminę. Datę należy wprowadzić w formacie [dd-mm-rr]	Należy podać imię i nazwisko Wnioskodawcy.	Należy wskazać zakres żądania, jaki zobowiązany jest zrealizować dedykowany pracownik Gminy.	Należy wskazać termin wynikający z Procedury obsługi żądań podmiotów danych (określony w załącznikach A–I do Procedury)	W tym miejscu można wpisać wszelkie dodatkowe informacje, które mogą okazać się pomocne w realizacji żądania przez pracownika merytorycznego.
10.					
11.					
12.					
13.					
14.					

Załącznik M – Wzór rejestru żądań

REJESTR ŻĄDAŃ DOTYCZĄCYCH PRAW PODMIOTÓW DANYCH								
Lp.	**Data wpływu żądania**	**Wniosko-dawca**	**Forma żądania**	**Przedmiot żądania**	**Sposób rozstrzygnięcia**	**Termin realizacji żądania**	**Forma realizacji żądania**	**Dodatkowe uwagi**
15.	Należy wskazać dokładną datę otrzymania żądania przez Gminę. Datę należy wprowadzić w formacie [dd-mm-rr].	Należy podać imię i nazwisko Wnioskodawcy.	Należy wskazać formę w jakiej żądanie zostało zgłoszone Gminie (elektroniczna/ papierowa/inna).	Należy wskazać rodzaj żądania, a także zakres danych osobowych objętych żądaniem (np. żądanie aktualizacji danych w zakresie nazwiska i adresu korespondencyjnego)	Należy wskazać, czy i w jakim zakresie żądanie zostało uwzględnione. W razie odmowy uwzględnienia żądania należy krótko wskazać przyczyny odmowy.	Należy wskazać dokładną datę udzielenia odpowiedzi na żądanie.	Należy wskazać formę, w jakiej udzielono odpowiedzi.	W tym miejscu można wpisać wszelkie dodatkowe informacje, które mogą okazać się pomocne w realizacji wniosku przez pracownika merytorycznego.
16.								
17.								
18.								
19.								

GMINA MIEDŹNO

POLITYKA ANALIZY RYZYKA I OCENY SKUTKÓW PRZETWARZANIA DANYCH OSOBOWYCH

METRYKA DOKUMENTU	
STATUS	Dokument wewnętrzny
WERSJA DOKUMENTU	1.0
DATA DOKUMENTU	31.10.2023 r.
LICZBA STRON	183
CEL DOKUMENTU	Niniejszy dokument opisuje zasady realizacji obowiązków wynikających z RODO w zakresie analizy ryzyka oraz prowadzenie oceny skutków przetwarzania danych.
SPIS TREŚCI	1. Definicje ..... 100 2. Postanowienia ogólne ..... 101 3. Ocena Privacy by Design ..... 101 4. Ocena prawdopodobieństwa (Preewaluacja) ..... 102 5. Uproszczona ocena ..... 103 6. Ocena skutków przetwarzania dla ochrony danych (DPIA) ..... 103 7. Postanowienia końcowe 104

DEFINICJE

Administrator - **Gmina Miedźno** z siedzibą w Miedźnie ul. Ułańska 25, 42-120 Miedźno, NIP: 5742055080.

Dane osobowe – wszelkie informacje dotyczące osoby fizycznej lub z nią związane, np. imię, nazwisko, adres IP, informacje zebrane przez pliki cookies, linie papilarne, dane o lokalizacji, numery ID, wizerunek twarzy / osoby (w tym dane z monitoringu), numer rachunku bankowego, adres zamieszkania, adres zameldowania, nr dowodu osobistego, paszportu, prawa jazdy, PESEL, NIP, REGON, wykształcenie, zawód, stanowisko, stan rodzinny, imiona rodziców, sygn. akt / nr decyzji w przypadku orzeczeń sądowych, administracyjnych, jednostki chorobowe, nałogi, informacje o aktywności użytkownika strony internetowej, informacje o przebiegu współpracy (np. historia zamówień), informacje o poglądach politycznych, informacje o orientacji seksualnej itp.

DPIA lub **Ocena DPIA –** ocena skutków przetwarzania danych osobowych, dokonywana w przypadku, gdy w wyniku Preewaluacji stwierdzono duże prawdopodobieństwo wystąpienia wysokiego ryzyka naruszenia praw lub wolności osób fizycznych.

IOD – Inspektor Ochrony Danych, wyznaczony przez Gminę nadzorujący przestrzeganie przepisów o ochronie danych osobowych w Gminie, wykonujący zadania określone w art. 39 RODO.

Nowa Inicjatywa – każda nowa inicjatywa operacyjna lub strategiczna, której istota realizacji lub jej produktu końcowego polega na przetwarzaniu danych osobowych – inna niż poprzednia podobna Nowa Inicjatywa, dla której analiza ryzyka była już realizowana (tzn. inna pod względem kategorii podmiotów danych, zakresu danych, celu i sposobów przetwarzania). Nową Inicjatywą nie jest dokonywanie zakupu programów komputerowych (systemów, aplikacji) będących jedynie narzędziem informatycznym wykorzystywanym w celu realizacji inicjatywy.

Organ nadzorczy – Prezes Urzędu Ochrony Danych Osobowych, lub ewentualnie właściwy organ nadzorczy w zakresie danych osobowych wyznaczony przez inne państwo członkowie Unii Europejskiej.

Osoba odpowiedzialna – osoba odpowiedzialna za realizację Nowej Inicjatywy, a w odniesieniu do Procesów istniejących w chwili przyjęcia Polityki osoba odpowiedzialna za realizację danego Procesu. Osoba odpowiedzialna może przy wykonywaniu zadań określonych Polityką posługiwać się innymi osobami, co nie zwalnia jej z odpowiedzialności za wykonanie tych zadań.

Polityka – niniejsza Polityka analizy ryzyka i oceny skutków przetwarzania danych osobowych.

Preewaluacja – ocena prawdopodobieństwa wystąpienia wysokiego ryzyka naruszenia praw lub wolności osób fizycznych.

Proces przetwarzania danych osobowych lub **Proces –** proces przetwarzania danych osobowych zidentyfikowany w rejestrze czynności przetwarzania prowadzonym przez Administratora.

Uproszczona ocena – uproszczona ocena Nowych Inicjatyw lub Procesów, dokonywana w przypadku, gdy w wyniku Preewaluacji nie stwierdzono dużego prawdopodobieństwa wystąpienia wysokiego ryzyka naruszenia praw lub wolności osób fizycznych.

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.

Zagrożenie – potencjalne zagrożenie dotyczące operacji przetwarzania danych osobowych, mogące skutkować naruszeniem poufności, integralności lub dostępności tych danych, zidentyfikowane w ramach dokonywania Oceny DPIA.

POSTANOWIENIA OGÓLNE

Polityka opisuje zasady prowadzenia analizy ryzyka dla ochrony danych osobowych w Gminie**.**

Analiza ryzyka składa się z następujących elementów:

Oceny Privacy by Design;

Preewaluacji;

w zależności od wyników oceny prawdopodobieństwa wystąpienia wysokiego ryzyka naruszenia prywatności: Oceny skutków przetwarzania dla ochrony danych (DPIA) albo Uproszczonej oceny.

OCENA PRIVACY BY DESIGN

Przedmiotem Oceny Privacy by Design są wszystkie Nowe Inicjatywy.

Celem Oceny Privacy by Design jest dostosowanie założeń Nowych Inicjatyw do podstawowych zasad RODO – w szczególności w zakresie spełnienia zasady zgodności z prawem, rzetelności i przejrzystości, zasady minimalizacji danych, zasady ograniczenia celu oraz zasady ograniczenia przechowywania – tak, aby spełnić wymogi RODO oraz chronić prawa osób, których dane dotyczą.

Ocena Privacy by Design dokonywana jest:

z wykorzystaniem narzędzia (formularza) zawartego w załączniku A do Polityki;

przez Osobę odpowiedzialną, w porozumieniu z IOD oraz przy wsparciu prawnym;

bezpośrednio po ustaleniu założeń Nowej Inicjatywy (które powinny zostać wskazane w Opisie Nowej Inicjatywy w formularzu zawartym w załączniku A), ale przed przystąpieniem do jej realizacji.

OCENA PRAWDOPODOBIEŃSTWA (PREEWALUACJA)

Przedmiotem Preewaluacji są wszystkie Nowe Inicjatywy oraz Procesy realizowane w chwili wejścia w życie Polityki.

Celem Preewaluacji jest ustalenie, czy Nowa Inicjatywa lub Proces przetwarzania danych osobowych wymaga przeprowadzenia Oceny DPIA.

Preewaluacja dokonywana jest z wykorzystaniem narzędzia (formularza) zawartego w załączniku A do Polityki.

Preewaluacja dokonywana jest przez Osobę odpowiedzialną, w porozumieniu z IOD oraz przy wsparciu prawnym.

Preewaluacja dokonywana jest:

- w przypadku Procesów przetwarzania danych osobowych istniejących w dniu przyjęcia Polityki – w terminie do 3 miesięcy do wejścia w życie polityki.
- w przypadku Nowych Inicjatyw – na etapie projektowania w ramach pracy nad Nową Inicjatywą.

W wyniku Preewaluacji Osoba odpowiedzialna, po zasięgnięciu opinii IOD, podejmuje decyzję o:

- przeprowadzeniu Oceny DPIA – w przypadku Procesów lub Nowych Inicjatyw, które z dużym prawdopodobieństwem mogą powodować wysokie ryzyko naruszenia praw lub wolności osób fizycznych; albo
- przeprowadzeniu Uproszczonej oceny – w przypadku Procesów lub Nowych Inicjatyw innych niż wskazane w pkt 0.

Wynik Preewaluacji ustala się, opierając się na następujących zasadach:

- jeżeli Proces lub Nowa Inicjatywa znajduje się w wykazie opublikowanym przez Organ nadzorczy, przeprowadzenie DPIA jest konieczne; w takim wypadku nie ma obowiązku wypełniania formularza zawartego w załączniku A w pozostałym zakresie;
- jeżeli spełnione są co najmniej dwa kryteria pozytywne wskazane w formularzu stanowiącym załącznik A i nie występuje kryterium negatywne, należy co do zasady przyjąć, że przeprowadzenie DPIA jest konieczne. Osoba odpowiedzialna może jednak uznać – biorąc pod uwagę dodatkowe okoliczności i po zasięgnięciu opinii IOD – że nie występuje sytuacja, która „może powodować wysokie ryzyko", uzasadniająca przeprowadzanie DPIA. W takich przypadkach należy tę decyzję uzasadnić i udokumentować powody, dla których nie przeprowadzono Oceny DPIA;
- jeśli spełnione jest tylko jedno lub nie spełniono żadnego kryterium pozytywnego, należy co do zasady przyjąć, że nie jest konieczne przeprowadzenie DPIA i należy przeprowadzić Uproszczoną ocenę. Osoba odpowiedzialna może jednak uznać – biorąc pod uwagę dodatkowe okoliczności – że takie przetwarzanie będzie wymagało przeprowadzenia DPIA (np. z uwagi na cel przetwarzania danych);

jako zasadę należy przyjąć, że im więcej kryteriów zostało spełnionych, tym większe jest prawdopodobieństwo wystąpienia wysokiego ryzyka naruszenia praw i wolności osób, których dane dotyczą, i tym bardziej zalecane jest przeprowadzenie DPIA.

UPROSZCZONA OCENA

Przedmiotem Uproszczonej oceny są Nowe Inicjatywy oraz Procesy przetwarzania danych osobowych, o ile nie podlegają wymogowi przeprowadzenia DPIA.

Celem Uproszczonej oceny jest ustalenie, jakie środki (organizacyjne oraz techniczne) są niezbędne i proporcjonalne dla zapewnienia odpowiedniego stopnia ochrony danych osobowych wykorzystywanych w Nowej Inicjatywie lub Procesie tak, aby spełnić wymogi RODO oraz chronić prawa osób, których dane dotyczą. Środki te dotyczą w szczególności zapewnienia legalności przetwarzania danych osobowych oraz instrumentów legalizujących ich przekazywanie podmiotom zewnętrznym; realizacji podstawowych zasad przetwarzania danych; zachowania praw osób, których dane dotyczą.

Uproszczona ocena dokonywana jest przez Osobę odpowiedzialną, w porozumieniu z IOD oraz przy wsparciu prawnym.

Uproszczona ocena dokonywana jest z wykorzystaniem narzędzia (formularza) zawartego w załączniku A do Polityki lub w inny sposób, określony przez Osobę odpowiedzialną.

Uproszczona ocena dokonywana jest:

w przypadku Procesów przetwarzania danych osobowych istniejących w dniu przyjęcia Polityki – w terminie do 6 miesięcy od wejścia w życie polityki.

w przypadku Nowych Inicjatyw – na etapie projektowania w ramach pracy nad Nową Inicjatywą.

OCENA SKUTKÓW PRZETWARZANIA DLA OCHRONY DANYCH (DPIA)

Przedmiotem DPIA są Procesy przetwarzania danych osobowych oraz Nowe Inicjatywy, o ile podlegają wymogowi przeprowadzenia Oceny DPIA na podstawie dokonanej Preewaluacji.

Celem Oceny DPIA jest zapewnienie przez Administratora przestrzegania przepisów RODO oraz właściwego zarządzania ryzykiem, a w szczególności umożliwienie wykazania (zgodnie z zasadą rozliczalności) przestrzegania tych przepisów, przy uwzględnieniu m.in. ryzyka naruszenia praw lub wolności osób fizycznych o różnym prawdopodobieństwie i różnej istotności zagrożenia.

Ocena DPIA składa się z następujących elementów:

szczegółowego opisu operacji przetwarzania oraz środków zabezpieczenia danych, który przygotowywany jest w załączniku A na etapie Privacy by Design;

oceny, jakie środki (organizacyjne i techniczne) są niezbędne oraz proporcjonalne dla zapewnienia odpowiedniego stopnia ochrony danych osobowych, w szczególności

w celu zapewnienia realizacji podstawowych zasad przetwarzania danych oraz zachowania praw osób, których dane dotyczą;

szczegółowej oceny stopnia ryzyka wynikającego z przetwarzania danych osobowych w Nowej Inicjatywie lub Procesie oraz doboru adekwatnych środków (organizacyjnych, fizycznych i technicznych) mających na celu ograniczenie ryzyka.

Ocena DPIA dokonywana jest przez Osobę odpowiedzialną, w porozumieniu z IOD oraz przy wsparciu prawnym.

Ocena DPIA dokonywana jest z wykorzystaniem narzędzia (formularza) zawartego w załączniku B oraz zgodnie z instrukcją stanowiącą załącznik C do Polityki.

Ocena DPIA dokonywana jest:

w przypadku Procesów przetwarzania danych osobowych istniejących w dniu przyjęcia Polityki – w terminie do 6 miesięcy od wejścia w życie polityki.

w przypadku Nowych Inicjatyw – na etapie projektowania w ramach pracy nad Nową Inicjatywą.

POSTANOWIENIA KOŃCOWE

Wszelkie czynności realizowane na podstawie Polityki, w szczególności podejmowane decyzje i wydawane opinie lub prowadzone konsultacje, są dokumentowane w formie pisemnej lub elektronicznej, w szczególności w formie odpowiednio uzupełnionych formularzy. Wyniki wszelkich prac dokonywanych w ramach Polityki (w szczególności uzupełnione formularze) przechowuje IOD.

Polityka wchodzi w życie z dniem ogłoszenia.

Integralną część dokumentu stanowią załączniki:

Załącznik A – Formularz Analizy Ryzyka;

Załącznik B – Formularz Oceny DPIA;

Załącznik C – Instrukcja wypełniania formularza Oceny DPIA.

GMINA MIEDŹNO

PROCEDURA OCENY I NOTYFIKACJI NARUSZEŃ OCHRONY DANYCH OSOBOWYCH

1) METRYKA DOKUMENTU	
STATUS	Dokument wewnętrzny

WERSJA	1.0
DATA	31.10.2023 r.
LICZBA STRON	183
CEL DOKUMENTU	Niniejszy dokument opisuje zasady oceny i notyfikacji naruszeń ochrony danych osobowych.
SPIS TREŚCI	1. Definicje ..... 107 2. Zasady ogólne ..... 108 3. Postępowanie w sytuacji podejrzenia Naruszenia ..... 108 4. Postępowanie w sytuacji stwierdzenia Naruszenia ..... 109 5. Rejestr Naruszeń ochrony Danych osobowych ..... 110 6. Postanowienia końcowe ..... 110 Załącznik A – Instrukcja dla pracowników / współpracowników w zakresie podstaw rozpoznawania naruszeń ochrony danych osobowych ..... 112 Załącznik B – Rejestr naruszeń ochrony danych ..... 114 Załącznik C – Szablon zgłoszenia naruszenia organowi nadzorczemu ..... 116 Załącznik D – Wzór informacji dla osoby, której dane dotyczą, o naruszeniu ochrony danych osobowych ..... 118 Załącznik E – Metodologia oceny powagi naruszenia praw lub wolności osoby fizycznej 119

15. DEFINICJE

15.1. **Administrator – Gmina Miedźno** z siedzibą w Miedźnie ul. Ułańska 25, 42-120 Miedźno, NIP: 5742055080

15.2. **Dane szczególnych kategorii** – dane ujawniające pochodzenie rasowe lub etniczne, poglądy polityczne, przekonania religijne lub światopoglądowe, przynależność do związków zawodowych oraz dane genetyczne, dane biometryczne przetwarzane w celu jednoznacznego zidentyfikowania osoby fizycznej lub dane dotyczące zdrowia, seksualności czy orientacji seksualnej osoby fizycznej.

15.3. **IOD** – Inspektor Ochrony Danych, wyznaczony przez Gminę, nadzorujący przestrzeganie przepisów o ochronie danych osobowych w Gminie, wykonujący zadania określone w art. 39 RODO. W przypadku braku powołania w Gminie IOD, zadania związane z zapewnieniem zgodności przetwarzania danych osobowych w Gminie z obowiązującym prawem wykonuje **Koordynator ds. ochrony danych osobowych** (**KODO**).

15.4. **Naruszenie** lub **Naruszenie ochrony Danych osobowych** – naruszenie bezpieczeństwa prowadzące do przypadkowego lub niezgodnego z prawem zniszczenia, utracenia, zmodyfikowania, nieuprawnionego ujawnienia lub nieuprawnionego dostępu do Danych osobowych przesyłanych, przechowywanych lub w inny sposób przetwarzanych przez Administratora.

15.5. **Organ nadzorczy** – Prezes Urzędu Ochrony Danych osobowych lub ewentualnie właściwy organ nadzorczy w zakresie Danych osobowych wyznaczony przez inne państwo członkowskie Unii Europejskiej.

15.6. **Podmiot danych** – osoba fizyczna, której dotyczą Dane osobowe przetwarzane przez Administratora.

15.7. **Pracownik** – osoba fizyczna zatrudniona przez Administratora na podstawie umowy o pracę.

15.8. **Rejestr** – Rejestr naruszeń ochrony Danych osobowych.

15.9. **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.

15.10. **Współpracownik** – osoba fizyczna świadcząca na rzecz Administratora usługi na podstawie umowy cywilnoprawnej (np. umowa zlecenie, umowa o dzieło).

16. ZASADY OGÓLNE

2.1. Procedura określa ogólne zasady oceny, ewidencji i notyfikacji Naruszeń ochrony Danych osobowych zgodnie z RODO.

2.2. Jeśli procedura nie stanowi inaczej, zadania opisane w Procedurze realizuje w imieniu Administratora IOD.

2.3. Administrator dokłada starań, aby Pracownicy i Współpracownicy mieli wiedzę niezbędną do prawidłowego rozpoznawania sytuacji mogących stanowić Naruszenie ochrony Danych osobowych. W szczególności Administrator zapewnia, że każdy Pracownik i Współpracownik został zapoznany z pracowniczą instrukcją postępowania na wypadek sytuacji mogących stanowić Naruszenie, stanowiącą załącznik A do Procedury.

2.4. Administrator zapewnia, że podmioty przetwarzające dane na zlecenie Administratora zobowiązały się do informowania Administratora o Naruszeniach dotyczących powierzonych im do przetwarzania Danych osobowych, a także zobowiązały się do współpracy przy wyjaśnianiu okoliczności Naruszenia, w szczególności do udzielania na żądanie Administratora informacji dotyczących Naruszenia.

2.5. W przypadku Naruszenia po stronie podmiotu przetwarzającego, któremu Administrator powierzył przetwarzanie Danych osobowych, Procedurę stosuje się odpowiednio.

17. POSTĘPOWANIE W SYTUACJI PODEJRZENIA NARUSZENIA

3.1. Każdy Pracownik i Współpracownik jest zobowiązany do zgłaszania bezpośredniemu przełożonemu lub bezpośrednio IOD sytuacji, które mogą stanowić Naruszenie ochrony Danych osobowych. Szczegółowe wytyczne w tym zakresie są zawarte w załączniku A do Procedury.

3.2. Każdy przypadek mogący stanowić Naruszenie ochrony danych powinien zostać natychmiast zgłoszony IOD. Jeśli natychmiastowe zgłoszenie nie jest możliwe, Pracownik/Współpracownik powinien podjąć działania zmierzające do zgłoszenia Naruszenia w terminie nie dłuższym niż 4 h od czasu zaobserwowania sytuacji mogącej stanowić Naruszenie.

3.3. IOD prowadzi postępowanie wyjaśniające w każdej zgłoszonej sytuacji, w której Naruszenia ochrony danych nie można wykluczyć. Oceny, czy Naruszenia nie można wykluczyć, dokonuje IOD na podstawie informacji uzyskanych od zgłaszającego. Postępowanie wyjaśniające należy rozpocząć niezwłocznie po otrzymaniu zgłoszenia.

3.4. Postępowanie wyjaśniające polega na zebraniu informacji niezbędnych do wypełnienia Rejestru oraz zmierza do określenia na podstawie tych informacji, czy doszło do Naruszenia (stwierdzenie Naruszenia). Stwierdzenie Naruszenia następuje w chwili, gdy na podstawie zebranych informacji można racjonalnie przyjąć, że do Naruszenia doszło lub z dużym prawdopodobieństwem doszło.

3.5. W celu zebrania potrzebnych informacji IOD może komunikować się (bezpośrednio oraz za pomocą środków porozumiewania się na odległość) z Pracownikami i osobami

trzecimi, uzyskiwać dostęp do pomieszczeń, urządzeń i schowków, przy czym niedopuszczalna jest ingerencja w prywatność jakiejkolwiek osoby.

3.6. Działania podejmowane w ramach postępowania wyjaśniającego są dokumentowane w postaci notatki. Notatki oraz zgromadzone materiały, dokumenty etc. są przechowywane przez czas niezbędny do wyjaśnienia okoliczności Naruszenia, co obejmuje także ewentualne czynności podejmowane przez Organ nadzorczy lub sąd (do czasu ostatecznych rozstrzygnięć), a następnie jeszcze przez 6 miesięcy.

18. POSTĘPOWANIE W SYTUACJI STWIERDZENIA NARUSZENIA

18.1. W przypadku stwierdzenia Naruszenia (niezależnie od jego ostatecznej kwalifikacji) należy odnotować datę i godzinę, w której doszło do stwierdzenia Naruszenia.

18.2. Dzięki informacjom uzyskanym w toku postępowania wyjaśniającego Administrator ocenia:

18.2.1. czy jest prawdopodobne, że stwierdzone Naruszenie skutkuje ryzykiem naruszenia praw lub wolności osób fizycznych;

18.2.2. jaka jest waga Naruszenia praw lub wolności osób fizycznych.

18.3. W celu dokonania oceny Naruszenia, o której mowa w punkcie 18.2 powyżej, stosuje się metodologię opisaną w załączniku E do Procedury.

18.4. W przypadku ustalenia, iż **jest mało prawdopodobne, że Naruszenie skutkuje ryzykiem** naruszenia praw lub wolności osób fizycznych:

18.4.1. Administrator nie jest zobowiązany do podejmowania żadnych działań, z zastrzeżeniem Rozdziału 19 Procedury;

18.4.2. w razie stwierdzenia takiej potrzeby Administrator wdraża odpowiednie środki zaradcze zapobiegające Naruszeniom.

18.5. W przypadku ustalenia, iż **jest prawdopodobne, że Naruszenie skutkuje ryzykiem** naruszenia praw lub wolności osób fizycznych, zgodnie ze szczegółowymi wytycznymi zawartymi w punkcie 2.4 załącznika E do Procedury:

18.5.1. Administrator dokonuje zgłoszenia Naruszenia Organowi nadzorczemu, na formularzu zgłoszenia udostępnionym przez Organ nadzorczy. Jeżeli taki formularz nie został udostępniony, należy dokonać zgłoszenia zgodnie z wzorem stanowiącym załącznik C do Procedury;

18.5.2. o ile przepisy nie stanowią inaczej i Organ nadzorczy nie określił innego trybu zgłaszania Naruszeń, Administrator dokonuje zgłoszenia, przesyłając skan zgłoszenia na adres Organu nadzorczego oraz oryginał listem poleconym na adres Organu nadzorczego;

18.5.3. zgłoszenia należy dokonać niezwłocznie, nie później niż w ciągu 72 godzin od stwierdzenia Naruszenia. Jeśli przekazanie kompletu wymaganych informacji nie jest możliwe w tym czasie, należy przesłać część informacji, wskazując jednocześnie rodzaj informacji, które zostaną uzupełnione, i termin tego

uzupełnienia. W przypadku uchybienia terminowi należy dokonać zgłoszenia, wyjaśniając powody niedotrzymania terminu.

18.6. W przypadku ustalenia, że **Naruszenie może powodować wysokie ryzyko naruszenia praw lub wolności osób fizycznych**, zgodnie ze szczegółowymi wytycznymi zawartymi w punkcie 2.4 załącznika E do Procedury Administrator dokonuje zgłoszenia, o którym mowa w punkcie 18.5 Procedury, a ponadto niezwłocznie informuje o Naruszeniu Podmioty danych, których dotyczy Naruszenie. Administrator informuje Podmioty danych o Naruszeniu za pośrednictwem e-maila lub innego środka komunikacji pozwalającego dostarczyć informację w najkrótszym możliwym czasie. Wzór informacji dla Podmiotu danych znajduje się w załączniku D do Procedury. Jeśli wyczerpujące określenie Podmiotów danych, których dotyczy Naruszenie, nie jest możliwe, Administrator zamieszcza informację na swojej stronie internetowej lub przekazuje ją w inny sposób, który maksymalizuje szansę dotarcia informacji do odpowiednich Podmiotów danych.

19. REJESTR NARUSZEŃ OCHRONY DANYCH OSOBOWYCH

19.1. Administrator prowadzi Rejestr naruszeń ochrony Danych osobowych w formie elektronicznej, według wzoru stanowiącego załącznik B do Procedury.

19.2. Każdy przypadek Naruszenia ochrony Danych osobowych powinien zostać wpisany do Rejestru i opisany zgodnie z systematyką Rejestru. W każdym przypadku Naruszenia, w którym Administrator nie dokonuje zgłoszenia do Organu nadzorczego lub nie informuje Podmiotów danych, których dotyczy Naruszenie, należy w Rejestrze dokładnie opisać powody takiej decyzji.

19.3. Rejestr stanowi tajemnicę przedsiębiorstwa Administratora. Dostęp do informacji zawartych w Rejestrze jest ograniczony do Inspektora Ochrony Danych lub wyznaczonych Pracowników czy Współpracowników. Rejestr jest ujawniany Organowi nadzorczemu na jego żądanie.

19.4. Nie rzadziej niż jeden raz w roku Administrator analizuje wpisy w Rejestrze w celu:

19.4.1. oceny skuteczności środków technicznych i organizacyjnych zabezpieczenia Danych osobowych;

19.4.2. zidentyfikowania powtarzających się Naruszeń;

19.4.3. zaplanowania, w zależności od wyników oceny, działań zmierzających do poprawy środków organizacyjnych i technicznych zabezpieczenia Danych osobowych.

20. POSTANOWIENIA KOŃCOWE

20.1. Procedura jest aktualizowana przez Administratora, z zastrzeżeniem pkt 20.2, w zależności od potrzeb. IOD jest uprawniony do składania wniosku o aktualizację Procedury.

20.2. IOD jest uprawniony do samodzielnej zmiany załączników A, C i D do Procedury. O każdej takiej zmianie IOD zawiadamia Administratora, a o zmianie załącznika A oraz D – także Pracowników lub Współpracowników Administratora.

20.3. Procedura wchodzi w życie z dniem określonym w zarządzeniu Wójta Gminy Miedźno.

20.4. Integralną część Procedury stanowią jej załączniki:

20.4.1. Załącznik A – Instrukcja dla pracowników / współpracowników w zakresie podstaw rozpoznawania naruszeń ochrony danych osobowych;

20.4.2. Załącznik B – Rejestr naruszeń ochrony danych;

20.4.3. Załącznik C – Szablon zgłoszenia naruszenia organowi nadzorczemu;

20.4.4. Załącznik D – Wzór informacji dla osoby, której dane dotyczą, o naruszeniu ochrony danych osobowych;

20.4.5. Załącznik E – Metodologia oceny powagi naruszenia praw lub wolności osoby fizycznej.

Załącznik A – Instrukcja dla pracowników / współpracowników w zakresie podstaw rozpoznawania naruszeń ochrony danych osobowych

1. Pamiętaj, że naruszeniem ochrony danych jest nie tylko duży wyciek danych, atak hakerski czy włamanie do biura. Z naruszeniem ochrony danych możesz się zetknąć przy wykonywaniu standardowych czynności w ramach swojej pracy. Takie sytuacje często są wynikiem błędu ludzkiego (np. błędne zaadresowanie korespondencji), nieprawidłowego działania urządzenia (np. automatyczne, przedwczesne wykasowanie części bazy danych), zdarzenia losowego (takiego jak pożar), a tylko w skrajnych przypadkach – rażącego niedbalstwa lub umyślnego działania (np. kradzież bazy danych).

2. Zwróć uwagę, że sytuacje naruszenia ochrony danych generalnie mogą polegać na:

nieuprawnionym zniszczeniu danych osobowych (np. skasowaniu),
utracie danych osobowych (np. kradzieży laptopa służbowego lub zgubieniu dysku przenośnego),
nieuprawnionym zmodyfikowaniu danych osobowych (np. nadpisaniu, pomieszaniu),
nieuprawnionym ujawnieniu danych osobowych (np. przesłaniu na błędny adres),
nieuprawnionym uzyskaniu dostępu do danych osobowych (np. kradzieży bazy danych).

3. Twoją czujność powinny wzbudzić:

nieznanego pochodzenia uszkodzenia fizyczne stacji roboczych, drzwi, zamków, skrytek,
niestandardowe komunikaty wyświetlane na ekranie urządzeń,
znaczne spowolnienie działania systemu informatycznego,
błędy w funkcjonowaniu systemu informatycznego (brak możliwości logowania, niedostępność funkcji, modułów lub aplikacji systemowych),
przedłużający się brak możliwości odnalezienia określonych dokumentów, nośników danych lub urządzeń służących do przetwarzania danych (np. komputera, telefonu)

– te sytuacje nie zawsze świadczą o wystąpieniu naruszenia, ale należy je wyjaśnić.

4. Pamiętaj, że mamy obowiązek podjęcia określonych prawem działań w sytuacji stwierdzenia naruszenia ochrony danych, dlatego Twoja współpraca, szczególnie wykonywanie obowiązków opisanych poniżej, ma kluczowe znaczenie i może nas uchronić przed karami finansowymi.

5. Pamiętaj, że Twoim obowiązkiem jest poinformowanie bezpośredniego przełożonego o sytuacji, która w Twojej ocenie może stanowić naruszenie ochrony danych osobowych. Powinieneś to zrobić natychmiast po zaobserwowaniu lub uzyskaniu wiedzy o takiej sytuacji. Powinieneś także podjąć rozsądne działania zmierzające do ograniczenia skutków naruszenia, a w następnej kolejności – odpowiednio do okoliczności – zabezpieczyć ślady mogące wskazywać na naruszenie (np. zrobić zrzut ekranu, zabezpieczyć pomieszczenie).

6. Pamiętaj, że jeśli naruszenie jest wynikiem Twojego błędu lub niedopatrzenia, to zgłaszając nam tę sytuację, działasz wyłącznie na swoją korzyść.

7. Pamiętaj, że informując o możliwym naruszeniu ochrony danych osobowych, dajesz nam szansę na odpowiednią reakcję i zapobiegnięcie negatywnym konsekwencjom naruszenia.

W tym miejscu należy opisać typowe sytuacje wymagające oceny z punktu widzenia Naruszenia ochrony Danych osobowych. Opis powinien uwzględniać specyfikę działalności Administratora, w szczególności wskazywać powtarzalne sytuacje, które z mniejszą lub większą regularnością występują u danego Administratora i powinny być zgłaszane zgodnie z Procedurą, np. w przypadku działalności kurierskiej – zagubienie paczki, w przypadku działalności B2C – wysłanie monitu wzywającego do zapłaty należności na niewłaściwy adres.

Także w tym miejscu należy opisać ścieżkę raportowania Naruszeń z uwzględnieniem struktury Administratora i specyfiki jego działalności.

Instrukcja powinna być zbiorem prostych i praktycznych wskazówek opisujących sposób zachowania się Pracownika / Współpracownika w sytuacji, w której podejrzewa, że mogło dojść do Naruszenia ochrony Danych osobowych.

Załącznik B – Rejestr naruszeń ochrony danych

POLE INFORMACYJNE	WYJAŚNIENIA
Opis zdarzenia	Należy opisać okoliczności zdarzenia stanowiącego naruszenie ochrony danych, w tym w miarę możliwości wskazać kategorie i przybliżoną liczbę osób, których dane dotyczą, oraz kategorie i przybliżoną liczbę wpisów (rekordów) danych osobowych, których dotyczy naruszenie.
Dane kontaktowe	Należy wskazać dane kontaktowe osoby, która może udzielić szczegółowych informacji dotyczących naruszenia, w tym w szczególności Inspektora Danych Osobowych Administratora, a w przypadku, gdy dane osobowe zostały powierzone podmiotowi trzeciemu – dane kontaktowe tego podmiotu i jego Inspektora Ochrony Danych.
Chwila stwierdzenia naruszenia	Należy określić chwilę stwierdzenia przez Administratora naruszenia bezpieczeństwa danych tak dokładnie, jak to możliwe (z dokładnością co do godziny).
Ocena naruszenia	Należy wskazać co najmniej wynik oceny naruszenia, a także przyjęte wartości dla czynników KP, I oraz ON.
Zgłoszenie naruszenia organowi nadzorczemu	Należy wskazać: a) imię i nazwisko osoby dokonującej zgłoszenia; b) chwilę dokonania zgłoszenia (z dokładnością co do godziny). W przypadku, gdy zgłoszenie nie zostało dokonane, należy wpisać: n/d.
Przyczyny niezgłoszenia naruszenia organowi nadzorczemu	Należy uzupełnić tylko w przypadku, gdy naruszenie nie zostało zgłoszone. Należy określić przyczyny niezgłoszenia naruszenia uzasadniające małe prawdopodobieństwo, by naruszenie to skutkowało ryzykiem naruszenia praw lub wolności osób fizycznych.
Zawiadomienie osoby, której dane dotyczą	Należy wskazać: a) kiedy zostało zrealizowane zawiadomienie; b) sposób, w jaki osoby, których dane dotyczą, zostały zawiadomione o naruszeniu, w tym poprzez wskazanie, że został wydany publiczny komunikat dotyczący naruszenia. W przypadku, gdy osoby, których dane dotyczą, nie były informowane o naruszeniu, należy wpisać: n/d.
Przyczyny zaniechania zawiadomienia o naruszeniu osób, których dane dotyczą	Należy uzupełnić tylko w przypadku, gdy osoby, których dane dotyczą, nie zostały zawiadomione o naruszeniu. Uzasadnienie powinno wskazywać:

POLE INFORMACYJNE	WYJAŚNIENIA
	a) że naruszenie nie może powodować wysokiego ryzyka naruszenia praw i wolności osób fizycznych oraz przyczyny takiego stanowiska ALBO b) w przypadku, gdy naruszenie może powodować wysokie ryzyko naruszenia praw i wolności osób fizycznych, wskazanie, że Administrator wdrożył odpowiednie techniczne i organizacyjne środki ochrony oraz zastosował je do danych, których dotyczy naruszenie, zastosował środki eliminujące prawdopodobieństwo wysokiego ryzyka, o którym mowa powyżej, lub też – że zawiadomienie zostało zastąpione publicznym komunikatem, ponieważ zawiadomienie osób, których dane dotyczą, wymagałoby niewspółmiernie dużego wysiłku.
Skutki naruszenia	Należy opisać faktycznie zaistniałe skutki naruszenia bezpieczeństwa ochrony danych, w tym: a) skutki dla praw i wolności podmiotów danych; b) skutki dla Administratora; c) skutki dla osób trzecich.
Podjęte działania zaradcze	Należy szczegółowo opisać działania podjęte przez Administratora w celu usunięcia skutków naruszenia oraz zminimalizowania ryzyka powtórzenia się naruszenia w przyszłości.
Dane wprowadził/a	Imię i nazwisko osoby, która dokonała wpisu w rejestrze.
Data wprowadzenia informacji do rejestru	Data (z dokładnością do dnia i godziny).
Dane zmienił/a	Imię i nazwisko osoby, która dokonała zmiany wpisu w rejestrze.
Data zmiany informacji w rejestrze	Data (z dokładnością do dnia i godziny).
Treść zmiany	Informacja, co zostało zmienione i w jaki sposób.
Powód zmiany	Przyczyna, dla której zmieniono treść informacji wprowadzonej pierwotnie do rejestru.

Załącznik C – Szablon zgłoszenia naruszenia organowi nadzorczemu

2) LP.	3) PYTANIE	4) ODPOWIEDŹ
Oznaczenie podmiotu zgłaszającego naruszenie i osoby kontaktowej		
1.	Nazwa i siedziba Administratora danych zgłaszającego naruszenie	
2.	Imię, nazwisko, adres e-mail, numer telefonu, adres pocztowy, stanowisko służbowe osoby kontaktowej po stronie Administratora danych (np. Inspektora Ochrony Danych, jeśli został wyznaczony)	
3.	Czy Administrator zamierza uzupełnić zgłoszenie naruszenia o dodatkowe informacje? Jeśli tak, należy wskazać, w jakim terminie i jakiego rodzaju informacje zostaną uzupełnione	
Opis naruszenia		
4.	Nazwa i rola podmiotu, u którego doszło do naruszenia – administrator danych / procesor (należy wskazać rolę)	
5.	Opis naruszenia (należy podać możliwie jak najbardziej szczegółowy opis naruszenia i jego okoliczności)	
6.	Data wykrycia naruszenia oraz czas, przez jaki naruszenie miało miejsce, o ile naruszenie miało charakter ciągły	
7.	W jaki sposób Administrator dowiedział się o naruszeniu?	
8.	Jeśli od stwierdzenia naruszenia do zgłoszenia go organowi nadzorczemu upłynęło więcej niż 72 godziny, należy opisać	

2) LP.	3) PYTANIE	4) ODPOWIEDŹ
	powody opóźnienia w raportowaniu	
9.	Jakie są prawdopodobne przyczyny naruszenia?	
10.	Jakie są potencjalne konsekwencje i niekorzystne skutki dla osób, których naruszenie dotyczy?	
Zakres danych objętych naruszeniem		
11.	Jakich kategorii osób dotyczy naruszenie?	
12.	Ilu (w przybliżeniu) osób dotknęło naruszenie?	
13.	Jakich danych osobowych dotyczyło naruszenie? (należy wskazać możliwie szczegółowo przynajmniej kategorie danych; jeśli naruszenie dotyczyło danych szczególnych kategorii lub danych o karalności, należy ten fakt wskazać)	
14.	Jaka jest skala naruszenia? (należy wskazać, ilu w przybliżeniu wpisów danych / rekordów dotyczy naruszenie)	
Opis podjętych i planowanych działań		
15.	Jakie kroki podjął lub zamierza podjąć Administrator w celu minimalizacji niekorzystnych skutków naruszenia dla osób, których ono dotknęło?	
16.	Jakie kroki podjął lub zamierza podjąć Administrator, aby zapobiec analogicznym do naruszenia zdarzeniom w przyszłości?	

Załącznik D – Wzór informacji dla osoby, której dane dotyczą, o naruszeniu ochrony danych osobowych

[*Miejsce sporządzenia*], [*DD/MM/RRRR*]

[*Oznaczenie Administratora*]
[*Adres Administratora*]

Szanowny Panie / Szanowna Pani,

Informujemy, że zidentyfikowaliśmy naruszenie ochrony danych osobowych, które dotyczy Pani / Pana danych obejmujących [*rodzaj lub kategorie danych objętych naruszeniem*].

Naruszenie polega na [*syntetyczny opis naruszenia*].

Skutkiem naruszenia dla Pani / Pana może być [*wskazanie możliwych ryzyk wynikających z naruszenia dla podmiotów danych*].

Jest nam przykro z powodu zaistniałej sytuacji. Zapewniamy, że podejmujemy wszelkie możliwe działania w celu zminimalizowania ryzyka i ewentualnych negatywnych konsekwencji naruszenia dla Pani / Pana sytuacji. W szczególności [*ogólny opis podjętych lub zaplanowanych działań naprawczych*].

W zaistniałej sytuacji rekomendujemy [*opis rekomendowanych działań, np. zmiana hasła w innych miejscach, w których było wykorzystywane*].

Dodatkowe informacje może Pani / Pan uzyskać, kontaktując się z nami [*dane kontaktowe, w tym numer telefonu lub adres e-mail IOD lub osoby wyznaczonej jako osoba kontaktowa w związku z naruszeniem*].

[*podpis*]

Załącznik E – Metodologia oceny powagi naruszenia praw lub wolności osoby fizycznej

1. KRYTERIA OCENY NARUSZENIA

1.1. Głównymi kryteriami, które należy uwzględnić przy ocenie naruszenia ochrony praw lub wolności osoby fizycznej, są:

1.1.1. **kontekst przetwarzania danych** – kryterium odnosi się do rodzaju danych będących przedmiotem naruszenia wraz z szeregiem pomniejszych czynników powiązanych z ogólnym kontekstem przetwarzania danych.

1.1.2. **łatwość identyfikacji** – kryterium dotyczy łatwości określenia tożsamości osób fizycznych, którą umożliwiają dane będące przedmiotem naruszenia.

1.1.3. **okoliczności naruszenia** – kryterium odnosi się do okoliczności powiązanych z zaistniałym typem naruszenia (w tym jego umyślności / nieumyślności).

2. OBLICZANIE OCENY NARUSZENIA

2.1. Ocena Naruszenia wyrażana jest wartością liczbową, przy uwzględnieniu kryteriów wskazanych w pkt 1.1 oraz przy założeniu, że:

2.1.1. **kontekst przetwarzania danych (KP)** jest najważniejszym kryterium i służy ocenie krytyczności danych będących przedmiotem naruszenia. Metodę ewaluacji tego kryterium opisano w pkt 3 poniżej;

2.1.2. **łatwość identyfikacji (I)** stanowi element korygujący współczynnik kontekstu przetwarzania danych. Metodę oceny tego kryterium opisano w pkt 4 poniżej.

2.1.3. **okoliczności naruszenia (ON)** jest kryterium dostosowującym wstępną ocenę punktową. Sposób oszacowania kryterium opisano w pkt 5 poniżej.

2.2. Ocenę Naruszenia (**P**) stanowi iloczyn kryterium kontekstu przetwarzania danych (**KP**) oraz łatwości identyfikacji (**I**), powiększony o współczynnik okoliczności naruszenia (**ON**), zgodnie z następującym wzorem:

$$P = KP \times I + ON$$

2.3. Administrator może zmodyfikować uzyskaną wartość oceny Naruszenia (P) poprzez jej zwiększenie lub zmniejszenie, przy uwzględnieniu następujących czynników:

2.3.1. liczba podmiotów danych dotkniętych naruszeniem przekracza liczbę stu osób – im większy zakres podmiotowy naruszenia, tym wyższy poziom naruszenia;

2.3.2. nieczytelność danych dotkniętych naruszeniem (np. fakt, że naruszeniem danych objęte zostały wyłącznie dane osobowe, które zostały zaszyfrowane);

2.3.3. inne czynniki mające wpływ na wagę naruszenia lub prawdopodobieństwo wystąpienia ryzyka naruszenia praw lub wolności osób fizycznych.

2.4. Uzyskaną ostatecznie wartość P należy przypisać do jednego z czterech poziomów Naruszenia (**PN**):

5) POZIOM NARUSZENIA (PN)			
OCENA	**NAZWA POZIOMU NARUSZENIA**	**WAGA NARUSZENIA PRAW LUB WOLNOŚCI OSÓB FIZYCZNYCH**	**WYMAGANE DZIAŁANIA**
PN < 2	**NISKI**	• Podmioty danych nie ucierpią z powodu naruszenia lub spotkają je drobne niedogodności, którym można sprostać bez trudności (np. czas wymagany na ponowne wpisanie danych, niepokój, rozdrażnienie itp.).	1. Wpisanie Naruszenia do Rejestru; 2. w razie potrzeby podjęcie działań zaradczych – zgodnie z pkt 18.4 Procedury.
2 ≤ PN < 3	**ŚREDNI**	• Podmioty danych mogą napotkać znaczące niedogodności, którym można sprostać pomimo trudności (np. dodatkowe koszty, odmowa dostępu do usług biznesowych, obawa, brak zrozumienia, stres, drobne dolegliwości zdrowotne).	3. Wpisanie Naruszenia do Rejestru; 4. podjęcie działań zaradczych; 5. zawiadomienie o Naruszeniu Organu nadzorczego – zgodnie z pkt 18.5 Procedury.
3 ≤ PN < 4	**WYSOKI**	• Podmioty danych mogą ponieść poważne konsekwencje, które powinny móc pokonać pomimo poważnych trudności (np. sprzeniewierzenie środków finansowych, wpisanie na czarną listę banku, uszkodzenie własności, utrata pracy, wezwanie do sądu, pogorszenie stanu zdrowia). •	6. Wpisanie Naruszenia do Rejestru; 7. podjęcie działań zaradczych; 8. zawiadomienie o Naruszeniu Organu nadzorczego; 9. zawiadomienie o Naruszeniu Podmiotów danych – zgodnie z pkt 18.6 Procedury. •
4 ≤ PN	**BARDZO WYSOKI**	• Podmioty danych mogą ponieść poważne lub nawet nieodwracalne konsekwencje, które mogą być niemożliwe do pokonania (np. problemy finansowe takie jak znaczne zadłużenie lub niezdolność do pracy, długotrwałe problemy psychiczne lub fizyczne, śmierć).	

3. OKREŚLANIE WARTOŚCI PUNKTOWEJ DLA CZYNNIKA – KONTEKST PRZETWARZANIA DANYCH (KP)

3.1. Wartość punktowa kontekstu przetwarzania (KP) może przyjąć wartości od 1 do 4.

3.2. Dla określenia wartości punktowej kontekstu przetwarzania danych (KP) należy podjąć następujące kroki:

3.2.1. określić rodzaj danych osobowych będących przedmiotem naruszenia poprzez przypisanie ich do jednej z następujących kategorii:

dane podstawowe – np. imię i nazwisko; adres zamieszkania / korespondencyjny; adres IP; numer telefonu; informacje o wykształceniu i doświadczeniu zawodowym itp.;

dane behawioralne – np. dane dotyczące lokalizacji; dane o ruchu; dane dotyczące przyzwyczajeń i preferencji itp.;

dane finansowe – np. wysokość wynagrodzenia; informacja o korzystaniu z usług banku; numer rachunku bankowego; informacja o dokonywanych transakcjach finansowych itp. (także dane dotyczące korzystania ze wsparcia opieki społecznej);

dane wrażliwe – wszelkie dane szczególnej kategorii (np. dane dotyczące stanu zdrowia, orientacji seksualnej, poglądów politycznych);

3.2.2. przypisać do rodzajów danych podstawową wartość punktową kontekstu przetwarzania (**PWP**) w następujący sposób:

dla naruszenia dotyczącego danych podstawowych: PWP = 1;

dla naruszenia dotyczącego danych behawioralnych: PWP = 2;

dla naruszenia dotyczącego danych finansowych: PWP = 3;

dla naruszenia dotyczącego danych wrażliwych: PWP = 4;

dla naruszenia dotyczącego danych dostępowych (uwierzytelniających) należy przypisać PWP w zależności od danych, do których umożliwiają one dostęp;

3.2.3. jeżeli dane dają się przyporządkować do więcej niż jednej kategorii, kroki należy przeprowadzić dla każdej z kategorii. W takich przypadkach wartością KP jest najwyższy osiągnięty wynik.

3.3. Ostateczna wartość punktowa kontekstu przetwarzania (**KP**) może być wyższa lub niższa od PWP w zależności od wystąpienia czynników podwyższających lub obniżających ryzyko związane z naruszeniem. W celu ustalenia KP Administrator może odpowiednio zwiększyć lub zmniejszyć uzyskaną PWP, w szczególności w zależności od wystąpienia następujących czynników:

3.3.1. **ilość danych –** ten czynnik powinien zwiększyć przypisaną podstawową wartość punktową, przy czym ilość danych powinna być rozważana zarówno w aspekcie czasowym (dane tego samego rodzaju, gromadzone przez pewien okres), jak i treści (naruszenie dotyczące kompletu danych dotyczących danej osoby fizycznej, zgromadzonych przez Administratora);

3.3.2. **szczególne cechy osób, których dotyczy naruszenie –** przypisaną podstawową wartość punktową należy zwiększyć w przypadku, gdy osoby te należą do grupy społecznej o szczególnych potrzebach (np. osoby nieletnie, niepełnosprawne);

3.3.3. **nieprawidłowość / niedokładność danych –** przypisaną podstawową wartość punktową należy zmniejszyć, jeżeli dane są nieprawidłowe, nieaktualne lub niedokładne (np. ze względu na odległą datę ich zebrania lub zawartość);

3.3.4. **dostępność publiczna (przed incydentem) –** przypisaną podstawową wartość punktową należy zmniejszyć w przypadku, gdy naruszone dane były już ogólnie dostępne przed naruszeniem lub można je łatwo zebrać lub uzyskać do nich dostęp za pośrednictwem publicznie dostępnych źródeł;

3.3.5. **charakter danych –** czynnik może doprowadzić do zmniejszenia podstawowej wartości punktowej w szczególnych przypadkach, w sytuacji, gdy dane nie ujawniają znaczących informacji dotyczących osoby fizycznej, pomimo że są danymi szczególnego rodzaju (np. zaświadczenie lekarskie potwierdzające jedynie możliwość podjęcia pracy z uwagi na ogólny stan zdrowia).

3.4. W zależności od wystąpienia powyższych czynników KP może mieć wartość niższą lub wyższą od PWP, zgodnie z poniższą tabelą:

NAZWA KATEGORII	PRZYKŁADY OKOLICZNOŚCI WPŁYWAJĄCYCH NA OSTATECZNĄ WARTÓŚĆ PUNKTOWĄ KP	KP
DANE PODSTAWOWE PWP = 1	• PWP powinna zostać podwyższona o 1 pkt w przypadku, gdy ilość danych podstawowych umożliwia profilowanie podmiotów danych lub pozwala na przyjęcie założeń dotyczących statusu ekonomicznego podmiotów danych.	• **2**
	• PWP powinna zostać podwyższona o 2 pkt np. w przypadku, gdy dane podstawowe pozwalają wyciągać wnioski o stanie zdrowia osoby, której dane dotyczą, jej preferencjach seksualnych czy poglądach politycznych.	• **3**
	• PWP powinna zostać podwyższoną o 3 pkt np. w przypadku, gdy z uwagi na cechy charakterystyczne dla osoby informacja może mieć szczególne znaczenie dla bezpieczeństwa tej osoby lub jej stanu fizycznego czy psychicznego (np. grupy szczególnie wrażliwe, dzieci).	• **4**
• **DANE BEHAWIORALNE**	• PWP powinna zostać obniżona o 1 pkt np. w przypadku, gdy charakter zbioru danych nie zapewnia istotnego wglądu	• **1**

NAZWA KATEGORII	PRZYKŁADY OKOLICZNOŚCI WPŁYWAJĄCYCH NA OSTATECZNĄ WARTÓŚĆ PUNKTOWĄ KP	KP
• **PWP = 2** • **DANE BEHAWIORALNE** • **PWP = 2**	w informacje dotyczące zachowania podmiotu danych lub dane mogą być łatwo gromadzone (niezależnie od naruszenia) za pośrednictwem publicznie dostępnych źródeł (na przykład połączenie informacji z wyszukiwarek internetowych).	
	• PWP powinna zostać podwyższona o 1 pkt np. w przypadku, gdy ilość danych behawioralnych umożliwia profilowanie podmiotów danych lub pozwala na przyjęcie założeń dotyczących statusu ekonomicznego podmiotów danych.	• **3**
	• PWP powinna zostać podwyższona o 2 pkt np. w przypadku, gdy w oparciu o dane możliwe jest stworzenie profilu osoby obejmującego jej dane wrażliwe.	• **4**
• **DANE FINANSOWE** • **PWP = 3**	• PWP powinna zostać obniżona o 2 pkt np. w przypadku, gdy charakter danych nie daje wglądu do istotnych aspektów sytuacji finansowej osoby fizycznej (np. informacja o byciu klientem konkretnego banku, bez żadnych dodatkowych informacji). •	• **1**
	• PWP powinna zostać obniżona o 1 pkt np. przypadku, gdy dane zawierają specyficzne i konkretne informacje, jednak bez ujawniania istotnych aspektów sytuacji finansowej osoby fizycznej (np. numer rachunku bankowego).	• **2**
	• PWP powinna zostać podwyższona o 1 pkt np. w sytuacji, gdy natura lub ilość danych ujawnia informacje w zakresie umożliwiającym oszustwo lub stworzenie pełnego, szczegółowego profilu finansowego osoby fizycznej.	• **4**
• **DANE SZCZEGÓLNEJ KATEGORII** • **PWP = 4**	• PWP powinna zostać obniżona o 1 pkt np. w przypadku, gdy charakter danych może prowadzić do wyciągania wniosków o wrażliwych aspektach życia osoby fizycznej, mogących skutkować dla niej szkodą (np. informacja o uczestnictwie w zgromadzeniu zwolenników określonej partii politycznej).	• **3**
	• PWP powinna zostać obniżona o 2 pkt np. w przypadku, gdy charakter danych może prowadzić do ogólnych wniosków na temat wrażliwych aspektów życia osoby fizycznej (np. informacja o posiadaniu konta w serwisie randkowym o określonym profilu).	• **2**
	• PWP powinna zostać obniżona o 3 pkt np. w przypadku, gdy charakter danych nie pozwala na ujawnianie istotnych	• **1**

NAZWA KATEGORII	PRZYKŁADY OKOLICZNOŚCI WPŁYWAJĄCYCH NA OSTATECZNĄ WARTÓŚĆ PUNKTOWĄ KP	KP
	informacji dotyczących wrażliwych aspektów życia osoby fizycznej (np. informacja o poddaniu się standardowemu badaniu krwi). •	

4. OKREŚLANIE WARTOŚCI PUNKTOWEJ DLA CZYNNIKA – ŁATWOŚĆ IDENTYFIKACJI (I)

4.1. Wartość punktowa łatwości identyfikacji (I) może przyjąć wartości od 0,25 do 1.

4.2. Łatwość identyfikacji oznacza łatwość jednoznacznego połączenia danych z określoną osobą fizyczną z punktu widzenia dowolnej osoby fizycznej mającej dostęp do danych będących przedmiotem naruszenia.

4.3. Przy dokonywaniu oceny łatwości identyfikacji należy w szczególności wziąć pod uwagę następujące czynniki:

4.3.1. łatwość identyfikacji dokonywanej w sposób pośredni lub bezpośredni;

4.3.2. wszystkie prawdopodobne środki, które mogą zostać wykorzystane do identyfikacji.

4.4. Łatwość identyfikacji może być określona na jednym z następujących poziomów:

4.4.1. poziom niski: I = 0,25;
4.4.2. poziom ograniczony: I = 0,5;
4.4.3. poziom znaczny: I = 0,75;
4.4.4. poziom maksymalny: I = 1.

4.5. Poziom niski występuje w sytuacji, gdy łatwość identyfikacji jest niewielka, co oznacza, że połączenie danych z określoną osobą jest bardzo trudne, ale w pewnych warunkach możliwe.

4.6. Poziom maksymalny oznacza, że identyfikacja jest możliwa bezpośrednio przy pomocy danych będących przedmiotem naruszenia bez konieczności prowadzenia innych badań, aby określić tożsamość danej osoby.

5. OKREŚLANIE WARTOŚCI PUNKTOWEJ DLA CZYNNIKA – OKOLICZNOŚCI NARUSZENIA (ON)

5.1. Wartość punktowa dla okoliczności naruszenia (ON) może przyjmować wartości od 0 do 0,5. Poszczególne ocenione okoliczności należy zsumować (brak maksymalnej granicy możliwej do przypisania wartości) i uwzględnić w Ocenie Naruszenia.

5.2. Okoliczności naruszenia są oceniane poprzez uwzględnienie następujących aspektów:

5.2.1. **utrata poufności** – oznacza sytuację, w której dostęp do danych uzyskują osoby nieupoważnione;

5.2.2. **utrata integralności** – oznacza sytuację, gdy pierwotne dane ulegną modyfikacji, która może mieć negatywne skutki dla podmiotu danych;

5.2.3. **utrata dostępności** – oznacza sytuację, w której brakuje dostępu do danych pomimo takiej konieczności;

5.2.4. **zamierzone działanie** – oznacza sytuację, w której naruszenie było spowodowane działaniem intencjonalnym.

5.3. Wartość punktowa dla okoliczności naruszenia (ON) przypisywana jest na następujących zasadach:

5.3.1. **utrata poufności:**

dane narażone na utratę poufności, brak okoliczności wskazujących na niezgodne z prawem przetwarzanie tych danych: ON = 0;
dane ujawnione określonej liczbie zidentyfikowanych odbiorców: ON = 0,25;
dane ujawnione nieznanej liczbie niezidentyfikowanych odbiorców: ON = 0,5;

5.3.2. **utrata integralności:**

dane zmodyfikowane, brak okoliczności wskazujących na nieprawidłowe lub bezprawne użycie danych: ON = 0;
dane zmodyfikowane, występują okoliczności wskazujące na możliwe nieprawidłowe lub bezprawne użycie danych, jednak jest możliwość odwrócenia zaistniałych skutków: ON = 0,25;
dane zmodyfikowane, występują okoliczności wskazujące na możliwe nieprawidłowe lub bezprawne użycie danych, bez możliwości odwrócenia zaistniałych skutków: ON = 0,5;

5.3.3. **utrata dostępności** – brakuje dostępu do danych pomimo takiej konieczności:

dane da się odzyskać bez trudności: ON = 0;
czasowa niedostępność danych: ON = 0,25;
dane zostały utracone i nie da się ich odzyskać: ON = 0,5;

5.3.4. **zamierzone działanie** – należy określić, czy naruszenie było spowodowane działaniem przypadkowym, czy intencjonalnym:

stwierdzona lub prawdopodobna intencja spowodowania naruszenia: ON = 0,5.

REJESTR NARUSZEŃ BEZPIECZEŃSTWA DANYCH OSOBOWYCH

				Ocena naruszenia															
Lp.	Opis zdarzenia	Dane kontaktowe	Chwila stwierdzenia naruszenia	Kontekst przetwarzania	Łatwość identyfikacji	Okoliczności naruszenia	Poziom Naruszenia	Zgłoszenie naruszenia organowi nadzorczemu	Przyczyny niezgłoszenia naruszenia organowi nadzorczemu...	Zawiadomienie osób, których dane dotyczą	Przyczyny zaniechania zawiadomienia o naruszeniu osób, których dane dotyczą	Skutki naruszenia	Podjęte działania zaradcze	Dane wprowadził/a	Data wprowadzenia informacji do	Dane zmienił/a	Data zmiany informacji w rejestrze	Treść zmiany	Powód zmiany
	Należy opisać okoliczności zdarzenia stanowiącego naruszenie ochrony danych, w tym w miarę możliwości wskazać kategorie i przybliżoną liczbę osób, których dane dotyczą, oraz kategorie i przybliżoną liczbę wpisów (rekordów) danych osobowych, których dotyczy naruszenie.	Należy wskazać dane kontaktowe osoby, która może udzielić szczegółowych informacji dotyczących naruszenia, w tym w szczególności Koordynatora Ochrony Danych Osobowych, a w przypadku, gdy dane osobowe zostały powierzone podmiotowi trzeciemu - dane kontaktowe tego podmiotu i jego Inspektora Ochrony Danych lub Koordynatora Ochrony Danych.	Należy określić chwilę stwierdzenia przez Administratora naruszenia bezpieczeństwa danych tak dokładnie, jak to możliwe (z dokładnością co do godziny).	Należy wskazać ostateczną wartość punktową przypisaną do czynnika KP, w przedziale od 1 do 4	Należy wskazać wartość punktową przypisaną do czynnika I, w przedziale od 0,25 do 1	Należy wskazać sumaryczną wartość punktową przypisaną do czynnika ON (należy uwzględnić wszystkie opisane w Metodyce okoliczności i zsumować je do wartości od 0 do 2).		Należy wskazać: a) imię i nazwisko osoby dokonującej zgłoszenia; b) chwilę dokonania zgłoszenia (z dokładnością co do godziny). W przypadku, gdy zgłoszenie nie zostało dokonane, należy wpisać: n/d	Należy uzupełnić tylko w przypadku, gdy w kolumnie I wskazano, że naruszenie nie zostało zgłoszone. Należy określić przyczyny niezgłoszenia naruszenia uzasadniające małe prawdopodobieństwo, by naruszenie to skutkowało ryzykiem naruszenia praw lub wolności osób fizycznych.	Należy wskazać: a) kiedy zostało zrealizowane zawiadomienie; b) sposób, w jaki osoby, których dane dotyczą, zostały zawiadomione o naruszeniu, w tym poprzez wskazanie, że został wydany publiczny komunikat dotyczący naruszenia. W przypadku, gdy osoby, których dane dotyczą, nie były informowane o naruszeniu, należy wpisać: n/d	Należy uzupełnić tylko w przypadku, gdy w kolumnie I wskazano, że osoby, których dane dotyczą, nie zostały zawiadomione o naruszeniu. Uzasadnienie powinno wskazywać: a) że naruszenie nie może powodować wysokiego ryzyka naruszenia praw i wolności osób fizycznych, oraz wskazanie przyczyn takiego stanowiska ALBO b) w przypadku, gdy naruszenie może powodować wysokie ryzyko naruszenia praw i wolności osób fizycznych, wskazanie, że, że administrator wdrożył odpowiednie techniczne i organizacyjne środki ochrony i zastosował je do danych, których dotyczy naruszenie, zastosował środki eliminujące prawdopodobieństwo wysokiego ryzyka, o którym mowa powyżej, lub też - że zawiadomienie zostało zastąpione publicznym komunikatem z tego względu że zawiadomienie osób, których dane dotyczą, wymagałoby niewspółmiernie dużego wysiłku.	Należy opisać faktycznie zaistniałe skutki naruszenia bezpieczeństwa ochrony danych, w tym: a) skutki dla praw i wolności podmiotów danych b) skutki dla Administratora c) skutki dla osób trzecich	Należy szczegółowo opisać działania zaradcze podjęte przez Administratora w celu usunięcia skutków naruszenia oraz zminimalizowania ryzyka powtórzenia się naruszenia w przyszłości.						
1							NISKI												
2				2	1	0,75	ŚREDNI												
3				2	1	0,25	ŚREDNI												
4							NISKI												
5							NISKI												
6							NISKI												
7							NISKI												
8							NISKI												
9							NISKI												
10							NISKI												
11							NISKI												
12							NISKI												
13							NISKI												
14							NISKI												
15							NISKI												
16							NISKI												
17							NISKI												
18							NISKI												
19							NISKI												
20							NISKI												
21							NISKI												
22							NISKI												
23							NISKI												
24							NISKI												
25							NISKI												
26							NISKI												
27							NISKI												
28							NISKI												
29							NISKI												
30							NISKI												
31							NISKI												
32							NISKI												
33							NISKI												
34							NISKI												
35							NISKI												
36							NISKI												
37							NISKI												
38							NISKI												
39							NISKI												
40							NISKI												
41							NISKI												
42							NISKI												
43							NISKI												
44							NISKI												
45							NISKI												
46							NISKI												
47							NISKI												
48							NISKI												
49							NISKI												
50							NISKI												
51							NISKI												
52							NISKI												
53							NISKI												
54							NISKI												
55							NISKI												
56							NISKI												
57							NISKI												
58							NISKI												
59							NISKI												
60							NISKI												

POLITYKA WYBORU DOSTAWCY PRZETWARZAJĄCEGO DANE OSOBOWE

METRYKA DOKUMENTU	
WERSJA	1.0
DATA	31.10.2023 r.
LICZBA STRON	183
CEL DOKUMENTU	Niniejsza polityka ma na celu zapewnienie zgodności z RODO w zakresie wyboru podmiotów przetwarzających dane na zlecenie Gminy, tj. spełnienie obowiązku korzystania wyłącznie z usług podmiotów, które zapewniają wystarczające gwarancje wdrożenia odpowiednich środków technicznych i organizacyjnych, by przetwarzanie spełniało wymogi RODO oraz chroniło prawa osób, których dane dotyczą.
SPIS TREŚCI	1. Postanowienia ogólne ..... 130 2. Warunki dopuszczalności zawarcia umowy powierzenia z Dostawcą ... 131 3. Zawarcie umowy z Dostawcą ..... 132 4. Zasada de minimis ..... 132 5. Weryfikacja kandydata na Dostawcę ..... 133 6. Uprawnienia IOD ..... 134 7. Lista Zweryfikowanych Dostawców ..... 134 8. Postanowienia końcowe ..... 135 Załącznik B – Warunki dopuszczalności zawarcia Umowy w trybie PZP 136

1. POSTANOWIENIA OGÓLNE

- Niniejsza Polityka określa sposób przeprowadzenia procesu wyboru Dostawców, którym Gmina powierza przetwarzanie Danych osobowych.

- Pojęcia pisane wielką literą mają znaczenie zdefiniowane poniżej:

    - **Administrator** - **Gmina Miedźno** z siedzibą w Miedźnie ul. Ułańska 25, 42-120 Miedźno, NIP: 5742055080,

    - **Biuro Zakupów** – jednostka organizacyjna w biorąca udział w procesie wyboru Dostawców zgodnie z Polityką. W przypadku, gdy nie została wydzielona taka jednostka, zadania Biura Zakupów określone w Polityce realizuje inna osoba wyznaczona zgodnie z odrębnymi procedurami.

    - **Dane osobowe** – informacje o zidentyfikowanej lub możliwej do zidentyfikowania osobie fizycznej („osobie, której dane dotyczą"); możliwa do zidentyfikowania osoba fizyczna to osoba, którą można bezpośrednio lub pośrednio zidentyfikować, w szczególności na podstawie identyfikatora takiego jak: imię i nazwisko, numer identyfikacyjny, dane o lokalizacji, identyfikator internetowy lub jeden bądź kilka szczególnych czynników określających fizyczną, fizjologiczną, genetyczną, psychiczną, ekonomiczną, kulturową lub społeczną tożsamość tej osoby.

    - **Dostawca** – osoba fizyczna prowadząca działalność gospodarczą lub jednostka organizacyjna posiadająca osobowość prawną lub nieposiadająca osobowości prawnej (niezależnie od tego, czy taka jednostka jest członkiem grupy kapitałowej), która na podstawie umowy zawartej z Gminą dotyczącej korzystania przez Gminę z Usług przetwarza Dane osobowe, których Gmina jest administratorem lub w stosunku do których jest podmiotem przetwarzającym Dane osobowe na zlecenie administratora.

    - **EOG** – Europejski Obszar Gospodarczy obejmujący kraje UE oraz Islandię, Norwegię i Liechtenstein.

    - **IOD** – Inspektor Ochrony Danych, wyznaczony przez Gminę, nadzorujący przestrzeganie przepisów o ochronie danych osobowych w Gminie, wykonujący zadania określone w art. 39 RODO.

    - **Kandydat na Dostawcę** – podmiot, z którym Gmina rozważa zawarcie Umowy lub który zostaje poddany weryfikacji zgodnie z Polityką.

    - **Lista Zweryfikowanych Dostawców** – lista Dostawców, o której mowa w rozdziale 7 Polityki.

    - **Podmiot Danych** – osoba, której dotyczą Dane osobowe przetwarzane przez Gminę.

    - **Polityka** – niniejsza Polityka wyboru Dostawcy – podmiotu przetwarzającego Dane osobowe na zlecenie Gminy.

    - **RODO** – Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z

przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych).

- **Szczególne Kategorie Danych** – Dane osobowe ujawniające pochodzenie rasowe lub etniczne, poglądy polityczne, przekonania religijne lub światopoglądowe, przynależność do związków zawodowych oraz dane genetyczne, dane biometryczne przetwarzane w celu jednoznacznego zidentyfikowania osoby fizycznej lub dane dotyczące zdrowia, seksualności albo orientacji seksualnej tej osoby.

- **Umowa** – umowa pomiędzy Gminą a Dostawcą, w ramach wykonania której Dostawca przetwarza Dane osobowe pochodzące od Gminy.

- **Umowa Powierzenia** – umowa powierzenia przetwarzania Danych osobowych lub umowa dalszego powierzenia przetwarzania Danych osobowych, która ma zostać zawarta pomiędzy Gminą a Dostawcą w związku z Umową.

- **Usługi** – usługi lub inne świadczenia wykonywane przez Dostawcę na rzecz Gminy, z którymi wiąże się przetwarzanie przez Dostawcę Danych osobowych pochodzących od Gminy.

- **Właściciel Biznesowy** – jednostka organizacyjna w Gminy zgłaszająca potrzebę zawarcia Umowy z Dostawcą.

2. WARUNKI DOPUSZCZALNOŚCI ZAWARCIA UMOWY POWIERZENIA Z DOSTAWCĄ

- Warunkiem dopuszczalności powierzenia przetwarzania Danych osobowych jest zapewnienie przez kandydata na Dostawcę gwarancji wdrożenia odpowiednich środków technicznych i organizacyjnych, tak by przetwarzanie spełniało wymogi RODO i chroniło prawa Podmiotów Danych.

- Gmina może powierzyć kandydatowi na Dostawcę przetwarzanie Danych osobowych na podstawie Umowy Powierzenia w następujących przypadkach:

  - gdy kandydat na Dostawcę jest wpisany na Listę Zweryfikowanych Dostawców zgodnie z rozdziałem 7 Polityki;

  - gdy kandydat na Dostawcę stosuje zatwierdzony kodeks postępowania, o którym mowa w art. 40 RODO;

  - gdy kandydat na Dostawcę posiada zatwierdzony mechanizm certyfikacji lub znak jakości w zakresie ochrony Danych osobowych, o których mowa w art. 42 RODO i które obejmują całość operacji przetwarzania danych przez kandydata na Dostawcę w ramach realizacji Umowy;

  - gdy spełnione są warunki określone w rozdziale 4 Polityki;

- gdy kandydat na Dostawcę przeszedł pozytywną weryfikację zgodnie z rozdziałem 5 Polityki;

- W szczególnie uzasadnionych przypadkach Gmina może zawrzeć Umowę z danym kandydatem na Dostawcę bez konieczności jego weryfikacji. Właściwa osoba działająca z upoważnienia Gminy zobowiązany jest udokumentować przyczyny odstąpienia od weryfikacji Dostawcy.

3. ZAWARCIE UMOWY Z DOSTAWCĄ

- Właściciel Biznesowy, przy wsparciu Biura Zakupów, ustala, czy spełniony został choćby jeden z warunków określonych w pkt 0.□□ – 0.□□. W takim przypadku Gmina może zawrzeć z kandydatem na Dostawcę Umowę.

- W razie, gdy żaden z warunków określonych w pkt 0.□□ – 0.□□ nie jest spełniony, Gmina przystępuje do weryfikacji Dostawcy zgodnie z rozdziałem 5.

- Przed zawarciem Umowy Właściciel Biznesowy i Biuro Zakupów mogą zasięgnąć opinii IOD. IOD ma prawo wydania negatywnej opinii w przedmiocie zawarcia Umowy z kandydatem na Dostawcę w każdym przypadku, także gdy spełnione są przesłanki określone w punktach 0.□□ – 0.□□. Ostateczną decyzję w przedmiocie zawarcia Umowy z Dostawcą podejmuje Gmina.

4. ZASADA DE MINIMIS

- Jeżeli kandydat na Dostawcę nie jest wpisany na Listę Zweryfikowanych Dostawców ani nie zachodzą przypadki określone w pkt 0.□□ lub 0.□□, Gmina może zawrzeć Umowę z Dostawcą bez konieczności jego weryfikacji w sposób określony w rozdziale 5, jeżeli spełnione są łącznie wszystkie następujące warunki:

    - powierzenie nie zakłada profilowania Podmiotów danych przez Dostawcę na zlecenie Gminy; oraz

    - powierzenie nie obejmuje zautomatyzowanego podejmowania decyzji wobec Podmiotów danych przez Gminę z wykorzystaniem Usług kandydata na Dostawcę; oraz

    - powierzenie nie zakłada systematycznego monitorowania (obserwacji) zachowań Podmiotów danych; oraz

    - powierzenie nie obejmuje Szczególnych Kategorii Danych ani danych dotyczących wyroków skazujących, ani naruszeń prawa; oraz

    - powierzenie nie wiąże się z przetwarzaniem na dużą skalę Danych osobowych przez Dostawcę (przy ocenie tego kryterium należy wziąć pod uwagę liczbę Podmiotów danych, zakres powierzanych danych, czas trwania powierzenia oraz zakres geograficzny przetwarzania); oraz

- powierzenie nie wiąże się z innowacyjnym wykorzystaniem nowych rozwiązań technologicznych (np. wykorzystaniem aplikacji „Internetu rzeczy"), przy czym za innowacyjne wykorzystanie nowych technologii nie uważa się znanych już sposobów wykorzystania nowych technologii; oraz

- kandydat na Dostawcę ma siedzibę w państwie należącym do EOG; oraz

- w ramach powierzenia nie dochodzi do transferu Danych osobowych poza EOG.

- Oceny spełnienia warunków wskazanych w pkt 0.□ dokonuje Właściciel Biznesowy przy wsparciu Biura Zakupów. W razie potrzeby Właściciel Biznesowy zasięga opinii IOD.

- Przed zawarciem Umowy z Dostawcą w przypadku, o którym mowa w niniejszym rozdziale, Gmina zasięga opinii IOD. IOD może zarekomendować w szczególności przeprowadzenie weryfikacji kandydata na Dostawcę zgodnie z rozdziałem 5 Polityki.

- Ostateczną decyzję w przedmiocie zawarcia Umowy z kandydatem na Dostawcę podejmuje Gmina.

5. WERYFIKACJA KANDYDATA NA DOSTAWCĘ

- W przypadku powzięcia decyzji w przedmiocie przeprowadzenia weryfikacji kandydata na Dostawcę, weryfikacja przeprowadzana jest poprzez analizę wszystkich lub wybranych następujących informacji lub czynników:

    - oświadczenia złożone w ramach ankiety weryfikacji Dostawcy; wzór ankiety stanowi Załącznik A do Polityki;

    - informacje publikowane przez kandydata na Dostawcę na stronie internetowej oraz inne informacje uzyskane od podmiotu na etapie zapytań ofertowych, w tym informacje o tym, czy kandydat na Dostawcę dysponuje odpowiednią wiedzą fachową nt. ochrony Danych osobowych oraz środkami technicznymi i organizacyjnymi gwarantującymi bezpieczeństwo Danych osobowych;

    - opinie i rekomendacje nt. współpracy z kandydatem na Dostawcę dostępne w Internecie lub uzyskane z innych możliwych źródeł w granicach obowiązującego prawa;

    - posiadany przez kandydata na Dostawcę certyfikat lub przedłożone oświadczenie dotyczące wdrożonego systemu zarządzania bezpieczeństwem informacji, zgodnego z wymaganiami normy ISO/IEC 27001 lub innymi adekwatnymi normami;

    - doświadczenia Gminy lub podmiotów należących do grupy kapitałowej Gminy związane z dotychczasową współpracą z kandydatem na Dostawcę;

    - informacje nt. toczących się w stosunku do kandydata na Dostawcę postępowań administracyjnych lub sądowych dotyczących ochrony Danych osobowych, ochrony informacji niejawnych lub tajemnic szczególnie chronionych.

- Weryfikacji dokonuje Właściciel Biznesowy, przy wsparciu Biura Zakupów oraz IOD. Właściciel Biznesowy podejmuje decyzję, które z informacji i czynników należy wziąć pod uwagę w związku z prowadzoną weryfikacją.

- Gmina może dokonać weryfikacji prawidłowości oświadczeń kandydata na Dostawcę w sposób uzgodniony z IOD.

- Przed zawarciem Umowy z Dostawcą w przypadku, o którym mowa w niniejszym rozdziale, Gmina zasięga opinii IOD. Ostateczną decyzję w przedmiocie zawarcia Umowy z kandydatem na Dostawcę podejmuje Gmina, na podstawie analizy całości zgromadzonego materiału.

6. UPRAWNIENIA IOD

- W każdym przypadku przed zawarciem Umowy z kandydatem na Dostawcę Biuro Zakupów ma obowiązek poinformować IOD o sposobie weryfikacji kandydata na Dostawcę zgodnie z niniejszą procedurą oraz o wynikach takiej weryfikacji.

- W każdym przypadku IOD:

    - ma prawo wyrażenia opinii w przedmiocie zawarcia Umowy z kandydatem na Dostawcę oraz metod weryfikacji. Opinia powinna być sporządzona na piśmie lub w formie e-maila. Opinia negatywna powinna być umotywowana. Brak informacji ze strony IOD w terminie 5 dni roboczych od dnia otrzymania wniosku o przedstawienie opinii uważany będzie za brak przeciwwskazań do zawarcia Umowy z kandydatem na Dostawcę;

    - ma prawo żądać dodatkowych informacji od kandydata na Dostawcę, jeżeli w jego ocenie takie dodatkowe informacje są w danym przypadku niezbędne w celu dokonania oceny kandydata na Dostawcę;

    - ma prawo zarekomendować przeprowadzenie audytu u kandydata na Dostawcę lub zlecić podmiotowi zewnętrznemu przeprowadzenie takiego audytu, jeżeli w jego ocenie przeprowadzenie audytu w danym przypadku jest niezbędne w celu dokonania oceny kandydata na Dostawcę.

- Opinie IOD, wydawane na podstawie Polityki, nie mają charakteru wiążącego.

7. LISTA ZWERYFIKOWANYCH DOSTAWCÓW

- Gmina prowadzi Listę Zweryfikowanych Dostawców.

- Na Listę Zweryfikowanych Dostawców może zostać wpisany Dostawca, który:

    - został pozytywnie zweryfikowany zgodnie z rozdziałem 5 Polityki;

    - stosuje zatwierdzony kodeks postępowania, o którym mowa w art. 40 RODO;

    - posiada zatwierdzony mechanizm certyfikacji lub znak jakości w dziedzinie ochrony Danych osobowych, o których mowa w art. 42 RODO, obejmujący całość

operacji przetwarzania danych oferowanych przez kandydata na Dostawcę w ramach realizacji Usług na rzecz Gminy.

- Pozytywny wynik weryfikacji Dostawcy umożliwiający wpis na Listę Zweryfikowanych Dostawców zachowuje ważność przez 12 miesięcy z zastrzeżeniem pkt. 0.□ – 0.□ poniżej.

- IOD może w każdej chwili zarekomendować Gminy dokonanie weryfikacji, przewidzianej w rozdziale 5 Polityki, Dostawcy wpisanego na Listę Zweryfikowanych Dostawców.

- W przypadku naruszenia przez Dostawcę wpisanego na Listę Zweryfikowanych Dostawców zawartej Umowy Powierzenia, skutkującego żądaniem przez Gminę zapłaty kary umownej dotyczącej naruszenia zasad przetwarzania Danych osobowych lub rozwiązaniem Umowy Powierzenia z przyczyn leżących po stronie Dostawcy, Gmina przeprowadza ponowną weryfikację Dostawcy zgodnie z Polityką.

8. POSTANOWIENIA KOŃCOWE

- W odniesieniu do Usług świadczonych na rzecz Gminy w trybie ustawy z dnia 29 stycznia 2004 r. – Prawo zamówień publicznych, Polityka znajduje zastosowanie wyłącznie w zakresie:
  - Rozdziału 1 i 8 Polityki oraz
  - Załącznika B do Polityki („Warunki dopuszczalności zawarcia Umowy w trybie PZP")
- Postanowienia Polityki odnoszące się do IOD stosuje się odpowiednio do KODO.
- Wszystkie czynności podejmowane na podstawie Polityki są dokumentowane w formie pisemnej lub elektronicznej (w tym e-mailowej).
- Integralną częścią Polityki stanowią załączniki:
  - Załącznik A – Ankieta weryfikacji Dostawcy;
  - Załącznik B – Warunki dopuszczalności zawarcia Umowy w trybie PZP.
- Polityka jest aktualizowana przez Administratora w zależności od potrzeb. IOD jest uprawniony do składania wniosku o aktualizację Polityki.
- Polityka obowiązuje od dnia wskazanego w Zarządzenia Wójta Gminy Miedźno.

Załącznik B – Warunki dopuszczalności zawarcia Umowy w trybie PZP

Na potrzeby niniejszego załącznika znajdują zastosowanie następujące definicje:

PZP – ustawa z dnia 29 stycznia 2004 r. – Prawo zamówień publicznych;

Rozporządzenie – Rozporządzenie Ministra Rozwoju z dnia 26 lipca 2016 r. w sprawie rodzajów dokumentów, jakich może żądać zamawiający od wykonawcy w postępowaniu o udzielenie zamówienia.

Warunkiem dopuszczalności powierzenia przetwarzania Danych osobowych jest zapewnienie przez kandydata na Dostawcę gwarancji wdrożenia odpowiednich środków technicznych i organizacyjnych, tak by przetwarzanie spełniało wymogi RODO i chroniło prawa Podmiotów Danych.

W przypadku postępowań prowadzonych w trybie PZP weryfikacja zapewnienia przez kandydata na Dostawcę gwarancji, o których mowa w pkt 0, może polegać w szczególności na:

żądaniu przedstawienia certyfikatów, o których mowa w art. 42 Rozporządzenia 2016/679, w zakresie obejmującym całość operacji przetwarzania danych niezbędnych do realizowania Umowy głównej lub oświadczenia o stosowaniu zatwierdzonego kodeksu postępowania, o którym mowa w art. 40 Rozporządzenia 2016/679, lub złożenia równoważnych im oświadczeń; Gmina żąda dokumentów, o których mowa w niniejszym punkcie, na podstawie § 13 ust. 1 Rozporządzenia w sprawie rodzajów dokumentów; certyfikaty lub równoważne im oświadczenia traktowane są wówczas jako dokumenty przedmiotowe, analogicznie jak np. dokumenty wymienione w § 13 ust. 1 pkt 2 Rozporządzenia w sprawie rodzajów dokumentów;

określeniu wymogów dotyczące kwalifikacji personelu w zakresie wiedzy i doświadczenia w obszarze ochrony Danych osobowych (jako wymagań podmiotowych) oraz odpowiednio wymagań w zakresie składanych dokumentów, tzn. wykazu osób, o którym mowa w § 2 ust. 4 pkt 10 Rozporządzenia;

zawarciu w projekcie Umowy Powierzenia stosownych oświadczeń i zapewnień Dostawcy, w tym dotyczących stosowanych zabezpieczeń, kwalifikacji personelu oraz obowiązujących regulacji wewnętrznych.

Sposób sformułowania wymagań oraz oświadczeń, o których mowa w pkt 0, w zależności od poziomu ryzyka związanego z powierzeniem przetwarzania Danych osobowych, w razie potrzeby konsultuje się z IOD.

GMINA MIEDŹNO

POLITYKA WSPÓŁPRACY Z ORGANEM OCHRONY DANYCH OSOBOWYCH

METRYKA DOKUMENTU	
STATUS	Dokument wewnętrzny
WERSJA DOKUMENTU	1.0
DATA DOKUMENTU	31.10.2023
LICZBA STRON	183
CEL DOKUMENTU	Niniejszy dokument określa możliwe zdarzenia, które będą mogły skutkować nawiązaniem współpracy z organem nadzorczym.
SPIS TREŚCI	1. Definicje ..... 139 2. Ogólne zasady komunikacji z Prezesem UODO ..... 139 3. Wyznaczanie Inspektora Ochrony Danych ..... 140 4. Postępowanie kontrolne ..... 140 5. Postępowanie administracyjne i sądowoadministracyjne ..... 142 6. Informowanie o naruszeniach ..... 142 7. Uprzednie konsultacje ..... 142 8. Certyfikacja i inne postępowania przed Prezesem UODO ..... 143 9. Postanowienia końcowe 143

6. DEFINICJE

6.1. **Administrator - Gmina Miedźno** z siedzibą w Miedźnie ul. Ułańska 25, 42-120 Miedźno, NIP: 5742055080

6.2. **IOD –** Inspektor Ochrony Danych, wyznaczony przez Gminę, nadzorujący przestrzeganie przepisów o ochronie danych osobowych w Gminie, wykonujący zadania określone w art. 39 RODO.

6.3. **Konsultacje –** konsultacje z Prezesem UODO dokonywane w przypadku, o którym mowa w art. 36 ust. 1 RODO, tzn. w przypadku, gdy ocena skutków przetwarzania dla ochrony danych (DPIA) wskazuje, że przetwarzanie powodowałoby wysokie ryzyko, gdyby Administrator nie zastosował środków w celu zminimalizowania tego ryzyka.

6.4. **Kontrolujący –** osoba prowadząca postępowanie kontrolne zgodnie z Ustawą.

6.5. **Organ nadzorczy –** Prezes Urzędu Ochrony Danych Osobowych, lub ewentualnie właściwy organ nadzorczy w zakresie danych osobowych wyznaczony przez inne państwo członkowie Unii Europejskiej.

6.6. **Polityka –** niniejsza Polityka współpracy z organem ochrony danych osobowych.

6.7. **Polityka analizy ryzyka –** Polityka analizy ryzyka i oceny skutków przetwarzania danych przyjęta w Gminie.

6.8. **Procedura notyfikacji naruszeń –** Procedura oceny i notyfikacji naruszeń ochrony danych osobowych przyjęta w Gminie.

6.9. **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.

6.10. **Ustawa –** ustawa z dnia 10 maja 2018 r. o ochronie danych osobowych (Dz. U. 2018 poz. 1000 z późn. zm.).

7. OGÓLNE ZASADY KOMUNIKACJI Z PREZESEM UODO

7.1. Osobą upoważnioną do składania oświadczeń, w tym kierowania pism lub prowadzenia korespondencji z Prezesem UODO w imieniu Gminy, jest IOD.

7.2. O wyznaczeniu IOD lub o zmianie jego danych należy zawiadomić Prezesa UODO w sposób określony w Ustawie. Zawiadomienia dokonuje IOD lub inna osoba upoważniona do tego przez Gminę.

8. WYZNACZANIE INSPEKTORA OCHRONY DANYCH

8.1. Wyznaczenie IOD jest obowiązkowe w przypadkach i na zasadach określonych w art. 37 RODO. Wyznaczenie IOD odbywa się w oparciu o zarządzenie Kierownika Jednostki.

8.2. Gmina zawiadamia Organ nadzorczy o wyznaczeniu IOD w terminie 14 dni od dnia jego wyznaczenia. Zawiadomienie powinno być dokonane i opatrzone kwalifikowanym podpisem elektronicznym albo podpisem potwierdzonym profilem zaufanym ePUAP. Zawiadomienie powinno być dokonane zgodnie ze wzorem aktualnie dostępnym na stronie Organu nadzorczego.

8.3. Zawiadomienie powinno obejmować co najmniej:

8.3.1. informacje dotyczące IOD w zakresie: imienia i nazwiska, adresu poczty elektronicznej lub numer telefonu;

8.3.2. dane dotyczące Gminy: nazwa oraz adres siedziby Gminy, numer REGON.

8.4. Gmina publikuje dane kontaktowe IOD w zakresie: imię i nazwisko, adres poczty elektronicznej lub numer telefonu, na swojej stronie internetowej.

9. POSTĘPOWANIE KONTROLNE

9.1. Kontrola Prezesa UODO co do zasady jest uprzednio zapowiadana.

9.2. W postępowaniu kontrolnym Gminę reprezentuje IOD. W razie braku możliwości udziału IOD w postępowaniu kontrolnym – a także w innych przypadkach, jeśli Administrator uzna to za konieczne – Administrator wyznacza osobę zobowiązaną do reprezentowania Gminy w tym postępowaniu. Gmina sporządza pisemne upoważnienie do reprezentowania w trakcie kontroli.

9.3. Osoba reprezentująca Gminę w postępowaniu kontrolnym powinna zapewnić, że:

9.3.1. przed przystąpieniem do kontroli Kontrolujący okazał wymagane Ustawą imienne upoważnienie do przeprowadzenia kontroli oraz legitymację służbową. W przypadku, gdy Kontrolującym jest członek lub pracownik Organu nadzorczego innego państwa Unii Europejskiej, Kontrolujący powinien przedstawić imienne upoważnienie oraz dokument potwierdzający tożsamość;

9.3.2. zostały dokonane wymagane wpisy w książce kontroli Gminy;

9.3.3. w każdej czynności postępowania kontrolnego umożliwia się udział osobie reprezentującej Gminę.

9.4. Kontrolującemu należy zapewnić warunki i środki niezbędne do sprawnego przeprowadzenia kontroli, w tym w szczególności:

9.4.1. umożliwić wstęp na teren i do lokali lub innych pomieszczeń Gminy;

9.4.2. w miarę możliwości udostępnić odrębne pomieszczenie w lokalu Gminy w celu prowadzenia czynności kontrolnych;

9.4.3. wykonywać żądane przez Kontrolującego kopie lub wydruki dokumentów czy informacji utrwalonych na dowolnych nośnikach;

9.4.4. umożliwić dostęp do wszelkich zasobów mających związek z przedmiotem kontroli, w tym w szczególności do dokumentów, informacji lub urządzeń technicznych.

9.5. Wszystkie osoby zatrudnione w Gminie są zobowiązane do współpracy z Kontrolującym w postępowaniu kontrolnym, w tym do składania wyjaśnień, okazywania dokumentów i umożliwiania dostępu do sprzętu służącego do przetwarzania danych. Wszystkie osoby zatrudnione w Gminie zobowiązane są w szczególności:

9.5.1. wykonywać polecenia przełożonego oraz IOD w zakresie współpracy z Kontrolującym;

9.5.2. zachowywać spokój, zwracać się uprzejmie i z szacunkiem do Kontrolującego;

9.5.3. w przypadku pytań ze strony Kontrolującego:

4.5.3.1. upewnić się, że o kontroli został poinformowany IOD;
4.5.3.2. przed udzieleniem odpowiedzi poprosić o udział w czynności pracownika lub IOD;
4.5.3.3. upewnić się, że pytanie jest zrozumiałe;
4.5.3.4. udzielać rzeczowych odpowiedzi oraz
4.5.3.5. sporządzić notatkę z listą pytań i odpowiedzi;

9.5.4. nie utrudniać kontroli, w szczególności poprzez:

4.5.4.1. blokowanie fizycznego dostępu do budynków, pomieszczeń, przedmiotów lub osób;
4.5.4.2. usuwanie, niszczenie lub chowanie dokumentów, komputerów, dysków czy innego sprzętu bądź ich zawartości;
4.5.4.3. udzielanie nieprawdziwych lub nierzetelnych informacji w odpowiedzi na pytania Kontrolującego;
4.5.4.4. omawianie kwestii będących przedmiotem kontroli z osobami spoza Gminy lub pracownikami innymi niż IOD..

9.6. W razie wątpliwości, czy żądanie lub polecenie Kontrolującego pozostaje w związku z przedmiotem kontroli, lub w przypadku, gdy Gmina odmawia spełnienia żądania albo polecenia Kontrolującego, należy zadbać o zamieszczenie odpowiedniej wzmianki w protokole kontroli ze wskazaniem przyczyn takiej decyzji. Odmowa spełnienia żądania lub polecenia Kontrolującego ze względów wskazanych w zdaniu poprzedzającym dopuszczalna jest tylko za zgodą Kierownika Jednostki.

9.7. W razie zażądania przez Kontrolującego dostępu do danych lub informacji stanowiących tajemnicę przedsiębiorstwa, tajemnicę zawodową lub inną tajemnicę bądź informację prawnie chronioną, takie dane lub informacje należy ujawnić, jednocześnie żądając odnotowania w protokole kontroli powyższej okoliczności. W przypadku przekazywania Kontrolującemu kopii lub odpisu dokumentu zawierającego informacje stanowiące tego rodzaju tajemnicę lub informację prawnie chronioną, należy przekazać również wersję dokumentu niezawierającą

tych informacji. W razie wątpliwości, czy żądane dane lub informacje są prawnie chronione, należy zasięgnąć opinii prawnika jednostki.

9.8. W razie utrwalania (nagrywania) przez Kontrolującego przebiegu kontroli, należy zapewnić, by nagranie zostało załączone do protokołu kontroli.

9.9. W razie zamiaru utrwalania (nagrywania) przebiegu kontroli przez Administratora, osoba reprezentująca Administratora w postępowaniu kontrolnym:

9.9.1. informuje Kontrolującego o zamiarze utrwalania (nagrywania) przebiegu kontroli;

9.9.2. stosuje się do decyzji Kontrolującego w tym zakresie, również w przypadku, gdy Kontrolujący nie zezwala na utrwalenie (nagranie) przebiegu kontroli;

9.9.3. zapewnia, by wzmianka o poinformowaniu o zamiarze utrwalenia (nagrywania) przebiegu kontroli, jak również odpowiedź udzielona przez Kontrolującego zostały zawarte w protokole kontroli.

9.10. Protokół kontroli podpisuje IOD lub inna osoba reprezentująca Administratora w postępowaniu kontrolnym. W razie zastrzeżeń do protokołu IOD lub osoba reprezentująca Administratora w postępowaniu kontrolnym zgłasza je Kontrolującemu w formie pisemnej w terminie 7 dni od dnia przedstawienia protokołu do podpisu. W razie wątpliwości w tym zakresie IOD lub osoba reprezentująca Administratora w postępowaniu kontrolnym zasięga opinii prawnika jednostki.

10. POSTĘPOWANIE ADMINISTRACYJNE I SĄDOWOADMINISTRACYJNE

10.1. Dział prawny w razie konieczności zasięga opinii IOD co do treści pism lub innej dokumentacji związanej z postępowaniem administracyjnym oraz sądowo-administracyjnym.

10.2. Oceniając zasadność wniesienia do sądu administracyjnego skargi na decyzję (postanowienie) Prezesa UODO, Dział prawny zasięga opinii IOD. IOD zobowiązany jest przedstawić opinię w terminie 5 dni roboczych od dnia zgłoszenia żądania przez Dział prawny.

11. INFORMOWANIE O NARUSZENIACH

11.1. Zasady informowania Prezesa UODO o naruszeniach ochrony danych osobowych określone zostały w Procedurze oceny i notyfikacji naruszeń.

12. UPRZEDNIE KONSULTACJE

12.1. IOD kieruje do Prezesa UODO wniosek o przeprowadzenie Konsultacji w sposób określony w Ustawie w przypadku, gdy łącznie zostaną spełnione następujące warunki:

12.1.1. zostaną spełnione warunki zobowiązujące Gminę do przeprowadzenia Konsultacji w związku z przeprowadzoną przez Gminę oceną skutków przetwarzania zgodnie z Polityką analizy ryzyka oraz

12.1.2. Zarząd podejmie decyzję o złożeniu wniosku o przeprowadzenie Konsultacji.

12.2. Treść wniosku o przeprowadzenie Konsultacji powinna zostać zaopiniowana przez Dział prawny.

13. CERTYFIKACJA I INNE POSTĘPOWANIA PRZED PREZESEM UODO

13.1. W przypadku podjęcia przez Gminę decyzji o wdrożeniu mechanizmu certyfikacji IOD przygotowuje analizę dotyczącą spełnienia przez Gminę kryteriów certyfikacji oraz przedstawia rekomendację co do podmiotu mającego udzielić certyfikacji.

13.2. W postępowaniu o udzielenie certyfikacji Gminę reprezentuje IOD.

13.3. IOD prowadzi bieżącą weryfikację spełniania przez Gminę kryteriów certyfikacji. W razie konieczności IOD przedstawia Administratorowi stosowny raport.

13.4. Do postępowania w zakresie znaków jakości lub rozpoczęcia stosowania kodeksu postępowania pkt. 13.1–13.3 stosuje się odpowiednio.

14. POSTANOWIENIA KOŃCOWE

14.1. Postanowienia Polityki dotyczące IOD stosuje się odpowiednio do KODO.

14.2. Procedura wchodzi w życie z dniem wskazanym w zarządzeniu Wójta Gminy Miedźno.

GMINA MIEDŹNO

ZASADY DOKUMENTOWANIA TECHNICZNYCH I ORGANIZACYJNYCH ŚRODKÓW BEZPIECZEŃSTWA OCHRONY DANYCH

METRYKA DOKUMENTU	
STATUS	Dokument wewnętrzny
WERSJA DOKUMENTU	1.0
DATA DOKUMENTU	31.10.2023 r.
LICZBA STRON	183
CEL DOKUMENTU	Niniejszy dokument zawiera wykaz technicznych i organizacyjnych środków zabezpieczających przetwarzanie danych osobowych.
SPIS TREŚCI	1. Definicje ..... 146 2. Zasady dokumentowania stosowanych środków ochrony danych 146 3. Postanowienia końcowe ..... 146 Załącznik A – Wykaz środków bezpieczeństwa 147

15. DEFINICJE

15.1. **Administrator** (także **Gmina** lub **Organizacja**) **– Gmina Miedźno** z siedzibą w Miedźnie ul. Ułańska 25, 42-120 Miedźno, NIP: 5742055080

15.2. **IOD** – Inspektor Ochrony Danych wyznaczony przez Gminę, nadzorujący przestrzeganie przepisów o ochronie danych osobowych w Gminy.

15.3. **KODO** – koordynator ds. ochrony danych osobowych, tj. osoba wyznaczona do wykonywania zadań związanych z zapewnieniem zgodności przetwarzania danych osobowych w Gminy z obowiązującym prawem w przypadku, gdy nie został powołany IOD.

15.4. **RCP** – rejestr czynności przetwarzania, o którym mowa w art. 30 RODO, prowadzony przez Gminę.

15.5. **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.

15.6. **Wykaz** – wykaz technicznych i organizacyjnych środków bezpieczeństwa stosowanych w Gminy, uwzględniający aktualne wnioski wynikające z analizy RODO, a także wytyczne europejskich oraz krajowych organów ochrony danych, wytyczne Europejskiej Agencji ds. Bezpieczeństwa Sieci i Informacji (ENISA), rekomendacje Komisji Nadzoru Finansowego oraz normę ISO 27001:2013.

15.7. **Zasady dokumentowania** – niniejsze zasady dokumentowania technicznych i organizacyjnych środków ochrony danych osobowych, wdrożonych w Gminy.

16. ZASADY DOKUMENTOWANIA STOSOWANYCH ŚRODKÓW OCHRONY DANYCH

16.1. Administrator zapewnia, że wdrażane środki bezpieczeństwa ochrony danych są adekwatne do poziomu ryzyka, zidentyfikowanego zgodnie z odrębnymi procedurami, a stan ich wdrożenia w organizacji jest dokumentowany.

16.2. Za prowadzenie i bieżącą aktualizację Wykazu odpowiada IOD.

16.3. Aktualizacja Wykazu obejmuje w szczególności:

16.3.1. bieżące i odpowiadające stanowi rzeczywistemu określanie, które środki zostały wdrożone w Gminy i w jakim zakresie;

16.3.2. uzupełnianie Wykazu w razie wdrożenia środka bezpieczeństwa dotychczas w nim nieuwzględnionego;

16.3.3. zapewnienie zgodności wpisów dotyczących stosowanych środków bezpieczeństwa w Wykazie i RCP.

17. POSTANOWIENIA KOŃCOWE

17.1. Zasady dokumentowania odnoszące się do IOD stosuje się odpowiednio do KODO.

17.2. Zasady dokumentowania obowiązują od dnia wskazanego w zarządzeniu kierownika jednostki.

Załącznik A – Wykaz środków bezpieczeństwa[23]

1. ORGANIZACJA, ROLE I ODPOWIEDZIALNOŚCI			
RODZAJ ŚRODKA	**TAK**	**NIE**	**SPOSÓB I ZAKRES ZASTOSOWANIA ŚRODKA W ORGANIZACJI**
1.1. Wyznaczenie osoby (osób) odpowiedzialnej za zarządzanie bezpieczeństwem informacji.	☐	☐	
1.2. Powołanie Inspektora Ochrony Danych lub innej osoby odpowiedzialnej za obszar ochrony danych osobowych (koordynatora ds. ochrony danych osobowych).	☐	☐	
1.3. Określenie zasad (procedur) dotyczących zarządzania systemami informatycznymi, w tym zarządzania zmianą, konfiguracją, pojemnością, wydajnością, bezpieczeństwem itp.	☐	☐	
1.4. Wdrożenie procedury oceny skutków dla ochrony danych osobowych.	☐	☐	
1.5. Prowadzenie regularnych szkoleń dla pracowników / współpracowników w zakresie ochrony danych osobowych.	☐	☐	

[23] Wykaz uwzględnia w szczególności wytyczne zawarte w normie ISO 27001:2013; rekomendację D dotyczącą zarządzania obszarami technologii informacyjnej i bezpieczeństwa środowiska teleinformatycznego w bankach wydaną przez Komisję Nadzoru Finansowego, wytyczne Europejskiej Agencji ds. Bezpieczeństwa Sieci i Informacji: *Guidelines for SMEs on the security of personal data processing* oraz wytyczne Generalnego Inspektora Ochrony Danych Osobowych (https://giodo.gov.pl/pl/p/opinie-wytyczne-wskazowki - dostęp 11/03/2018).

1. ORGANIZACJA, ROLE I ODPOWIEDZIALNOŚCI			
RODZAJ ŚRODKA	**TAK**	**NIE**	**SPOSÓB I ZAKRES ZASTOSOWANIA ŚRODKA W ORGANIZACJI**
1.6. Zapoznawanie pracowników / współpracowników z obowiązującymi procedurami (politykami) w zakresie ochrony danych osobowych przed udzieleniem dostępu do ich przetwarzania.	☐	☐	
1.7. Zobowiązywanie pracowników / współpracowników do przestrzegania obowiązujących procedur (polityk) z zakresu ochrony danych osobowych.	☐	☐	
1.8. Przypisanie ról i zakresu odpowiedzialności w procesach przetwarzania danych osobowych każdemu uczestnikowi danego procesu.	☐	☐	
1.9. Nadawanie pracownikom / współpracownikom upoważnień do przetwarzania danych osobowych.	☐	☐	
1.10. Prowadzenie imiennej ewidencji nadawanych upoważnień.	☐	☐	
1.11. Zobowiązywanie pracowników / współpracowników do zachowania	☐	☐	

1. ORGANIZACJA, ROLE I ODPOWIEDZIALNOŚCI			
RODZAJ ŚRODKA	**TAK**	**NIE**	**SPOSÓB I ZAKRES ZASTOSOWANIA ŚRODKA W ORGANIZACJI**
w poufności danych osobowych oraz informacji dotyczących ich zabezpieczeń.			
1.12. Prowadzenie regularnych audytów bezpieczeństwa, w tym w zakresie aktualności dokumentacji i jej stosowania przez pracowników.	☐	☐	

2. DOSTĘP DO SYSTEMÓW PRZETWARZAJĄCYCH DANE OSOBOWE			
RODZAJ ŚRODKA	**TAK**	**NIE**	**SPOSÓB I ZAKRES ZASTOSOWANIA ŚRODKA W ORGANIZACJI**
2.1. Określenie zasad nadawania / zmiany / odbioru uprawnień dostępowych do poszczególnych systemów informatycznych.	☐	☐	
2.2. Prowadzenie okresowych kontroli uprawnień posiadanych przez użytkowników w systemach informatycznych.	☐	☐	
2.3. Określenie zasad zdalnego dostępu do zasobów zawierających dane osobowe.	☐	☐	
2.4. Wprowadzenie ograniczenia dostępu do systemów IT wyłącznie dla autoryzowanych urządzeń.	☐	☐	
2.5. Wdrożenie zasad przypisywania każdemu użytkownikowi systemu informatycznego służącego do przetwarzania danych osobowych indywidualnego loginu i hasła (lub innego środka uwierzytelniającego).	☐	☐	
2.6. Stosowanie rozwiązania wymagającego każdorazowego uwierzytelniania użytkownika przy logowaniu do systemu informatycznego służącego do przetwarzania danych osobowych.	☐	☐	

2. DOSTĘP DO SYSTEMÓW PRZETWARZAJĄCYCH DANE OSOBOWE			
RODZAJ ŚRODKA	**TAK**	**NIE**	**SPOSÓB I ZAKRES ZASTOSOWANIA ŚRODKA W ORGANIZACJI**
2.7. Stosowanie systemu rejestracji dostępu do systemów informatycznych, w których przetwarzane są dane osobowe.	☐	☐	
2.8. Wdrożenie zasady nadawania konta administratora wyłącznie w przypadku, gdy działania w systemie nie mogą być wykonywane za pomocą konta o niższych uprawnieniach.	☐	☐	
2.9. Wprowadzenie mechanizmu blokady dostępu do systemu informatycznego służącego do przetwarzania danych osobowych w przypadku dłuższej nieaktywności użytkownika.	☐	☐	
2.10. Stosowanie wygaszaczy ekranów na stanowiskach, na których przetwarzane są dane osobowe.	☐	☐	
2.11. Zabezpieczenie dostępu do danych osobowych przetwarzanych z wykorzystaniem komputera za pomocą hasła domenowego.	☐	☐	

3. ZARZĄDZANIE INCYDENTAMI, CIĄGŁOŚĆ DZIAŁANIA			
RODZAJ ŚRODKA	**TAK**	**NIE**	**SPOSÓB I ZAKRES ZASTOSOWANIA ŚRODKA W ORGANIZACJI**
3.1. Wdrożenie procedury obsługi incydentów stanowiących naruszenie ochrony danych osobowych.	☐	☐	
3.2. Prowadzenie rejestru naruszeń ochrony danych osobowych.	☐	☐	
3.3. Wdrożenie rozwiązań technicznych umożliwiających wykrycie nietypowych zachowań użytkowników systemów informatycznych, za pomocą których przetwarzane są dane osobowe.	☐	☐	
3.4. Wdrożenie planu ciągłości działania oraz planu awaryjnego na wypadek zaburzenia ciągłości działania.	☐	☐	
3.5. Prowadzenie cyklicznych testów wdrożonych planów ciągłości działania.	☐	☐	

4. SPRZĘT I NOŚNIKI INFORMACJI			
RODZAJ ŚRODKA	**TAK**	**NIE**	**SPOSÓB I ZAKRES ZASTOSOWANIA ŚRODKA W ORGANIZACJI**
4.1. Prowadzenie rejestru zasobów informatycznych, za pomocą których przetwarzane są dane osobowe.	☐	☐	
4.2. Prowadzenie okresowych przeglądów zasobów informatycznych, za pomocą których przetwarzane są dane osobowe.	☐	☐	
4.3. Zdefiniowanie zasad korzystania z urządzeń przenośnych (np. laptopy, pendrive'y, płyty CD/DVD itp.)	☐	☐	
4.4. Zdefiniowanie procesu wydawania i zwrotu sprzętu w związku z zatrudnieniem.	☐	☐	
4.5. Zdefiniowanie zasad korzystania z prywatnych urządzeń w celach służbowych (BYOD).	☐	☐	
4.6. Zdefiniowanie zasad przechowywania i transportu nośników mobilnych.	☐	☐	
4.7. Zdefiniowanie zasad serwisowania zasobów informatycznych, na których przechowywane są dane osobowe.	☐	☐	

4. SPRZĘT I NOŚNIKI INFORMACJI			
RODZAJ ŚRODKA	**TAK**	**NIE**	**SPOSÓB I ZAKRES ZASTOSOWANIA ŚRODKA W ORGANIZACJI**
4.8. Określenie sposobu niszczenia nośników pamięci (usuwania danych).	☐	☐	
4.9. Wdrożenie obowiązku szyfrowania urządzeń mobilnych.	☐	☐	
4.10. Wdrożenie rozwiązania pozwalającego na zdalne usuwanie danych z urządzeń mobilnych (np. w przypadku ich utraty).	☐	☐	

5. ZARZĄDZANIE BEZPIECZEŃSTWEM SIECI ORAZ SYSTEMAMI IT			
RODZAJ ŚRODKA	**TAK**	**NIE**	**SPOSÓB I ZAKRES ZASTOSOWANIA ŚRODKA W ORGANIZACJI**
5.1. Zdefiniowanie architektury / schematu sieci.	☐	☐	
5.2. Stosowanie segmentacji sieci (np. za pomocą switchy).	☐	☐	
5.3. Stosowanie logicznego odseparowania sieci gościnnej (np. dla usługodawców, kontrahentów) od sieci korporacyjnej.	☐	☐	

5. ZARZĄDZANIE BEZPIECZEŃSTWEM SIECI ORAZ SYSTEMAMI IT			
RODZAJ ŚRODKA	**TAK**	**NIE**	**SPOSÓB I ZAKRES ZASTOSOWANIA ŚRODKA W ORGANIZACJI**
5.4. Wdrożenie polityki bezpiecznego użytkowania sieci przez użytkowników.	☐	☐	
5.5. Wdrożenie systemu uwierzytelniania i logowania użytkowników do sieci gościnnej.	☐	☐	
5.6. Zabezpieczenie sieci za pomocą systemu filtrowania adresów IP.	☐	☐	
5.7. Zabezpieczenie sieci za pomocą systemu IDS/IPS.	☐	☐	
5.8. Zabezpieczenie sieci w zakresie połączeń z różnych lokalizacji (np. za pomocą SSH lub VPN).	☐	☐	
5.9. Cykliczne skanowanie portów.	☐	☐	
5.10. Wdrożenie blokady portów.	☐	☐	
5.11. Cykliczne przeglądy logów.	☐	☐	
5.12. Prowadzenie analizy ruchu sieciowego i zgłaszania incydentów – np. w formie raportów (np. SIEM).	☐	☐	

5. ZARZĄDZANIE BEZPIECZEŃSTWEM SIECI ORAZ SYSTEMAMI IT			
RODZAJ ŚRODKA	**TAK**	**NIE**	**SPOSÓB I ZAKRES ZASTOSOWANIA ŚRODKA W ORGANIZACJI**
5.13. Deszyfrowanie ruchu sieciowego.	☐	☐	
5.14. Cykliczne skany aplikacji webowych.	☐	☐	
5.15. Wdrożenie zasad regulujących rozwój i testowanie oprogramowania z perspektywy ochrony danych osobowych.	☐	☐	
5.16. Zabezpieczenie urządzeń końcowych przed złośliwym oprogramowaniem (oprogramowanie antywirusowe).	☐	☐	
5.17. Wdrożenie rozwiązań umożliwiających centralne sterowanie oprogramowaniem chroniącym przed złośliwym oprogramowaniem.	☐	☐	
5.18. Wdrożenie mechanizmów szyfrowania danych osobowych podczas ich przechowywania, przesyłania, transportu i udostępniania.	☐	☐	
5.19. Wdrożenie zasad dotyczących wykonywania i testowania kopii zapasowych.	☐	☐	

6. KLASYFIKACJA INFORMACJI			
RODZAJ ŚRODKA	**TAK**	**NIE**	**SPOSÓB I ZAKRES ZASTOSOWANIA ŚRODKA W ORGANIZACJI**
6.1. Zdefiniowanie poziomów klasyfikacji danych osobowych ze względu na przetwarzanie danych szczególnych kategorii, o których mowa w art. 9 i 10 RODO, oraz określenie zasad bezpiecznego przetwarzania danych w zależności od ich klasyfikacji.	☐	☐	
6.2. Wdrożenie narzędzi zapewniających automatyczną klasyfikację informacji.	☐	☐	

7. POLITYKA HASEŁ			
RODZAJ ŚRODKA	**TAK**	**NIE**	**SPOSÓB I ZAKRES ZASTOSOWANIA ŚRODKA W ORGANIZACJI**
7.1. Wdrożenie jednolitej i adekwatnej do zidentyfikowanych ryzyk polityki haseł.	☐	☐	
7.2. Wdrożenie mechanizmu wymuszającego cykliczną zmianę hasła.	☐	☐	
7.3. Stosowanie środków ochrony kryptograficznej w razie teletransmisji haseł.	☐	☐	

8. KRYPTOGRAFIA I PSEUDONIMIZACJA			
RODZAJ ŚRODKA	**TAK**	**NIE**	**SPOSÓB I ZAKRES ZASTOSOWANIA ŚRODKA W ORGANIZACJI**
8.1. Stosowanie zabezpieczeń kryptograficznych podczas teletransmisji danych.	☐	☐	
8.2. Stosowanie zabezpieczeń kryptograficznych danych przechowywanych w systemach (*data at rest*).	☐	☐	
8.3. Stosowanie pseudonimizacji danych osobowych.	☐	☐	

9. BEZPIECZEŃSTWO FIZYCZNE			
RODZAJ ŚRODKA	**TAK**	**NIE**	**SPOSÓB I ZAKRES ZASTOSOWANIA ŚRODKA W ORGANIZACJI**
9.1. Zabezpieczenie budynku, w którym przetwarzane są dane, systemem alarmowym.	☐	☐	
9.2. Zabezpieczenie budynku, w którym przetwarzane są dane, systemem monitoringu.	☐	☐	
9.3. Objęcie budynku, w którym przetwarzane są dane, ochroną fizyczną 24 h na dobę.	☐	☐	
9.4. Zabezpieczenie budynku, w którym przetwarzane są dane, systemem kontroli wejścia / wyjścia (karty magnetyczne).	☐	☐	
9.5. Określenie zasad nadawania / modyfikacji / odbioru uprawnień dostępowych do budynku oraz pomieszczeń, w których przetwarzane są dane.	☐	☐	
9.6. Wdrożenie procedury rejestracji wstępu w przypadku, gdy dostęp do pomieszczeń, w których przetwarzane są dane, mają osoby trzecie (np. goście, kontrahenci).	☐	☐	
9.7. Wdrożenie procedury zapewniającej, że przebywanie w pomieszczeniach, w których przetwarzane są dane, przez osoby	☐	☐	

9. BEZPIECZEŃSTWO FIZYCZNE			
RODZAJ ŚRODKA	**TAK**	**NIE**	**SPOSÓB I ZAKRES ZASTOSOWANIA ŚRODKA W ORGANIZACJI**
trzecie możliwy jest wyłącznie w obecności pracownika / współpracownika.			
9.8. Zabezpieczenie pomieszczeń, w których przetwarzane są dane, systemem monitoringu.	☐	☐	
9.9. Zabezpieczenie pomieszczeń, w których przetwarzane są dane, systemem alarmowym.	☐	☐	
9.10. Zabezpieczenie pomieszczeń, w których przetwarzane są dane, drzwiami wzmacnianymi (nie antywłamaniowymi) zamykanymi na klucz.	☐	☐	
9.11. Zabezpieczenie pomieszczeń, w których przetwarzane są dane, drzwiami antywłamaniowymi zamykanymi na klucz.	☐	☐	
9.12. Prowadzenie ewidencji osób upoważnionych do pobierania kluczy do drzwi prowadzących do pomieszczeń, w których przetwarzane są dane.	☐	☐	
9.13. Zabezpieczenie okien w pomieszczeniach, w których przetwarzane są dane, za pomocą krat, rolet lub folii antywłamaniowej.	☐	☐	

9. BEZPIECZEŃSTWO FIZYCZNE			
RODZAJ ŚRODKA	**TAK**	**NIE**	**SPOSÓB I ZAKRES ZASTOSOWANIA ŚRODKA W ORGANIZACJI**
9.14. Określenie zasad dostępu do serwerowni.	☐	☐	
9.15. Prowadzenie ewidencji wejść / wyjść do / z serwerowni.	☐	☐	
9.16. Objęcie wejścia do serwerowni monitoringiem.	☐	☐	
9.17. Zabezpieczenie pomieszczenie serwerowni systemem alarmowym.	☐	☐	
9.18. Zabezpieczenie pomieszczenia serwerowni drzwiami zwykłymi zamykanymi na klucz (nie antywłamaniowymi).	☐	☐	
9.19. Zabezpieczenie pomieszczenia serwerowni drzwiami antywłamaniowymi zamykanymi na klucz.	☐	☐	

10. ODPORNOŚĆ NA CZYNNIKI NATURALNE			
RODZAJ ŚRODKA	**TAK**	**NIE**	**SPOSÓB I ZAKRES ZASTOSOWANIA ŚRODKA W ORGANIZACJI**
10.1. Zabezpieczenie budynku, w którym przetwarzane są dane, systemem przeciwpożarowym.	☐	☐	
10.2. Zabezpieczenie serwerowni systemem przeciwpożarowym.	☐	☐	
10.3. Wyposażenie budynku, w którym przetwarzane są dane, w zasilanie awaryjne lub generator prądu.	☐	☐	
10.4. Zapewnienie klimatyzacji pomieszczenia serwerowni.	☐	☐	
10.5. Wyposażenie pomieszczenia serwerowni w system monitorowania temperatury i wilgotności (np. STE2).	☐	☐	
10.6. Wyposażenie pomieszczenia serwerowni w system detekcji wycieków / zalania.	☐	☐	
10.7. Wyposażenie pomieszczenia serwerowni w drzwi antywłamaniowe o podwyższonej ognioodporności.	☐	☐	
10.8. Umieszczenie serwerowni w oddaleniu od pomieszczeń sanitarnych lub kuchennych.	☐	☐	

10. ODPORNOŚĆ NA CZYNNIKI NATURALNE			
RODZAJ ŚRODKA	**TAK**	**NIE**	**SPOSÓB I ZAKRES ZASTOSOWANIA ŚRODKA W ORGANIZACJI**
10.9. Przechowywanie serwerów w szafie serwerowej (typu RACK).	☐	☐	
10.10. Stosowanie zabezpieczeń antyprzepięciowych (np. listwy UPS).	☐	☐	

11. WSPÓŁPRACA Z DOSTAWCAMI			
RODZAJ ŚRODKA	**TAK**	**NIE**	**SPOSÓB I ZAKRES ZASTOSOWANIA ŚRODKA W ORGANIZACJI**
11.1. Wdrożenie zasad dotyczących przekazywania danych osobowych (w tym ich powierzania).	☐	☐	
11.2. Wdrożenie zasad określających zaangażowanie IOD / KODO w proces konsultacji umów powierzenia (oceny wiarygodności dostawcy) przed rozpoczęciem współpracy z dostawcą.	☐	☐	

12. ŚRODKI WŁAŚCIWE JEDYNIE DLA PRZETWARZANIA DANYCH W FORMIE PAPIEROWEJ			
RODZAJ ŚRODKA	**TAK**	**NIE**	**SPOSÓB I ZAKRES ZASTOSOWANIA ŚRODKA W ORGANIZACJI**
12.1. Wdrożenie obowiązku przechowywania danych osobowych przetwarzanych w formie papierowej w metalowych szafach zamykanych na klucz.	☐	☐	
12.2. Wdrożenie obowiązku przechowywania danych osobowych przetwarzanych w formie papierowej w zamkniętym sejfie lub kasie pancernej.	☐	☐	
12.3. Wdrożenie polityki wydruku dokumentów, które zawierają dane osobowe, wyłącznie pod nadzorem.	☐	☐	
12.4. Zabezpieczenie procesu druku dokumentów zawierających dane osobowe za pomocą kodu PIN.	☐	☐	
12.5. Wdrożenie procedury niszczenia dokumentacji papierowej zawierającej dane osobowe.	☐	☐	
12.6. Wdrożenie polityki „czystych biurek”.	☐	☐	

GMINA MIEDŹNO

PLAN UTRZYMANIA ZGODNOŚCI Z RODO (ciągłość wdrożenia)

METRYKA DOKUMENTU	
STATUS	Dokument wewnętrzny
WERSJA DOKUMENTU	1.0
DATA DOKUMENTU	31.10.2023 r.
LICZBA STRON	183
CEL DOKUMENTU	Niniejszy dokument opisuje zasady i zadania realizowane w zakresie utrzymania w organizacji zgodności z wymogami RODO.
SPIS TREŚCI	1. Definicje ..... 170 2. Zasady ogólne ..... 170 3. Harmonogram oraz realizowanie Zadań ..... 170 4. Raportowanie ..... 171 5. Postanowienia końcowe ..... 171 Załącznik nr 2 – Zakres czynności dla realizowanych Zadań ..... 172 Załącznik nr 3 – Wzór raportu 181

9. DEFINICJE

- **Administrator** lub **Gmina** – Gmina Miedźno z siedzibą w Miedźnie ul. Ułańska 25, 42-120 Miedźno, NIP: 5742055080
- **IOD** – Inspektor Ochrony Danych, wyznaczony przez Gminę, nadzorujący przestrzeganie przepisów o ochronie danych osobowych w Gminie, wykonujący zadania określone w art. 39 RODO.
- **Organ nadzorczy** – Prezes Urzędu Ochrony Danych Osobowych.
- **Podmiot danych** – osoba fizyczna, której dotyczą dane osobowe przetwarzane przez Administratora.
- **Plan utrzymania zgodności (Plan)** – niniejszy plan utrzymania zgodności z wymogami RODO wraz z załącznikami.
- **Pracownik** – osoba fizyczna zatrudniona przez Administratora na podstawie umowy o pracę lub innej umowy cywilnoprawnej.
- **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.

10. ZASADY OGÓLNE

- Plan określa obowiązki, które w ramach utrzymania zgodności powinien realizować IOD („**Zadania**"), harmonogram realizacji poszczególnych Zadań oraz czynności, które powinny zostać wykonane w związku z ich realizacją („**Czynności**").
- Kategorie Zadań, termin realizacji Zadań oraz szacowana czasochłonność realizacji Zadań zostały określone w załączniku nr 1 do Planu: Harmonogram.
- Zakres Czynności, które należy podjąć w celu realizacji poszczególnych Zadań, określony został w załączniku nr 2 do Planu: Zakres Czynności dla realizowanych Zadań.
- Jeśli Plan nie stanowi inaczej, Zadania opisane w Planie realizuje IOD. IOD może zlecać wykonanie poszczególnych Zadań lub określonych Czynności innym osobom.
- Wszyscy Pracownicy są zobowiązani do współdziałania z IOD w zakresie realizacji Zadań wynikających z Planu.

11. HARMONOGRAM ORAZ REALIZOWANIE ZADAŃ

- Każde Zadanie wskazane w Harmonogramie przypisane zostało do kategorii Zadania Stałe albo Zadania Cykliczne i określony został dla niego termin realizacji. Przypisania Zadań do Kategorii oraz ustalenia terminów ich realizacji dokonuje IOD. Ustalenia IOD w tym zakresie wymagają akceptacji Administratora.

- Do każdego Zadania zostały przypisane określone Czynności, które powinny zostać wykonane w celu jego realizacji. Czynności te zostały określone w załączniku nr 2 do Planu. IOD może zdecydować o wykonaniu dodatkowych Czynności, które nie zostały wskazane w załączniku nr 2.

- Zadania Stałe powinny być realizowane przez IOD przez cały okres obowiązywania Planu, w zakresie wynikającym z bieżącego zapotrzebowania.

- Zadania Cykliczne należy realizować w określonym kwartale, wskazanym w Harmonogramie. IOD może jednak podjąć decyzję o zrealizowaniu określonych Czynności w ramach Zadania w dowolnym momencie.

- W Harmonogramie IOD powinien określić szacowaną miesięczną czasochłonność potrzebną do zrealizowania poszczególnych Zadań. Czasochłonność określana jest w dniach roboczych (MD).

- Harmonogram ustalany jest na okres dwóch lat kalendarzowych, za wyjątkiem pierwszego Harmonogramu, który ustalany jest do końca grudnia 2020 roku.

12. RAPORTOWANIE

- IOD jest zobowiązany do dokumentowania realizacji Zadań określonych w Harmonogramie w formie raportów zgodnych ze wzorem stanowiącym załącznik nr 3 do Planu.

- IOD ma obowiązek sporządzać raport po każdym kwartale roku kalendarzowego, w którym realizowany jest Plan. Raport powinien być przekazany Administratorowi w ciągu 20 dni roboczych od zakończenia danego kwartału.

- Raport jest archiwizowany zgodnie z odrębną procedurą przyjętą przez Administratora.

13. POSTANOWIENIA KOŃCOWE

- Zmiana Planu wymaga zatwierdzenia w sposób przyjęty przez Administratora.

- Plan wchodzi w życie z dniem wskazanym w zarządzeniu kierownika jednostki.

- Integralną część Planu stanowią jego załączniki:

    - **Załącznik nr 1 –** Harmonogram;

    - **Załącznik nr 2 –** Zakres Czynności dla realizowanych Zadań;

    - **Załącznik nr 3 –** Wzór raportu.

Załącznik nr 2 – Zakres czynności dla realizowanych Zadań

A. ZADANIA STAŁE

Zadanie:	• Realizacja procesu: prowadzenie RCP oraz RKCP
• Czynności, które należy wykonać w celu realizacji zadania:	
1.	• Dokonywanie bieżących wpisów do rejestru czynności przetwarzania, o którym mowa w art. 30 ust. 1 RODO (RCP), w przypadku rozpoczęcia realizowania przez Administratora nowej czynności przetwarzania podlegającej ewidencji
2.	• Dokonywanie bieżących wpisów do rejestru kategorii czynności przetwarzania, o którym mowa w art. 30 ust. 2 RODO (RKCP), w przypadku rozpoczęcia realizowania przez Administratora (działającego jako podmiot przetwarzający) nowej kategorii czynności przetwarzania podlegającej ewidencji
3.	• Odnotowywanie w RCP wszelkich zmian w realizowanych przez Administratora czynnościach przetwarzania
4.	• Odnotowywanie w RKCP wszelkich zmian w realizowanych przez Administratora (działającego jako podmiot przetwarzający) kategoriach czynności przetwarzania

• **Zadanie**:	• Realizacja procesu: obsługa wniosków podmiotów danych
• Czynności, które należy wykonać w celu realizacji zadania:	
1.	• Dokonywanie, zgodnie z obowiązującą procedurą, bieżącej obsługi wniosków wpływających do Administratora
2.	• Dokonywanie bieżących wpisów do rejestru w zakresie nowych wniosków wpływających do Administratora
3.	• Odnotowywanie w rejestrze wniosków wszelkich zmian wynikających ze sposobu rozpatrzenia wniosku

Zadanie:	• Realizacja procesu: obsługa naruszeń ochrony danych osobowych
• Czynności, które należy wykonać w celu realizacji zadania:	
1.	• Dokonywanie, zgodnie z obowiązującą procedurą, bieżącej obsługi naruszeń ochrony danych występujących u Administratora
2.	• Przygotowywanie zawiadomień Prezesa Urzędu Ochrony Danych Osobowych (PUODO) oraz podmiotów danych o naruszeniu (w razie konieczności)

Zadanie:	• Realizacja procesu: obsługa naruszeń ochrony danych osobowych
• Czynności, które należy wykonać w celu realizacji zadania:	
3.	• Dokonywanie bieżących wpisów do rejestru naruszeń w zakresie nowych naruszeń występujących u Administratora
4.	• Odnotowywanie w rejestrze naruszeń wszelkich zmian wynikających ze sposobu zarządzania naruszeniem
5.	• Przygotowanie zaleceń dla Administratora w celu zapobiegania naruszeniom

Zadanie:	• Realizacja procesu: obsługa dostawców przetwarzających dane osobowe
• Czynności, które należy wykonać w celu realizacji zadania:	
1.	• Dokonywanie, zgodnie z obowiązującą procedurą, bieżącej weryfikacji potencjalnych dostawców zewnętrznych przetwarzających dane osobowe w imieniu Administratora
2.	• Dokonywanie bieżących wpisów do rejestru dostawców w zakresie nowych dostawców przetwarzających dane osobowe w imieniu Administratora
3.	• Odnotowywanie w rejestrze dostawców wszelkich zmian wynikających z charakteru współpracy z dostawcami
4.	• Zapewnianie bieżącego wsparcia w procesie negocjowania i zawierania umów powierzenia danych osobowych do przetwarzania

Zadanie:	• Realizacja procesu: prowadzenie analizy ryzyka (PIA)
• Czynności, które należy wykonać w celu realizacji zadania:	
1.	• Uczestniczenie, zgodnie z obowiązującą procedurą, w bieżącej analizie Privacy by Design
2.	• Uczestniczenie, zgodnie z obowiązującą procedurą, w procesie Preewaluacji ryzyka
3	• Uczestniczenie, zgodnie z obowiązującą procedurą, w ocenie skutków przetwarzania danych osobowych (DPIA)
4.	• Prowadzenie konsultacji z PUODO lub podmiotami danych, zgodnie z art. 36 RODO (w razie konieczności)

Zadanie:	• Realizacja procesu: wdrażanie osób nowozatrudnionych (onboarding)
• Czynności, które należy wykonać w celu realizacji zadania:	
1.	• Przeprowadzanie szkoleń obejmujących podstawowe zasady ochrony danych osobowych oraz procedury obowiązujące u Administratora dla każdej osoby nowozatrudnionej
2.	• Nadawanie upoważnień i dostępów w systemach informatycznych zgodnie z funkcją osoby nowozatrudnionej
3.	• Prowadzenie rejestru osób upoważnionych do przetwarzania danych osobowych

Zadanie:	• Realizacja procesu: podnoszenie kompetencji osób zatrudnionych
• Czynności, które należy wykonać w celu realizacji zadania:	
1.	• Ustalanie zapotrzebowania na podnoszenie wiedzy z zakresu danych osobowych w poszczególnych działach / departamentach funkcjonujących w organizacji Administratora
2.	• Opracowanie lub aktualizacja listy szkoleń dla poszczególnych obszarów w organizacji
3.	• Przeprowadzenie szkoleń w ustalonej z Administratorem formie

Zadanie:	• Realizacja procesu: współpraca z organem nadzorczym
• Czynności, które należy wykonać w celu realizacji zadania:	
1.	• Prowadzenie bieżącej korespondencji z Prezesem UODO (punkt kontaktowy)
2.	• Udział w czynnościach kontrolnych Prezesa UODO

Zadanie:	• Realizacja procesu: prowadzenie monitoringu prawnego
• Czynności, które należy wykonać w celu realizacji zadania:	
1.	• Dokonywanie bieżącej weryfikacji, czy nastąpiły zmiany w przepisach prawa z zakresu ochrony danych osobowych mające wpływ na funkcjonowanie organizacji Administratora (weryfikacja zmian w tekście RODO, weryfikacja zmian w przepisach sektorowych – ustawy krajowe)

Zadanie:	• Realizacja procesu: prowadzenie monitoringu prawnego
• Czynności, które należy wykonać w celu realizacji zadania:	
2.	• Dokonywanie bieżącej weryfikacji, czy zostały wydane wytyczne organów nadzoru lub orzecznictwo mające wpływ na funkcjonowanie organizacji Administratora (stanowiska Prezesa Urzędu Ochrony Danych Osobowych oraz innych organów nadzorczych w UE, stanowiska Europejskiej Rady Ochrony Danych, stanowiska Europejskiego Inspektora Ochrony Danych, orzecznictwo Trybunału Sprawiedliwości Unii Europejskiej, orzecznictwo krajowych sądów w państwach członkowskich UE)
3.	• W przypadku ustalenia, że zaszły zmiany w obowiązujących przepisach bądź zostały wydane wytyczne organów nadzoru lub orzeczenia sądu – podejmowanie decyzji, czy powinny zostać wdrożone niezwłocznie, czy zgodnie z harmonogramem dla zadań należących do obowiązków cyklicznych

B. ZADANIA CYKLICZNE

Zadanie:	• Weryfikacja procesów przetwarzania danych osobowych w obszarach krytycznych
• Czynności, które należy wykonać w celu realizacji zadania:	
1.	• Wdrożenie zmian w przepisach prawa mających wpływ na ocenę prawną przetwarzania danych w procesie – w zakresie, w jakim nie zostały wdrożone w ramach zadań należących do obowiązków stałych
2.	• Wdrożenie wydanych wytycznych organów nadzoru lub orzecznictwa mającego wpływ na ocenę prawną przetwarzania danych w procesie (stanowiska Prezesa Urzędu Ochrony Danych Osobowych oraz innych organów nadzorczych w UE, stanowiska Europejskiej Rady Ochrony Danych, stanowiska Europejskiego Inspektora Ochrony Danych, orzecznictwo Trybunału Sprawiedliwości Unii Europejskiej, orzecznictwo krajowych sądów w państwach członkowskich UE) – w zakresie, w jakim nie zostały wdrożone w ramach zadań należących do obowiązków stałych
3.	• Weryfikacja i aktualizacja klauzul zgód oraz informacyjnych stosowanych w procesie pod kątem kompletności i spójności (m.in. skrócone klauzule informacyjne, pełne klauzule informacyjne, polityka prywatności, polityka transparentności, regulaminy poszczególnych działań marketingowych)
4.	• Aktualizacja rejestru czynności przetwarzania (RCP) i rejestru kategorii czynności przetwarzania (RKCP) w zakresie weryfikowanych procesów

Zadanie:	• Weryfikacja procesów przetwarzania danych osobowych w pozostałych obszarach
• Czynności, które należy wykonać w celu realizacji zadania:	
1.	• Wdrożenie zmian w przepisach prawa mających wpływ na ocenę prawną przetwarzania danych w procesie – w zakresie, w jakim nie zostały wdrożone w ramach zadań należących do obowiązków stałych
2.	• Wdrożenie wydanych wytycznych organów nadzoru lub orzecznictwa mającego wpływ na ocenę prawną przetwarzania danych w procesie (stanowiska Prezesa Urzędu Ochrony Danych Osobowych oraz innych organów nadzorczych w UE, stanowiska Europejskiej Rady Ochrony Danych, stanowiska Europejskiego Inspektora Ochrony Danych, orzecznictwo Trybunału Sprawiedliwości Unii Europejskiej, orzecznictwo krajowych sądów w państwach członkowskich UE) – w zakresie, w jakim nie zostały wdrożone w ramach zadań należących do obowiązków stałych
3.	• Weryfikacja i aktualizacja klauzul zgód oraz informacyjnych stosowanych w procesie pod kątem kompletności i spójności (m.in. skrócone klauzule informacyjne, pełne klauzule informacyjne, polityka prywatności, polityka transparentności, regulaminy poszczególnych działań marketingowych)
4.	• Aktualizacja rejestru czynności przetwarzania (RCP) i rejestru kategorii czynności przetwarzania (RKCP) w zakresie weryfikowanych procesów

Zadanie:	• Weryfikacja procesu: obsługa wniosków podmiotów danych
• Czynności, które należy wykonać w celu realizacji zadania:	
1.	• Wdrożenie zmian w przepisach prawa mających wpływ na stosowaną w procesie procedurę w zakresie, w jakim nie zostały wdrożone w ramach zadań należących do obowiązków stałych
2.	• Wdrożenie wydanych wytycznych organów nadzoru lub orzecznictwa mającego wpływ na stosowaną w procesie procedurę (stanowiska Prezesa Urzędu Ochrony Danych Osobowych oraz innych organów nadzorczych w UE, stanowiska Europejskiej Rady Ochrony Danych, stanowiska Europejskiego Inspektora Ochrony Danych, orzecznictwo Trybunału Sprawiedliwości Unii Europejskiej, orzecznictwo krajowych sądów w państwach członkowskich UE) – w zakresie, w jakim nie zostały wdrożone w ramach zadań należących do obowiązków stałych
3.	• Ustalenie, czy procedura jest zgodna z najlepszymi praktykami rynkowymi (poradniki, publikacje itd.)
4.	• Zebranie informacji od osób odpowiedzialnych za realizację procedury na temat możliwej optymalizacji jej stosowania

Zadanie:	• Weryfikacja procesu: obsługa wniosków podmiotów danych
• Czynności, które należy wykonać w celu realizacji zadania:	
5.	• Przygotowanie i konsultacja propozycji zmian w procedurze z osobami odpowiedzialnymi za jej przestrzeganie lub zmian w sposobie jej realizacji (jeśli zachodzi taka konieczność)
6.	• Zapewnienie transferu wiedzy obejmującego zmiany w procedurze (przesłanie nowej procedury osobom zainteresowanym, szkolenie lub e-learning obejmujący wprowadzone zmiany)
7.	• Weryfikacja kompletności ewidencjonowanych wniosków w rejestrze (konsultacje z osobami odpowiedzialnymi za obsługę wniosków)
8.	• Weryfikacja spójności wpisów dokonywanych w rejestrze wniosków (granularność wpisów, stosowane słowniki)

Zadanie:	• Weryfikacja procesu: obsługa naruszeń ochrony danych osobowych
• Czynności, które należy wykonać w celu realizacji zadania:	
1.	• Wdrożenie zmian w przepisach prawa mających wpływ na stosowaną w procesie procedurę w zakresie, w jakim nie zostały wdrożone w ramach zadań należących do obowiązków stałych
2.	• Wdrożenie wydanych wytycznych organów nadzoru lub orzecznictwa mającego wpływ na stosowaną w procesie procedurę (stanowiska Prezesa Urzędu Ochrony Danych Osobowych oraz innych organów nadzorczych w UE, stanowiska Europejskiej Rady Ochrony Danych, stanowiska Europejskiego Inspektora Ochrony Danych, orzecznictwo Trybunału Sprawiedliwości Unii Europejskiej, orzecznictwo krajowych sądów w państwach członkowskich UE) – w zakresie, w jakim nie zostały wdrożone w ramach zadań należących do obowiązków stałych
3.	• Ustalenie, czy procedura jest zgodna z najlepszymi praktykami rynkowymi (poradniki, publikacje itd.)
4.	• Zebranie informacji od osób odpowiedzialnych za realizację procedury na temat możliwej optymalizacji jej stosowania
5.	• Przygotowanie i konsultacja propozycji zmian w procedurze z osobami odpowiedzialnymi za jej przestrzeganie lub zmian w sposobie jej realizacji (jeśli zachodzi taka konieczność)
6.	• Zapewnienie transferu wiedzy obejmującego zmiany w procedurze (np. przesłanie nowej procedury osobom zainteresowanym, szkolenie lub e-learning obejmujący wprowadzone zmiany)

Zadanie:	• Weryfikacja procesu: obsługa naruszeń ochrony danych osobowych
• Czynności, które należy wykonać w celu realizacji zadania:	
7.	• Weryfikacja kompletności ewidencjonowanych naruszeń w rejestrze (konsultacje z osobami odpowiedzialnymi za obsługę wniosków)
8.	• Weryfikacja spójności wpisów dokonywanych w rejestrze naruszeń (granularność wpisów, stosowane słowniki)

Zadanie:	• Weryfikacja procesu: obsługa dostawców przetwarzających dane osobowe
• Czynności, które należy wykonać w celu realizacji zadania:	
1.	• Wdrożenie zmian w przepisach prawa mających wpływ na stosowaną w procesie procedurę w zakresie, w jakim nie zostały wdrożone w ramach zadań należących do obowiązków stałych
2.	• Wdrożenie wydanych wytycznych organów nadzoru lub orzecznictwa mającego wpływ na stosowaną w procesie procedurę (stanowiska Prezesa Urzędu Ochrony Danych Osobowych oraz innych organów nadzorczych w UE, stanowiska Europejskiej Rady Ochrony Danych, stanowiska Europejskiego Inspektora Ochrony Danych, orzecznictwo Trybunału Sprawiedliwości Unii Europejskiej, orzecznictwo krajowych sądów w państwach członkowskich UE) – w zakresie, w jakim nie zostały wdrożone w ramach zadań należących do obowiązków stałych
3.	• Ustalenie, czy procedura jest zgodna z najlepszymi praktykami rynkowymi (poradniki, publikacje itd.)
4.	• Zebranie informacji od osób odpowiedzialnych za realizację procedury na temat możliwej optymalizacji jej stosowania
5.	• Przygotowanie i konsultacja propozycji zmian w procedurze z osobami odpowiedzialnymi za jej przestrzeganie lub zmian w sposobie jej realizacji (jeśli zachodzi taka konieczność)
6.	• Zapewnienie transferu wiedzy obejmującego zmiany w procedurze (np. przesłanie nowej procedury osobom zainteresowanym, szkolenie lub e-learning obejmujący wprowadzone zmiany)
7.	• Weryfikacja kompletności ewidencjonowanych wpisów w rejestrze dostawców (konsultacje z osobami odpowiedzialnymi za obsługę wniosków)
8.	• Weryfikacja spójności wpisów dokonywanych w rejestrze dostawców (granularność wpisów, stosowane słowniki)

Zadanie:	• Weryfikacja procesu: prowadzenie analizy ryzyka (PIA)
• Czynności, które należy wykonać w celu realizacji zadania:	
1.	• Wdrożenie zmian w przepisach prawa mających wpływ na stosowaną w procesie procedurę w zakresie, w jakim nie zostały wdrożone w ramach zadań należących do obowiązków stałych
2.	• Wdrożenie wydanych wytycznych organów nadzoru lub orzecznictwa mającego wpływ na stosowaną w procesie procedurę (stanowiska Prezesa Urzędu Ochrony Danych Osobowych oraz innych organów nadzorczych w UE, stanowiska Europejskiej Rady Ochrony Danych, stanowiska Europejskiego Inspektora Ochrony Danych, orzecznictwo Trybunału Sprawiedliwości Unii Europejskiej, orzecznictwo krajowych sądów w państwach członkowskich UE) – w zakresie, w jakim nie zostały wdrożone w ramach zadań należących do obowiązków stałych
3.	• Ustalenie, czy procedura jest zgodna z najlepszymi praktykami rynkowymi (poradniki, publikacje itd.)
4.	• Zebranie informacji od osób odpowiedzialnych za realizację procedury na temat możliwej optymalizacji jej stosowania
5.	• Przygotowanie i konsultacja propozycji zmian w procedurze z osobami odpowiedzialnymi za jej przestrzeganie lub zmian w sposobie jej realizacji (jeśli zachodzi taka konieczność)
6.	• Zapewnienie transferu wiedzy obejmującego zmiany w procedurze (np. przesłanie nowej procedury osobom zainteresowanym, szkolenie lub e-learning obejmujący wprowadzone zmiany)

Zadanie:	• Weryfikacja procesu: zapewnianie retencji danych
• Czynności, które należy wykonać w celu realizacji zadania:	
1.	• Wdrożenie zmian w przepisach prawa mających wpływ na stosowaną w procesie procedurę w zakresie, w jakim nie zostały wdrożone w ramach zadań należących do obowiązków stałych
2.	• Wdrożenie wydanych wytycznych organów nadzoru lub orzecznictwa mającego wpływ na stosowaną w procesie procedurę (stanowiska Prezesa Urzędu Ochrony Danych Osobowych oraz innych organów nadzorczych w UE, stanowiska Europejskiej Rady Ochrony Danych, stanowiska Europejskiego Inspektora Ochrony Danych, orzecznictwo Trybunału Sprawiedliwości Unii Europejskiej, orzecznictwo krajowych sądów w państwach członkowskich UE) – w zakresie, w jakim nie zostały wdrożone w ramach zadań należących do obowiązków stałych

Zadanie:	• Weryfikacja procesu: zapewnianie retencji danych
• Czynności, które należy wykonać w celu realizacji zadania:	
3.	• Ustalenie, czy procedura jest zgodna z najlepszymi praktykami rynkowymi (poradniki, publikacje itd.)
4.	• Zebranie informacji od osób odpowiedzialnych za realizację procedury na temat możliwej optymalizacji jej stosowania
5.	• Przygotowanie i konsultacja propozycji zmian w procedurze z osobami odpowiedzialnymi za jej przestrzeganie lub zmian w sposobie jej realizacji (jeśli zachodzi taka konieczność)
6.	• Zapewnienie transferu wiedzy obejmującego zmiany w procedurze (np. przesłanie nowej procedury osobom zainteresowanym, szkolenie lub e-learning obejmujący wprowadzone zmiany)

Załącznik nr 3 – Wzór raportu

RAPORT KWARTALNY ZA OKRES ….

RAPORT Z REALIZACJI ZADAŃ STAŁYCH

Lista zadań	Zrealizowane czynności	Uwagi
Realizacja procesu: prowadzenie RCP oraz RKCP	•	•
Realizacja procesu: obsługa wniosków podmiotów danych	•	•
Realizacja procesu: obsługa naruszeń ochrony danych osobowych	•	•
Realizacja procesu: obsługa dostawców przetwarzających dane osobowe	•	•
Realizacja procesu: prowadzenie analizy ryzyka (PIA)	•	•
Realizacja procesu: wdrażanie osób nowozatrudnionych (onboarding)	•	•

Lista zadań	Zrealizowane czynności	Uwagi
Realizacja procesu: podnoszenie kompetencji osób zatrudnionych	•	•
Realizacja procesu: współpraca z organem nadzorczym	•	•
Realizacja procesu: prowadzenie monitoringu prawnego	•	•

RAPORT Z REALIZACJI ZADAŃ CYKLICZNYCH

Lista zadań	Czy realizacja zadania była planowana?	Zrealizowane czynności	Uwagi (w tym przyczyny braku realizacji zaplanowanych zadań)
• Weryfikacja procesów przetwarzania danych osobowych w obszarach krytycznych	•	•	•
• Weryfikacja procesów przetwarzania danych osobowych w pozostałych obszarach	•	•	•
• Weryfikacja procesu: obsługa wniosków podmiotów danych	•	•	•
• Weryfikacja procesu: obsługa naruszeń ochrony danych osobowych	•	•	•

Lista zadań	Czy realizacja zadania była planowana?	Zrealizowane czynności	Uwagi (w tym przyczyny braku realizacji zaplanowanych zadań)
• Weryfikacja procesu: obsługa dostawców przetwarzających dane osobowe	•	•	•
• Weryfikacja procesu: prowadzenie analizy ryzyka (PIA)	•	•	•
• Weryfikacja procesu: zapewnianie retencji danych	•	•	•

Data sporządzenia raportu:

Podpis: