Załącznik nr 1 do Zarządzenia nr 184/2023
Wójta Gminy Bałtów
z dnia 28 grudnia 2023r.

POLITYKA BEZPIECZEŃSTWA
PRZETWARZANIA DANYCH OSOBOWYCH
W URZĘDZIE GMINY
W BAŁTOWIE

Spis treści

Rozdział I. Postanowienia ogólne. 3
Rozdział II. Skróty i definicje. 3
Rozdział III. Zasady przetwarzania danych osobowych i strategia bezpieczeństwa. 5
Rozdział IV. System ochrony danych osobowych. 5
Rozdział V. Inspektor Ochrony Danych. 6
Rozdział VI. Rejestr czynności przetwarzania danych. 6
Rozdział VII. Umowa powierzenia przetwarzania danych osobowych. 7
Rozdział VIII. Upoważnienia. 7
Rozdział IX. Obowiązek informacyjny. 8
Rozdział X. Obsługa praw jednostki. 9
Rozdział XI. Środki techniczne i organizacyjne zapewniające bezpieczeństwo danych. 11
Rozdział XII. Zasady korzystania z poczty elektronicznej. 13
Rozdział XIII. Obsługa naruszeń. 14
Rozdział XIV. Postanowienia końcowe. 16
Załącznik nr 1 Rejestr czynności przetwarzania 17
Załącznik nr 2 Umowa powierzenia danych do przetwarzania 19
Załącznik nr 3 Wykaz podmiotów, którym powierzono dane osobowe do przetwarzania 23
Załącznik nr 4 Rejestr kategorii przetwarzania 24
Załącznik nr 5 Upoważnienie do przetwarzania danych osobowych 26
Załącznik nr 6 Odwołanie upoważnienia do przetwarzania danych osobowych 27
Załącznik nr 7 Ewidencja upoważnień do przetwarzania danych osobowych 28
Załącznik nr 8 Rejestr realizacji żądań 29
Załącznik nr 9 Oświadczenie o zachowaniu poufności 31
Załącznik nr 10 Raport o naruszeniu danych osobowych 32
Załącznik nr 11 Rejestr naruszeń 34

Rozdział I. Postanowienia ogólne.

Polityka bezpieczeństwa przetwarzania danych osobowych w Urzędzie Gminy w Bałtowie zwana dalej "Polityką" lub „Polityką bezpieczeństwa" jest dokumentem wewnętrznym opracowanym w celu ustalenia zasad postępowania w procesach przetwarzania danych osobowych oraz ochrony interesów osób fizycznych, których dane są lub mogą być przetwarzane. Polityka została opracowana na podstawie i w celu spełnienia wymagań rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/676 z dnia 27 kwietnia 2016 roku w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych) (Dz. Urz. UE L 119, s. 1 ze zm.). oraz ustawy z dnia 10 maja 2018 r. o ochronie danych osobowych (Dz. U. z 2019 r. poz. 1781).
Polityka stanowi jeden ze środków organizacyjnych mających na celu wykazanie, że przetwarzanie danych osobowych odbywa się zgodnie z powyższym rozporządzeniem. Polityka, jest dokumentem, którego celem jest określenie zasad i sposobów dotyczących zapewnienia bezpieczeństwa danych osobowych poprzez zapewnienie ich poufności, integralności i dostępności, w tym w szczególności, aby dane te były przetwarzane zgodnie z prawem, zbierane dla oznaczonych, zgodnych z prawem celów i niepoddawane przetwarzaniu niezgodnemu z tymi celami, merytorycznie poprawne i adekwatne w stosunku do celów, w jakim są przetwarzane, przechowywane w postaci umożliwiającej identyfikację osób, których dotyczą, nie dłużej niż jest to niezbędne do osiągnięcia celu przetwarzania.
Polityka Bezpieczeństwa określa zasady postępowania z danymi osobowymi przetwarzanymi w całym obszarze przetwarzania danych osobowych w Urzędzie Gminy w Bałtowie, we wszystkich lokalizacjach, budynkach, pomieszczeniach, ma zastosowanie do wszystkich istniejących, wdrażanych obecnie lub w przyszłości systemów przetwarzania informacji zawierających dane osobowe, w tym systemów IT oraz zobowiązuje wszystkie osoby świadczące pracę lub wykonujące czynności na rzecz Urzędu Gminy w Bałtowie, posiadające dostęp do informacji podlegających ochronie do przestrzegania jej postanowień.

Rozdział II. Skróty i definicje.

RODO – rozporządzenie Parlamentu Europejskiego i Rady (UE) 2016/679 w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia Dyrektywy 95/46 z dnia 27 kwietnia 2016 r. (ogólne rozporządzenie o ochronie danych) (Dz. U. UE. L. z 2016 r. Nr 119, str. 1; zm.: Dz. U. UE. L. z 2018 r. Nr 127, str. 2 oraz z 2021 r. Nr 74, str. 35).
Ustawa - ustawa z dnia 10 maja 2018 r. o ochronie danych osobowych (Dz. U. z 2019 r. poz. 1781).
Administrator Danych Osobowych (ADO) - osoba fizyczna lub prawna, organ publiczny, jednostka lub inny podmiot, który samodzielnie lub wspólnie z innymi ustala cele i sposoby przetwarzania danych osobowych.
Inspektor Ochrony Danych (IOD) - osoba wyznaczona przez Administratora Danych Osobowych do monitorowania przestrzegania zasad ochrony danych osobowych, informowania administratora o obowiązkach spoczywających na nim, na mocy przepisów dotyczących ochrony danych osobowych, udzielania na żądanie zaleceń co do oceny skutków dla ochrony danych, współpracy z organem nadzorczym oraz pełnienia funkcji punktu kontaktowego dla organu nadzorczego w kwestiach związanych z przetwarzaniem danych osobowych.

Administrator Systemów Informatycznych (ASI) - osoba fizyczna wyznaczona przez Administratora Danych Osobowych, zajmująca się bezpieczeństwem organizacyjnym, fizycznym i technicznym danych osobowych przetwarzanych w systemie informatycznym.

Dane osobowe - informacje o zidentyfikowanej lub możliwej do zidentyfikowania osobie fizycznej. Osobą możliwą do zidentyfikowania jest osoba, którą można bezpośrednio lub pośrednio zidentyfikować, w szczególności na podstawie identyfikatora takiego jak imię i nazwisko, numer identyfikacyjny, dane o lokalizacji, identyfikator internetowy lub jeden bądź kilka szczególnych czynników określających fizyczną, fizjologiczną, genetyczną, psychiczną, ekonomiczną, kulturową lub społeczną tożsamość osoby fizycznej.

Przetwarzanie danych osobowych - zautomatyzowana lub niezautomatyzowana operacja lub zestaw operacji wykonywanych na danych osobowych, obejmuje m.in. zbieranie, rejestrowanie, organizowanie, strukturyzowanie, przechowywanie, adaptację lub zmianę, wyszukiwanie, konsultacje, wykorzystanie, ujawnianie poprzez transmisję, rozpowszechnianie lub udostępnianie w inny sposób, łączenie, ograniczenie, usunięcie lub niszczenie danych osobowych.

Zgoda osoby, której dane dotyczą - dobrowolne, konkretne, świadome i jednoznaczne wskazanie osoby, której dane dotyczą, za pomocą oświadczenia lub wyraźnego działania potwierdzającego, wyrażającego zgodę na przetwarzanie danych osobowych z nim związanych.

Podmiot danych - osoba fizyczna, której dane osobowe są przetwarzane.

Odbiorca - osoba fizyczna lub prawna, organ publiczny, jednostka lub inny podmiot, któremu ujawnia się dane osobowe, niezależnie od tego, czy jest stroną trzecią.

Podmiot przetwarzający (**Procesor)** - osoba fizyczna lub prawna, organ publiczny lub jakikolwiek inny organ przetwarzający dane osobowe w imieniu administratora.

Szczególne kategorie danych osobowych – dane ujawniające pochodzenie rasowe lub etniczne, poglądy polityczne, przekonania religijne lub filozoficzne, członkostwo w związkach zawodowych, dane genetyczne, dane biometryczne w celu jednoznacznej identyfikacji osoby fizycznej, dane dotyczące zdrowia, dane dotyczące życia seksualnego osoby, seksualności lub orientacji seksualnej.

Naruszenie ochrony danych osobowych - przypadkowy lub niezgodny z prawem incydent prowadzący do zniszczenia, utracenia, zmodyfikowania, nieuprawnionego ujawnienia lub nieuprawnionego dostępu do danych osobowych.

Prezes Urzędu Ochrony Danych Osobowych (Prezes UODO) –organ nadzorczy w kwestiach ochrony danych osobowych.

Bezpieczeństwo informacji - zachowanie poufności, integralności i dostępności informacji.

Użytkownik - osoba upoważniona do przetwarzania danych osobowych, której nadano identyfikator i przyznano hasło.

Identyfikator/login - ciąg znaków literowych, jednoznacznie identyfikujący osobę upoważnioną do przetwarzania danych osobowych w systemie informatycznym**.**

Hasło - ciąg znaków alfanumerycznych, używany w celu potwierdzenia tożsamości podczas logowania się do systemu, znany jedynie użytkownikowi.

Uwierzytelnienie - działanie, którego celem jest weryfikacja deklarowanej tożsamości podmiotu.

Obszar przetwarzania danych - budynki i pomieszczenia administratora, tworzące obszar, w którym przetwarzane są dane osobowe i inne informacje prawem chronione.

System informatyczny administratora/system IT - sprzęt komputerowy, oprogramowanie, dane eksploatowane w zespole współpracujących ze sobą urządzeń, programów, procedur przetwarzania informacji i narzędzi programowych; w systemie tym pracuje co najmniej jeden komputer centralny i system ten tworzy sieć teleinformatyczną administratora danych.

Rozdział III. Zasady przetwarzania danych osobowych i strategia bezpieczeństwa.

Urząd Gminy w Bałtowie przetwarza dane osobowe z poszanowaniem następujących zasad:

1. zasady zgodności z prawem, rzetelności i przejrzystości, przetwarza dane zgodnie z prawem, rzetelnie i w sposób przejrzysty dla osoby, której dane dotyczą;
2. zasady ograniczenia celu, zbiera dane tylko w konkretnych, wyraźnych i prawnie uzasadnionych celach i nie przetwarza dalej w sposób niezgodny z tymi celami;
3. zasady minimalizacji danych (adekwatności), przetwarza dane stosowne oraz ograniczone do tego, co jest niezbędne do celów, w których są przetwarzane;
4. zasady prawidłowości, przetwarza dane prawidłowe, w razie potrzeby uaktualnia je, podejmuje wszelkie rozsądne działania, aby dane osobowe, które są nieprawidłowe w świetle celów ich przetwarzania, zostały niezwłocznie usunięte lub sprostowane;
5. zasady ograniczenia przechowywania, przechowuje dane w formie umożliwiającej identyfikację osoby, której dane dotyczą, przez okres nie dłuższy, niż jest to niezbędne do celów, w których dane te są przetwarzane;
6. zasady integralności i poufności, dane przetwarzane są w sposób zapewniający ich odpowiednie bezpieczeństwo, w tym ochronę przed niedozwolonym lub niezgodnym z prawem przetwarzaniem oraz przypadkową utratą, zniszczeniem lub uszkodzeniem, za pomocą odpowiednich środków technicznych i organizacyjnych.

Powyższe zasady ochrony danych osobowych mają zastosowanie do wszystkich istniejących, wdrażanych obecnie lub w przyszłości czynności przetwarzania danych osobowych, systemów przetwarzania informacji zawierających dane osobowe, w tym systemów IT, wszystkich lokalizacji, budynków, pomieszczeń, w których są lub będą przetwarzane informacje podlegające ochronie oraz wszystkich osób świadczących pracę lub wykonujących czynności na rzecz Urzędu Gminy w Bałtowie mających dostęp do danych osobowych i informacji podlegających ochronie.

Rozdział IV. System ochrony danych osobowych.

System ochrony danych osobowych Urzędu Gminy w Bałtowie obejmuje w szczególności następujące elementy:

1. wyznaczenie Inspektora Ochrony Danych;
2. rejestrowanie czynności przetwarzania danych;
3. umowy powierzenia przetwarzania danych osobowych;
4. upoważnienia;
5. postępowanie dotyczące przetwarzania danych osobowych na podstawie zgody podmiotu danych;
6. obowiązek informacyjny;
7. obsługę praw jednostki;
8. środki techniczne i organizacyjne zapewniające bezpieczeństwo danych;
9. obsługę incydentów i naruszeń.

Rozdział V. Inspektor Ochrony Danych.

Urząd Gminy w Bałtowie wyznacza Inspektora Ochrony Danych na podstawie kwalifikacji zawodowych, a w szczególności wiedzy fachowej na temat prawa i praktyk w dziedzinie ochrony danych oraz umiejętności wypełnienia zadań, o których mowa w art. 39 RODO oraz publikuje jego dane kontaktowe na stronie internetowej ośrodka i zawiadamia o nich organ nadzorczy.
Do zadań Inspektora Ochrony Danych w szczególności należy:

- informowanie administratora oraz pracowników administratora, którzy przetwarzają dane osobowe, o obowiązkach spoczywających na nich na mocy przepisów RODO i innych przepisów o ochronie danych i doradzanie im w tej sprawie;
- monitorowanie przestrzegania RODO i innych przepisów o ochronie danych oraz polityk administratora w dziedzinie ochrony danych osobowych;
- podejmowanie działań zwiększających świadomość personelu w zakresie ochrony danych;
- udzielanie na żądanie zaleceń co do oceny skutków dla ochrony danych oraz monitorowanie jej wykonania;
- współpraca z Prezesem Urzędu Ochrony Danych Osobowych;
- pełnienie funkcji punktu kontaktowego dla Prezesa Urzędu Ochrony Danych Osobowych w kwestiach związanych z przetwarzaniem, w tym z uprzednimi konsultacjami;
- pełnienie roli punktu kontaktowego dla osób, których dane dotyczą, w sprawach związanych z przetwarzaniem ich danych osobowych oraz z wykonywaniem praw przysługujących im na mocy RODO.

Rozdział VI. Rejestr czynności przetwarzania danych.

Urząd Gminy w Bałtowie opracowuje, prowadzi i uaktualnia rejestr czynności przetwarzania danych osobowych. Rejestr jest narzędziem rozliczalności ochrony danych osobowych. Administrator inwentaryzuje w nim i monitoruje sposób, w jaki przetwarza dane osobowe.
W rejestrze czynności przetwarzania danych osobowych zamieszcza się następujące informacje:

- nazwę oraz dane kontaktowe administratora;
- nazwę oraz dane kontaktowe współadministratorów;
- imię i nazwisko oraz dane kontaktowe Inspektora Ochrony Danych;
- cele przetwarzania;
- opis kategorii osób, których dane dotyczą;
- opis kategorii danych osobowych;
- kategorie odbiorców, którym dane osobowe zostały lub zostaną ujawnione;
- informacje o przekazaniu danych osobowych do państwa trzeciego lub organizacji międzynarodowej, gdy ma to zastosowanie;
- planowane terminy usunięcia poszczególnych kategorii danych, jeżeli jest to możliwe;
- opis technicznych i organizacyjnych środków bezpieczeństwa, jeżeli jest to możliwe.

Urząd Gminy w Bałtowie prowadzi rejestr zgodnie z załącznikiem nr 1 Rejestr czynności przetwarzania. Kierownicy referatów oraz pracownicy zatrudnieni na samodzielnych stanowiskach zobowiązani są przed rozpoczęciem przetwarzania danych osobowych w każdej nowej czynności przetwarzania zgłosić ją do inspektora ochrony danych oraz podać ww. informacje dotyczące przetwarzania danych. Rejestr czynności przetwarzania prowadzi inspektor ochrony danych.

Rozdział VII. Umowa powierzenia przetwarzania danych osobowych.

Urząd Gminy w Bałtowie dobiera i weryfikuje przetwarzających dane osobowe na jego rzecz w celu zapewnienia, aby przetwarzający dawał wystarczające gwarancje wdrożenia odpowiednich środków organizacyjnych i technicznych dla zapewnienia bezpieczeństwa, realizacji praw jednostki i innych obowiązków ochrony danych spoczywających na administratorze. Do przetwarzania powierzonych danych osobowych mogą być jedynie dopuszczeni pracownicy podmiotów współpracujących lub świadczących usługi na rzecz Urzędu Gminy w Bałtowie w zakresie adekwatnym do celu powierzenia. W przypadku powierzenia przetwarzania danych do podmiotu przetwarzającego, Urząd Gminy w Bałtowie jest zobowiązany do sporządzenia z nim umowy powierzenia. Umowa powierzenia określa przedmiot i czas trwania przetwarzania, zakres, charakter i cel przetwarzania, rodzaj danych osobowych, kategorie osób, których dane dotyczą, obowiązki i prawa stron umowy**.** Wzór umowy powierzenia danych do przetwarzania stanowi załącznik nr 2 Umowa powierzenia danych do przetwarzania. Administrator prowadzi wykaz podmiotów, którym powierzono dane osobowe do przetwarzania. Wzór wykazu stanowi załącznik nr 3 Wykaz podmiotów, którym powierzono dane osobowe do przetwarzania. Za prowadzenie wykazu odpowiedzialny jest kierownik.
W przypadku powierzenia danych przez innego administratora do przetwarzania, Procesor, którym będzie Urząd Gminy w Bałtowie prowadzi Rejestr kategorii przetwarzania. Wzór rejestru stanowi załącznik nr 4 Rejestr kategorii przetwarzania. Umowa powierzenia danych do przetwarzania musi być zawarta.

Rozdział VIII. Upoważnienia.

Pracownicy i osoby współpracujące z Urzędem Gminy w Bałtowie, mogą przetwarzać dane osobowe na rzecz administratora tylko z jego upoważnienia i na jego polecenie.
W przypadku zatrudnienia osoby lub rozpoczęcia przez nią współpracy z Urzędem Gminy w Bałtowie w ramach umowy zlecenia, wolontariatu, stażu czy praktyk, przed dopuszczeniem tej osoby do przetwarzania danych osobowych pracownik zatrudniony na stanowisku ds. pracowniczych, w porozumieniu z bezpośrednim przełożonym tej osoby przygotowuje projekt upoważnienia do przetwarzania danych osobowych dla wskazanej osoby i przedkłada go administratorowi.
Po wystąpieniu zmian mających wpływ na treść upoważnienia, w szczególności w przypadku zmiany obowiązków osoby upoważnionej, upoważnienie jest zmieniane niezwłocznie poprzez odwołanie dotychczasowego upoważnienia i wydanie nowego upoważnienia. Upoważnienie jest odwoływane niezwłocznie po zakończeniu współpracy z osobą upoważnioną, jeżeli nastąpiła przed końcem okresu obowiązywania upoważnienia lub upoważnienie zostało nadane bez wskazania daty końcowej jego obowiązywania. Upoważnienie jest odwoływane także w sytuacji, gdy dalsze przetwarzanie danych osobowych nie będzie miało miejsca. W przypadku dłuższej nieobecności pracownika w pracy, spowodowanej w szczególności chorobą, urlopem bezpłatnym, trwającej powyżej 3 miesięcy upoważnienie jest odwoływane. Projekt odwołania upoważnienia przygotowuje pracownik ds. pracowniczych, w porozumieniu z bezpośrednim przełożonym wskazanej osoby i przedkłada go administratorowi.
W przypadku przetwarzania danych osobowych w ramach prac komisji powoływanych przez administratora projekt upoważnienia oraz projekt odwołania upoważnienia przygotowuje przewodniczący komisji oraz przedkłada go administratorowi. Upoważnienie zawiera oznaczenie administratora, imię i nazwisko oraz stanowisko służbowe osoby upoważnianej, okres jego

obowiązywania oraz określa czynności przetwarzania danych osobowych i ich zakres, do których wykonywania upoważniony jest uprawniony.
Upoważnienie do przetwarzania danych i odwołanie upoważnienia sporządzane jest w formie pisemnej, w dwóch egzemplarzach, jeden dla administratora, drugi dla osoby upoważnionej. Podpisane przez administratora upoważnienie do przetwarzania danych lub odwołanie upoważnienia do przetwarzania danych jest niezwłocznie przekazywane osobie upoważnionej bądź osobie, której odwołano upoważnienie. Osoba upoważniona przyjmuje upoważnienie, co potwierdza złożeniem podpisu na upoważnieniu.
Wzór upoważnienia do przetwarzania danych osobowych stanowi Załącznik nr 5 Upoważnienie do przetwarzania danych osobowych. Wzór odwołania upoważnienia do przetwarzania danych osobowych stanowi Załącznik nr 6 Odwołanie upoważnienia do przetwarzania danych osobowych. Pracownik zatrudniony na stanowisku ds. pracowniczych odnotowuje upoważnienie oraz odwołanie upoważnienia w ewidencji upoważnień do przetwarzania danych osobowych. Upoważnienie oraz odwołanie upoważnienia przechowywane są razem z ewidencją upoważnień do przetwarzania danych osobowych, którą w Urzędzie Gminy w Bałtowie prowadzi pracownik zatrudniony na stanowisku ds. pracowniczych zgodnie z wzorem ewidencji stanowiącej załącznik nr 7 Ewidencja osób upoważnionych do przetwarzania danych.

Rozdział IX. Obowiązek informacyjny.

Urząd Gminy w Bałtowie określa zgodne z prawem i efektywne sposoby wykonywania obowiązków informacyjnych.
Urząd Gminy w Bałtowie spełnia obowiązki informacyjne względem osób, których dane przetwarza. Przekazuje osobom wymagane prawem informacje dotyczące przetwarzania danych przez administratora, zgodnie z art. 13 i 14 RODO.
Administrator podczas pozyskiwania danych osobowych podaje osobie, której dane przetwarza następujące informacje:

1. swoją tożsamość i dane kontaktowe;
2. dane kontaktowe inspektora ochrony danych;
3. cele przetwarzania danych osobowych oraz podstawę prawną przetwarzania;
4. jeżeli przetwarzanie odbywa się na podstawie art. 6 ust. 1 lit. e lub f RODO – prawnie uzasadnione interesy realizowane przez administratora lub przez stronę trzecią;
5. okres, przez który dane osobowe będą przechowywane, a gdy nie jest to możliwe, kryteria ustalania tego okresu;
6. o odbiorcach danych osobowych lub o kategoriach odbiorców, jeżeli istnieją;
7. o zamiarze przekazania danych osobowych do państwa trzeciego lub organizacji międzynarodowej;
8. o prawie do żądania od administratora dostępu do danych osobowych dotyczących osoby, której dane dotyczą, ich sprostowania, usunięcia lub ograniczenia przetwarzania, a także o prawie do przenoszenia danych;
9. o prawie do wniesienia sprzeciwu wobec przetwarzania;
10. o prawie do cofnięcia zgody w dowolnym momencie bez wpływu na zgodność z prawem przetwarzania, którego dokonano na podstawie zgody przed jej cofnięciem, jeżeli przetwarzanie odbywa się na podstawie wyrażonej zgody;
11. o prawie wniesienia skargi do organu nadzorczego;

12. o konieczności bądź dobrowolności podania danych, informuje czy podanie danych osobowych jest wymogiem ustawowym lub umownym lub warunkiem zawarcia umowy oraz czy osoba, której dane dotyczą, jest zobowiązana do ich podania i jakie są ewentualne konsekwencje niepodania danych lub o źródle pochodzenia danych, gdy dane osobowe pozyskane zostały w sposób inny niż od osoby, której dane są przetwarzane;
13. o zautomatyzowanym podejmowaniu decyzji, w tym o profilowaniu.

Administrator podczas pozyskiwania danych osobowych w sposób inny niż od osoby, której dane przetwarza, podaje osobie informacje dotyczące przetwarzania jej danych, najpóźniej w ciągu miesiąca od pozyskania danych osobowych lub jeżeli dane osobowe mają być stosowane do komunikacji z osobą, której dane dotyczą - najpóźniej przy pierwszej komunikacji z tą osobą, lub jeżeli planuje ujawnić dane osobowe innemu odbiorcy - najpóźniej przy ich pierwszym ujawnieniu.

Rozdział X. Obsługa praw jednostki.

Urząd Gminy w Bałtowie zapewnia obsługę praw osób, których dane przetwarza. Realizując otrzymane w tym zakresie żądania ułatwia osobom korzystanie z ich praw, weryfikuje i zapewnia możliwość efektywnego wykonania każdego typu żądania przez siebie i swoich przetwarzających. Zapewnia odpowiednie procedury, aby żądania osób były realizowane w terminach i w sposób wymagany przez RODO i odpowiednio dokumentowane. Stosuje procedury pozwalające na ustalenie konieczności zawiadomienia osób dotkniętych zidentyfikowanym naruszeniem ochrony danych oraz bez zbędnej zwłoki zawiadamia osobę o naruszeniu ochrony danych osobowych, jeżeli może ono powodować wysokie ryzyko naruszenia praw lub wolności tej osoby.

Osoba, której dane dotyczą ma prawo:

1. dostępu do danych;
   Na żądanie osoby dotyczące dostępu do jej danych, Urząd Gminy w Bałtowie informuje osobę, czy przetwarza jej dane oraz informuje osobę o szczegółach przetwarzania, zgodnie z art. 15 RODO, a także udziela osobie dostępu do danych jej dotyczących. Dostęp do danych może być zrealizowany przez wydanie kopii danych. Urząd Gminy w Bałtowie odnotowuje fakt wydania pierwszej kopii danych.
2. sprostowania danych;
   Na żądanie osoby dotyczące sprostowania nieprawidłowych danych Urząd Gminy w Bałtowie dokonuje sprostowania danych. Administrator ma prawo odmówić sprostowania danych, chyba że osoba w rozsądny sposób wykaże nieprawidłowości danych, których sprostowania się domaga. W przypadku sprostowania danych Administrator informuje osobę o odbiorcach danych, na żądanie tej osoby.
3. usuwania danych;
   Urząd Gminy w Bałtowie usuwa dane osobowe, gdy dane te nie są niezbędne do celów, w których zostały zebrane ani nie są przetwarzane w innych celach, zgoda na ich przetwarzanie została cofnięta i nie ma innej podstawy prawnej przetwarzania, osoba wniosła skuteczny sprzeciw względem przetwarzania tych danych, dane były przetwarzane niezgodnie z prawem bądź konieczność usunięcia wynika z obowiązku prawnego.
4. ograniczenia przetwarzania;
   Urząd Gminy w Bałtowie ogranicza przetwarzanie danych osobowych poprzez, między innymi czasowe przeniesienie wybranych danych osobowych do innego systemu przetwarzania,

uniemożliwienie użytkownikom dostępu do wybranych danych lub czasowe usunięcie opublikowanych danych ze strony internetowej i mediów społecznościowych.

5. przenoszenia danych;
   Prawo do przenoszenia danych przysługuje wyłącznie, gdy dane osobowe są przetwarzane w sposób zautomatyzowany w celu zawarcia lub realizacji umowy (dane strony umowy) lub na podstawie zgody.
6. prawo do sprzeciwu;

Urząd Gminy w Bałtowie analizuje możliwość i zakres dalszego przetwarzania danych. W przypadku braku podstawy przetwarzania danych, dane osobowe usuwa w zakresie w jakim brak podstawy.

Urząd Gminy w Bałtowie przyjmuje następujące sposoby zgłaszania żądań wskazanych w art. 15-22 RODO, a także wniosków o wycofanie zgody:

- na adres mailowy administratora: gmina@gminabaltow.pl;
- na adres mailowy inspektora ochrony danych: iod@gminabaltow.pl;
- osobiście w siedzibie administratora: Urząd Gminy w Bałtowie, Bałtów 32, 27-423 Bałtów;
- listownie na adres administratora: Urząd Gminy w Bałtowie, Bałtów 32, 27-423 Bałtów.

Administrator ewidencjonuje wszelkie żądania podmiotów danych w rejestrze realizacji żądań stanowiącym załącznik nr 8 Rejestr realizacji żądań.

Inspektor ochrony danych prowadzi rejestr żądań i odnotowuje w nim każde żądanie, w szczególności: datę, treść i sposób wpływu, sposób udzielenia odpowiedzi na żądanie, a także sposób i termin spełnienia obowiązku.

Każdy pracownik do którego trafi żądanie w ramach praw podmiotu jest zobowiązany do niezwłocznego poinformowania o tym inspektora ochrony danych i przekazania mu treści żądania w celu oceny żądania pod kątem zgodności z przepisami RODO.

Inspektor Ochrony Danych weryfikuje tożsamość osoby składającej żądanie, a jeżeli istnieją uzasadnione wątpliwości co do tożsamości tej osoby, żąda dodatkowych informacji niezbędnych do potwierdzenia tożsamości osoby, której dane dotyczą. Jeżeli Inspektor nie jest w stanie zidentyfikować osoby, której dane dotyczą, informuje o tym osobę, której dane dotyczą. W takich przypadkach zastosowania nie mają art. 15–20 RODO, chyba że osoba, której dane dotyczą dostarczy dodatkowych informacji pozwalających ją zidentyfikować. Weryfikacja tożsamości nie może prowadzić do gromadzenia nadmiernych danych.

W przypadku wątpliwości co do rodzaju żądania i w razie wątpliwości IOD prosi osobę, wnoszącą żądanie o sprecyzowanie żądania. W konsultacji z osobą lub osobami przetwarzającymi dane podmiotu ustala w ramach jakiej kategorii podmiotów należy identyfikować zgłaszającego oraz określa w ramach których procesów przetwarzania danych, wskazanych w rejestrze czynności, dane zgłaszającego mogą być przetwarzane.

Jeżeli żądanie jest zasadne należy przekazać odpowiedź podmiotowi, który wniósł żądanie oraz odnotować sposób realizacji żądania ewidencji praw podmiotów. Osoby przetwarzające dane w imieniu administratora przygotowują informacje dotyczące żądań, przekazują do IOD który udziela kompleksowej informacji podmiotowi danych, na piśmie lub w sposób elektroniczny. Jeśli osoba, której dane dotyczą, przekazała swoje żądanie elektronicznie, informacje także są przekazywane elektronicznie, chyba że osoba, której dane dotyczą, zażąda innej formy.

Inspektor ochrony danych bez zbędnej zwłoki, najpóźniej w terminie miesiąca od otrzymania żądania udziela osobie, której dane dotyczą, informacji o działaniach podjętych w związku z żądaniem na podstawie art. 15–22 RODO. Z uwagi na skomplikowany charakter żądania lub liczbę żądań termin ten

może zostać przedłużony o kolejne dwa miesiące, o czym informuje się osobę, której dane dotyczą, z podaniem przyczyn opóźnienia.
Jeżeli administrator nie podejmuje działań w związku z żądaniem osoby, której dane dotyczą, to niezwłocznie – najpóźniej w terminie miesiąca od otrzymania żądania – informuje osobę, której dane dotyczą, o powodach niepodjęcia działań oraz o możliwości wniesienia skargi do organu nadzorczego oraz skorzystania ze środków ochrony prawnej przed sądem. Odmawiając podjęcia działań objętych treścią żądania, administrator wskazuje przyczyny takiego rozstrzygnięcia.
Realizacja praw jest wolna od opłat z wyjątkiem sytuacji, gdy żądania, są ewidentnie nieuzasadnione lub nadmierne, w szczególności ze względu na swój ustawiczny charakter. Administrator może pobrać rozsądną opłatę uwzględniając administracyjne koszty udzielenia informacji, prowadzenia komunikacji lub odmówić podjęcia działań w związku z żądaniem. Obowiązek wykazania, że żądanie ma ewidentnie nieuzasadniony lub nadmierny charakter, spoczywa na Administratorze.
Pierwsza kopia danych osobowych podlegających przetwarzaniu przekazywana jest podmiotowi danych bezpłatnie, za wszelkie kolejne kopie, o które zwróci się osoba, której dane dotyczą, administrator może pobrać opłatę w rozsądnej wysokości wynikającej z kosztów administracyjnych.
Administrator nie dopuszcza aby prawa podmiotów danych negatywnie wpływały na prawa lub wolności innych osób.
Administrator danych nie może zrealizować prawa podmiotu, w szczególności prawa do usuwania danych, jeżeli przetwarzanie jego danych jest niezbędne:

- do korzystania z prawa do wolności wypowiedzi i informacji;
- do wywiązania się z prawnego obowiązku wymagającego przetwarzania na mocy prawa lub do wykonania zadania realizowanego w interesie publicznym lub w ramach sprawowania władzy publicznej powierzonej administratorowi;
- z uwagi na względy interesu publicznego w dziedzinie zdrowia publicznego;
- do celów archiwalnych w interesie publicznym, do celów badań naukowych lub historycznych lub do celów statystycznych zgodnie z art. 89 ust. 1 RODO, o ile prawdopodobne jest, że prawo, o którym mowa w ust. 1, uniemożliwi lub poważnie utrudni realizację celów takiego przetwarzania;
- do ustalenia, dochodzenia lub obrony roszczeń.

Rozdział XI. Środki techniczne i organizacyjne zapewniające bezpieczeństwo danych.

Urząd Gminy w Bałtowie zapewnia stopień bezpieczeństwa odpowiadający ryzyku naruszenia praw i wolności osób fizycznych wskutek przetwarzania danych osobowych. Urząd Gminy w Bałtowie stosuje środki techniczne i organizacyjne mające na celu zabezpieczenie danych osobowych, które przetwarza, a w szczególności zabezpiecza dane przed ich udostępnieniem osobom nieupoważnionym, zapobiega przed zabraniem danych przez osobę nieuprawnioną, zapobiega przetwarzaniu danych z naruszeniem prawa oraz zmianie, utracie, uszkodzeniu lub zniszczeniu tych danych.
Urząd Gminy w Bałtowie przetwarza dane w wydzielonych pomieszczeniach, zabezpiecza wejścia do pomieszczeń, wyposaża pomieszczenia w zamykane szafy dające gwarancję bezpieczeństwa dokumentacji.
Pomieszczenia, w których są przetwarzane dane osobowe muszą być zamykane na klucz na czas nieobecności użytkowników. Dostęp do kluczy posiadają tylko wyznaczeni pracownicy. Administrator wyznacza osoby, które są upoważnione do otwierania i zamykania pomieszczeń przed rozpoczęciem i po zakończeniu pracy. Klucze do poszczególnych pomieszczeń Urzędu Gminy w Bałtowie zabezpieczone są w metalowej szafce. Puste pomieszczenia, w których przetwarzane są dane osobowe

zamykane są na klucz. Zabrania się pozostawiania klucza w drzwiach po ich zewnętrznej stronie. Klucze od biurek stanowiskowych i szaf biurowych są w posiadaniu pracowników, którzy ponoszą pełną odpowiedzialność za ich należyte zabezpieczenie.
Dokumenty z danymi osobowymi są przechowywane w pomieszczeniach zabezpieczonych drzwiami zwykłymi z zamkiem, okna są zabezpieczone roletami antywłamaniowymu. Pomieszczenia, w których przetwarzane są dane osobowe zabezpieczone są przed skutkami pożaru wolno stojącymi gaśnicami. Dokumenty z danymi osobowymi w formie papierowej przechowywane są w zamkniętych szafach metalowych lub drewnianych z zamkami na klucz. Kopie zapasowe przechowywane są w metalowym ognioodpornym sejfie. Dokumenty zawierające dane osobowe, po ustaniu przydatności przechowywane są przez okres archiwizacji w archiwum zakładowym, a po ustaniu okresu archiwizacji niszczone przez firmy specjalizujące się w brakowaniu dokumentacji archiwalnej. Natomiast dokumenty zbędne nie archiwalne na bieżąco niszczone są w niszczarkach. W przypadku konieczności udostępniania dokumentów i danych w nich zawartych, wśród których znajdują się dane osobowe niemające bezpośredniego związku z celem udostępnienia, należy bezwzględnie dokonać anonimizacji tych danych.
Dane osobowe przetwarzane w systemie IT, przetwarzane są przy użyciu komputerów stacjonarnych, na laptopach. Komputery, laptopy służące do przetwarzania danych osobowych połączone są ze sobą lokalną siecią komputerową. Zastosowano specjalistyczne urządzenia chroniące system informatyczny służący do przetwarzania danych osobowych przed skutkami awarii zasilania. Do ochrony dostępu do sieci komputerowej stosuje się zaporę sieciową FIREWALL. Dostęp do systemu operacyjnego komputera, w którym przetwarzane są dane osobowe zabezpieczony jest za pomocą procesu uwierzytelniania z wykorzystaniem identyfikatora użytkownika oraz hasła. System informatyczny stosowany w Urzędzie Gminy w Bałtowie posiada mechanizm wymuszający okresową zmianę haseł dostępu. Dla potrzeb ochrony danych osobowych przetwarzających w edytorach tekstu, arkuszach kalkulacyjnych lub systemach informatycznych stosuje się środki ochrony przed szkodliwym oprogramowaniem. Dla potrzeb ochrony danych osobowych przed skutkami awarii zastosowano macierz dyskową. Dla bezpieczeństwa danych osobowych stosuje się wygaszacze ekranów w przypadku dłuższej nieaktywności pracy użytkownika.
Użytkownik komputera przenośnego/laptopa poza siedzibą Urzędu Gminy w Bałtowie ma obowiązek jego ochrony, zabrania się pozostawiania ich bez opieki w miejscach, gdzie użytkownik nie ma możliwości sprawowania skutecznego nadzoru. Osoba używająca komputera przenośnego zawierającego dane osobowe zachowuje szczególną ostrożność podczas jego transportu, przechowywania i użytkowania, przestrzegając jednocześnie zaleceń producentów dotyczących ochrony sprzętu. Korzystanie z laptopa w miejscach publicznych i innych niechronionych wymaga ostrożności, by nie ujawnić danych osobowych osobom nieupoważnionym. Użytkowanie komputera przenośnego/laptopa poza siedzibą Urzędu Gminy w Bałtowie jest dopuszczalne tylko za zgodą ASI i sekretarza gminy. Każdy komputer/laptop jest szyfrowany za pomocą hasła. W wypadku potrzeby wyniesienia komputera przenośnego, osoba użytkująca komputer przenośny zawierający dane osobowe zachowuje szczególną ostrożność podczas jego transportu, przechowywania i użytkowania oraz nie zezwala na używanie komputera osobom nieupoważnionym. W przypadku utraty komputera przenośnego/laptopa użytkownik niezwłocznie powiadamia o tym fakcie swojego administratora oraz inspektora ochrony danych, a w przypadku kradzieży dokonuje również zgłoszenia tego faktu Policji. W szczególności w zawiadomieniu należy określić czy utracone wraz z komputerem dane miały charakter danych osobowych.

Urząd Gminy w Bałtowie stosuje środki organizacyjne mające na celu zabezpieczenie danych osobowych. Każda osoba przed dopuszczeniem do pracy z danymi osobowymi musi zostać przeszkolona i zapoznana z przepisami dotyczącymi ochrony danych osobowych oraz dokumentacją wewnętrzną z tego zakresu. Każdy pracownik zobowiązany jest do zapoznania się z Polityką bezpieczeństwa przetwarzania danych osobowych Urzędu Gminy w Bałtowie. Pracownicy zobowiązani są do zachowania poufności danych osobowych oraz sposobów ich zabezpieczenia przez Administratora. Zobowiązanie powinni złożyć na piśmie zgodnie z wzorem stanowiącym załącznik nr 9 Oświadczenie o zachowaniu poufności.
Dostęp do danych osobowych mogą mieć tylko i wyłącznie pracownicy posiadający pisemne, imienne upoważnienia do przetwarzania danych osobowych podpisane przez ADO. Każdy z pracowników powinien zachować szczególną ostrożność przy przetwarzaniu wszelkich danych osobowych, zobowiązany jest do ochrony danych przed dostępem do nich osób nieupoważnionych. Dane osobowe w formie papierowej mogą znajdować się na biurkach tylko na czas niezbędny na dokonanie czynności służbowych, a następnie muszą być chowane do szaf. Nie należy magazynować zbędnych dokumentów papierowych i wydruków, powinny być zniszczone w niszczarce do dokumentów, a za ich zniszczenie odpowiedzialny jest każdy pracownik.
Stacje komputerowe, na których przetwarzane są dane osobowe powinny mieć tak ustawione monitory, aby nie miały do nich wglądu osoby nieupoważnione. Każdy plik, w którym są zawarte dane osobowe powinien być zabezpieczony hasłem, jeśli nie jest to przetwarzanie danych w systemie informatycznym. W przypadku potrzeby przeniesienia danych osobowych pomiędzy komputerami należy dokonać tego z zachowaniem szczególnej ostrożności. Nośniki użyte do przenoszenia danych należy wyczyścić, nieodwracalnie skasować, aby nie zostały na nich dane osobowe. W wypadku niemożliwości skasowania danych z nośnika należy go zniszczyć fizycznie. Niezabezpieczonych danych osobowych nie należy przesyłać drogą elektroniczną. Pliki z danymi osobowymi należy szyfrować, a hasło do nich przekazywać inną drogą niż plik. Niepotrzebne, wykorzystane już pliki powinny zostać usunięte.

Rozdział XII. Zasady korzystania z poczty elektronicznej.

Urząd Gminy w Bałtowie wprowadza zasady korzystania ze służbowej poczty elektronicznej. Każdy pracownik posiadający służbowy adres elektroniczny do korespondencji mailowej w sprawach służbowych może używać wyłącznie służbowego adresu mailowego, zabronione jest korzystanie z prywatnego adresu mailowego w sprawach służbowych oraz wykorzystywanie służbowej poczty mailowej do celów prywatnych. Przed otworzeniem maila, należy ustalić czy nadawca wiadomości jest znany, czy pracownik otrzymywał już inne wiadomości od tego nadawcy, czy spodziewa się otrzymać wiadomość, czy tytuł wiadomości i nazwa załącznika mają sens, a w przypadku wątpliwości należy skonsultować się z administratorem systemów informatycznych lub inspektorem ochrony danych.
Każdy pracownik musi zachowywać szczególną uwagę na ataki phishingowe, fałszywe maile, linki aktywujące złośliwe oprogramowanie, uważnie czytać nadsyłane komunikaty, analizować adresy mailowe, czy są rzeczywiste, czy tylko łudząco podobne do znanych adresów. Zapobiegając uruchomieniu złośliwego oprogramowania, przesyłanego w postaci załączników do maili lub pobieranego po kliknięciu w odnośnik zawarty w mailu, nie wolno otwierać załączników (plików) w korespondencji mailowej nadesłanej przez nieznanego nadawcę lub nieoczekiwanych załączników, nie mających związku z treścią maila, budzących nieufność. Pracownik zobowiązany jest każdy załącznik w poczcie traktować jako potencjalnie niebezpieczny. W przypadku konieczności przesyłania w

korespondencji mailowej danych osobowych należy upewnić się, czy nie są przesyłane w nadmiernym zakresie, do właściwego adresata. Pliki zawierające dane osobowe należy szyfrować, zabezpieczać hasłem, a hasło należy przekazać odbiorcy inną drogą, innym kanałem komunikacji niż plik zawierający dane osobowe. Wiadomości elektroniczne, w miarę możliwości i zgodnie z zasadami archiwizowania należy kasować.

Rozdział XIII. Obsługa naruszeń.

Urząd Gminy w Bałtowie identyfikuje i ocenia naruszenie lub podejrzenie naruszenia. Definiuje katalog podatności i incydentów zagrażających bezpieczeństwu danych osobowych oraz opisuje sposób reagowania na nie w celu minimalizacji skutków wystąpienia incydentów bezpieczeństwa oraz ograniczenia ryzyka powstania zagrożeń i występowania incydentów w przyszłości.
Do typowych podatności bezpieczeństwa danych osobowych należą:

1. niewłaściwe zabezpieczenie fizyczne pomieszczeń, urządzeń i dokumentów;
2. niewłaściwe zabezpieczenie sprzętu IT, oprogramowania przed wyciekiem, kradzieżą i utratą danych osobowych;
3. nieprzestrzeganie zasad ochrony danych osobowych przez pracowników (np. niestosowanie zasady czystego biurka, niezamykanie pomieszczeń, szaf, biurek).

Do typowych incydentów bezpieczeństwa danych osobowych należą:

1. zagrożenia losowe zewnętrzne (np. klęski żywiołowe, przerwy w zasilaniu), ich występowanie może prowadzić do utraty integralności danych, ich zniszczenia i uszkodzenia infrastruktury technicznej systemu, ciągłość systemu zostaje zakłócona, nie dochodzi do naruszenia poufności danych.
2. zagrożenia losowe wewnętrzne (np. niezamierzone pomyłki operatorów, administratora, awarie sprzętowe, błędy oprogramowania), może dojść do zniszczenia danych, może zostać zakłócona ciągłość pracy systemu, może nastąpić naruszenie poufności danych.
3. zagrożenia zamierzone, świadome i celowe - najpoważniejsze zagrożenia, naruszenia poufności danych, (zazwyczaj nie następuje uszkodzenie infrastruktury technicznej i zakłócenie ciągłości pracy), zagrożenia te możemy podzielić na: nieuprawniony dostęp do systemu z zewnątrz (włamanie do systemu), nieuprawniony dostęp do systemu z jego wnętrza, nieuprawniony przekaz danych, pogorszenie jakości sprzętu i oprogramowania, bezpośrednie zagrożenie materialnych składników systemu.

Przypadki zakwalifikowane jako naruszenie lub uzasadnione podejrzenie naruszenia zabezpieczenia systemu informatycznego, w którym przetwarzane są informacje to głównie:

- sytuacje losowe lub nieprzewidziane oddziaływanie czynników zewnętrznych na zasoby systemu jak np.: wybuch gazu, pożar, zalanie pomieszczeń, katastrofa budowlana, napad, działania terrorystyczne, niepożądana ingerencja ekipy remontowej itp.;
- niewłaściwe parametry środowiska, jak np. nadmierna wilgotność lub wysoka temperatura; oddziaływanie pola elektromagnetycznego, wstrząsy;
- awaria sprzętu lub oprogramowania, które wyraźnie wskazują na umyślne działanie w kierunku naruszenia ochrony danych lub wręcz sabotaż, a także niewłaściwe działanie serwisu, a w tym sam fakt pozostawienia serwisantów bez nadzoru;
- pojawienie się odpowiedniego komunikatu alarmowego od tej części systemu, która zapewnia ochronę zasobów lub inny komunikat o podobnym znaczeniu;
- jakość danych w systemie lub inne odstępstwo od stanu oczekiwanego wskazujące na zakłócenia

systemu lub inną nadzwyczajną i niepożądaną modyfikację w systemie;
- nastąpiło naruszenie lub próba naruszenia integralności systemu lub bazy danych;
- stwierdzono próbę lub modyfikację danych lub zmianę w strukturze danych bez odpowiedniego upoważnienia (autoryzacji);
- nastąpiła niedopuszczalna manipulacja danymi osobowymi w systemie;
- ujawniono osobom nieupoważnionym dane osobowe lub objęte tajemnicą procedury ochrony przetwarzania albo inne strzeżone elementy systemu zabezpieczeń;
- praca w systemie lub jego sieci komputerowej wykazuje nieprzypadkowe odstępstwa od założonego rytmu pracy wskazujące na przełamanie lub zaniechanie ochrony informacji, np. praca przy komputerze lub w sieci osoby, która nie jest formalnie dopuszczona do jego obsługi, sygnał o uporczywym nieautoryzowanym logowaniu;
- ujawniono istnienie nieautoryzowanych kont dostępu do danych;
- podmieniono lub zniszczono nośniki z danymi bez odpowiedniego upoważnienia lub w sposób niedozwolony skasowano lub skopiowano dane;
- rażąco naruszono dyscyplinę pracy w zakresie przestrzegania procedur ochrony danych osobowych (nie wylogowanie się przed opuszczeniem stanowiska pracy, pozostawienie danych w drukarce, na ksero, nie zamknięcie pomieszczenia z komputerem, nie wykonanie w określonym terminie kopii bezpieczeństwa, prace na informacjach służbowych w celach prywatnych.

Każdy pracownik oraz osoba realizująca zadania na podstawie umowy cywilnoprawnej lub w inny sposób współpracująca z administratorem, która stwierdziła lub podejrzewa wystąpienie zdarzenia mogącego stanowić naruszenie ochrony danych osobowych, ma obowiązek zgłoszenia tego faktu inspektorowi ochrony danych lub administratorowi.

Zgłoszenie zdarzenia mogącego być naruszeniem ochrony danych osobowych powinno zawierać:
- opisanie symptomów naruszenia ochrony danych osobowych;
- określenie sytuacji i czasu, w jakim stwierdzono naruszenie ochrony danych osobowych;
- określenie wszelkich istotnych informacji mogących wskazywać na przyczynę naruszenia;
- określenie znanych danej osobie sposobów zabezpieczenia danych osobowych lub systemu oraz wszelkich kroków podjętych po ujawnieniu zdarzeń.

Stwierdzenie naruszenia następuje w momencie, kiedy administrator ma wystarczający stopień pewności co do tego, że miało miejsce zdarzenie zagrażające bezpieczeństwu, prowadzące do naruszenia bezpieczeństwa danych osobowych.

Administrator, przy współpracy z inspektorem ochrony danych podejmuje odpowiednie czynności zabezpieczające. Jeżeli to zasadne może nakazać przerwanie pracy w zakresie przetwarzania danych osobowych. Działa w celu wyjaśnienia okoliczności zdarzenia oraz przedstawia zalecenia w celu umożliwienia dalszego bezpiecznego przetwarzania danych.

Pracownicy mają obowiązek udzielania wyjaśnień i współpracy z inspektorem ochrony danych w celu analizy naruszenia, a odmowa traktowana będzie jako naruszenie obowiązków pracowniczych. Raport o naruszeniu danych osobowych przygotowuje inspektor ochrony danych według wzoru stanowiącego Załącznik nr 10 Raport o naruszeniu danych osobowych. Każde naruszenie Inspektor Ochrony Danych odnotowuje w rejestrze naruszeń stanowiącym załącznik nr 11 Rejestr naruszeń.

W przypadku, gdy naruszenie ochrony danych osobowych może skutkować ryzykiem naruszenia praw lub wolności osób fizycznych, musi zostać zgłoszone Prezesowi Urzędu Ochrony Danych Osobowych bez zbędnej zwłoki, ale nie później niż w terminie 72 godzin po stwierdzeniu naruszenia.

W zgłoszeniu naruszenia należy w szczególności:

1) opisać charakter naruszenia ochrony danych osobowych, w tym w miarę możliwości wskazać kategorie i przybliżoną liczbę osób, których dane dotyczą, oraz kategorie i przybliżoną liczbę wpisów danych osobowych, których dotyczy naruszenie;
2) wskazać dane kontaktowe osoby odpowiedzialnej u administratora za obsługę naruszenia;
3) opisać możliwe konsekwencje naruszenia ochrony danych osobowych;
4) opisać środki zastosowane lub proponowane w celu zaradzenia naruszeniu ochrony danych osobowych, w tym w stosownych przypadkach środki w celu zminimalizowania jego ewentualnych negatywnych skutków.

Jeżeli wszystkich informacji nie da się udzielić w tym samym czasie, można je udzielać organowi nadzorczemu sukcesywnie lecz bez zbędnej zwłoki, po dokonaniu pierwszego zgłoszenia. Należy przekazywać na bieżąco aktualne informacje. W przypadku uzyskania w toku dochodzenia dowodów na to, że opanowano zdarzenie, a w rzeczywistości żadne naruszenie nie miało miejsca, informację tę można dodać do informacji już przekazanych do organu nadzorczego, a następnie zarejestrować zaistniałe zdarzenie jako niestanowiące naruszenia ochrony danych osobowych. Do zgłoszenia przekazanego organowi nadzorczemu po upływie 72 godzin dołącza się wyjaśnienie przyczyn opóźnienia.

Jeżeli naruszenie ochrony danych osobowych może powodować wysokie ryzyko naruszenia praw lub wolności osób fizycznych, bez zbędnej zwłoki zawiadamia się o tym osoby, których dane dotyczą. Zawiadomienie należy przygotować jasnym i prostym językiem.

Zawiadomienie nie jest wymagane w następujących przypadkach, które należy wykazać przed organem nadzorczym:

1) gdy wdrożono odpowiednie techniczne i organizacyjne środki ochrony i środki te zostały zastosowane do danych osobowych, których dotyczy naruszenie, w szczególności takie jak szyfrowanie, uniemożliwiające odczyt osobom nieuprawnionym do dostępu do tych danych osobowych;
2) gdy zastosowano następnie środki eliminujące prawdopodobieństwo wysokiego ryzyka naruszenia praw lub wolności osoby, której dane dotyczą;
3) wymagałoby ono niewspółmiernie dużego wysiłku; w takim przypadku wydany zostaje publiczny komunikat lub zastosowany zostaje podobny środek, za pomocą którego osoby, których dane dotyczą, zostają poinformowane w równie skuteczny sposób.

Rozdział XIV. Postanowienia końcowe.

Polityka bezpieczeństwa przetwarzania danych osobowych Urzędu Gminy w Bałtowie jest dokumentem wewnętrznym Urzędu Gminy w Bałtowie. Przechowywana jest w wersji elektronicznej oraz w wersji papierowej w siedzibie administratora.

Każda osoba upoważniona do przetwarzania danych osobowych zobowiązana jest zapoznać się z niniejszą polityką oraz przestrzegać jej postanowień. Zabrania się udostępniania polityki osobom nieuprawnionym. Wobec osoby, która nie stosuje się do procedur i sposobów postępowania opisanych w polityce oraz wobec osoby, która ujawni kopie polityki osobom nieupoważnionym może zostać wszczęte postępowanie dyscyplinarne.

REJESTR CZYNNOŚCI PRZETWARZANIA

Administrator Danych Osobowych:

Urząd Gminy
w Bałtowie
Bałtów 32, 27-423 Bałtów
tel. 41 2641008
e-mail: gmina@gminabaltow.pl

Inspektor Ochrony Danych:
……..
e-mail: iod@ gminabaltow.pl

Nazwa czynności przetwarzania	
Cel przetwarzania	
Kategorie osób, których dane dotyczą	
Kategorie danych	
Podstawa prawna	
Źródło danych	
Planowany termin usunięcia danych	
Nazwa współadministratora, jeżeli dotyczy	
Nazwa podmiotu przetwarzającego, jeżeli dotyczy	
Kategorie odbiorców	
Ogólny opis technicznych i organizacyjnych środków bezpieczeństwa zgodnie z art. 32 ust. 1	
Transfer do kraju trzeciego lub organizacji międzynarodowej	
Jeśli transfer i art. 49 ust. 1 akapit drugi - dokumentacja odpowiednich zabezpieczeń	

Umowa powierzenia przetwarzania danych osobowych

zawarta w Bałtowie, w dniu …….…….. r., pomiędzy:
Gminą Bałtów, Bałtów 32, 27-423 Bałtów, reprezentowanym przez Wójta Gminy Bałtów …….., zwanym w dalszej części umowy „**Administratorem**",
a
……
……
……
zwanym w dalszej części umowy „**Podmiotem przetwarzającym**"
Administrator i Podmiot przetwarzający zwani są dalej łącznie **„Stronami"**, osobno zaś **„Stroną"**.
Strony postanawiają, co następuje:

§ 1
Powierzenie przetwarzania danych osobowych

1. Umowa ma charakter umowy powierzenia danych osobowych w rozumieniu art. 28 ust. 3 rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych) (Dz. U. UE. L. z 2016 r. Nr 119, str. 1 oraz z 2018 r. Nr 127, str. 2), zwanego w dalszej części umowy ,,Rozporządzeniem".
2. Administrator oświadcza, że jest Administratorem Danych Osobowych w rozumieniu przepisów Rozporządzenia w stosunku do danych powierzonych Podmiotowi przetwarzającemu.
3. Podmiot przetwarzający zobowiązuje się przetwarzać powierzone mu dane osobowe zgodnie z niniejszą umową, Rozporządzeniem oraz z innymi przepisami powszechnie obowiązującego prawa dotyczącego danych osobowych.
4. Podmiot przetwarzający oświadcza, że stosuje środki bezpieczeństwa spełniające wymogi Rozporządzenia, wdrożył odpowiednie środki techniczne i organizacyjne, zapewniające stopień bezpieczeństwa przetwarzania danych, uwzględniając stan wiedzy technicznej, koszt wdrażania oraz charakter, zakres, kontekst i cele przetwarzania oraz ryzyko naruszenia praw lub wolności osób fizycznych o różnym prawdopodobieństwie wystąpienia i wadze zagrożenia, zgodnie z art. 32 RODO, zapewnia poufność, integralność, dostępność i odporność systemów i usług przetwarzania oraz zdolność do szybkiego przywrócenia dostępności danych osobowych i dostępu do nich w razie incydentu fizycznego lub technicznego.

§ 2
Zakres i cel przetwarzania danych

1. Podmiot przetwarzający będzie przetwarzał, powierzone na podstawie umowy dane osobowe: .....
2. Powierzone przez Administratora dane osobowe będą przetwarzane przez Podmiot przetwarzający wyłącznie w celu realizacji umowy głównej z dnia ……, której przedmiotem jest …….

§ 3

Obowiązki podmiotu przetwarzającego

1. Podmiot przetwarzający zobowiązuje się, przy przetwarzaniu powierzonych danych osobowych, do ich zabezpieczenia poprzez stosowanie odpowiednich środków technicznych i organizacyjnych zapewniających adekwatny stopień bezpieczeństwa odpowiadający ryzyku związanym z przetwarzaniem danych osobowych, o których mowa w art. 32 Rozporządzenia.
2. Podmiot przetwarzający zobowiązuje się dołożyć należytej staranności przy przetwarzaniu powierzonych danych osobowych.
3. Podmiot przetwarzający zobowiązuje się do nadania upoważnień do przetwarzania danych osobowych wszystkim osobom, które będą przetwarzały powierzone dane w celu realizacji niniejszej umowy.
4. Podmiot przetwarzający zobowiązuje się zapewnić zachowanie w tajemnicy, (o której mowa w art. 28 ust 3 pkt b Rozporządzenia) przetwarzanych danych przez osoby, które upoważnia do przetwarzania danych osobowych w celu realizacji niniejszej umowy, zarówno w trakcie zatrudnienia ich w Podmiocie przetwarzającym, jak i po jego ustaniu.
5. Podmiot przetwarzający po zakończeniu świadczenia usług związanych z przetwarzaniem usuwa/zwraca Administratorowi wszelkie dane osobowe (*należy wybrać czy podmiot przetwarzający ma usunąć czy zwrócić dane*) oraz usuwa wszelkie ich istniejące kopie, chyba że prawo Unii lub prawo państwa członkowskiego nakazują przechowywanie danych osobowych.
6. W miarę możliwości Podmiot przetwarzający pomaga Administratorowi w niezbędnym zakresie wywiązywać się z obowiązku odpowiadania na żądania osoby, której dane dotyczą oraz wywiązywania się z obowiązków określonych w art. 32-36 Rozporządzenia.
7. Podmiot przetwarzający po stwierdzeniu naruszenia ochrony danych osobowych bez zbędnej zwłoki zgłasza je administratorowi w ciągu ..... (należy wskazać czas na dokonanie zgłoszenia, *np. w ciągu 24 godzin*).

§ 4

Prawo kontroli

1. Administrator danych zgodnie z art. 28 ust. 3 pkt h Rozporządzenia ma prawo kontroli, czy środki zastosowane przez Podmiot przetwarzający przy przetwarzaniu i zabezpieczeniu powierzonych danych osobowych spełniają postanowienia umowy.
2. Administrator danych realizować będzie prawo kontroli w godzinach pracy Podmiotu przetwarzającego i z minimum 3 dniowym jego uprzedzeniem.
3. Podmiot przetwarzający zobowiązuje się do usunięcia uchybień stwierdzonych podczas kontroli w terminie wskazanym przez Administratora danych nie dłuższym niż 7 dni.
4. Podmiot przetwarzający udostępnia Administratorowi wszelkie informacje niezbędne do wykazania spełnienia obowiązków określonych w art. 28 Rozporządzenia.

§ 5

Dalsze powierzenie danych do przetwarzania

1. Podmiot przetwarzający może powierzyć dane osobowe objęte niniejszą umową do dalszego przetwarzania podwykonawcom jedynie w celu wykonania umowy po uzyskaniu uprzedniej pisemnej zgody Administratora danych.

2. Przekazanie powierzonych danych do państwa trzeciego może nastąpić jedynie na pisemne polecenie Administratora danych chyba, że obowiązek taki nakłada na Podmiot przetwarzający prawo Unii lub prawo państwa członkowskiego, któremu podlega Podmiot przetwarzający. W takim przypadku przed rozpoczęciem przetwarzania Podmiot przetwarzający informuje Administratora danych o tym obowiązku prawnym, o ile prawo to nie zabrania udzielania takiej informacji z uwagi na ważny interes publiczny.
3. Podwykonawca, o którym mowa w § 5 ust. 1 umowy winien spełniać te same gwarancje i obowiązki jakie zostały nałożone na Podmiot przetwarzający w niniejszej umowie.
4. Podmiot przetwarzający ponosi pełną odpowiedzialność wobec Administratora za nie wywiązanie się ze spoczywających na podwykonawcy obowiązków ochrony danych.

§ 6

Odpowiedzialność Podmiotu przetwarzającego

1. Podmiot przetwarzający jest odpowiedzialny za udostępnienie lub wykorzystanie danych osobowych niezgodnie z treścią umowy, a w szczególności za udostępnienie powierzonych do przetwarzania danych osobowych osobom nieupoważnionym.
2. Podmiot przetwarzający zobowiązuje się do niezwłocznego poinformowania Administratora danych o jakimkolwiek postępowaniu, w szczególności administracyjnym lub sądowym, dotyczącym przetwarzania przez Podmiot przetwarzający danych osobowych określonych w umowie, o jakiejkolwiek decyzji administracyjnej lub orzeczeniu dotyczącym przetwarzania tych danych, skierowanych do Podmiotu przetwarzającego, a także o wszelkich planowanych, o ile są wiadome, lub realizowanych kontrolach i inspekcjach dotyczących przetwarzania w Podmiocie przetwarzającym tych danych osobowych, w szczególności prowadzonych przez Prezesa Urzędu Ochrony Danych Osobowych. Niniejszy ustęp dotyczy wyłącznie danych osobowych powierzonych przez Administratora danych.

§ 7

Czas obowiązywania umowy

1. Umowa zostaje zawarta na czas obowiązywania, zawartej między stronami, umowy z dnia …… w sprawie ……, tj. ……..
2. Każda ze stron może wypowiedzieć niniejszą umowę z zachowaniem jednomiesięcznego okresu wypowiedzenia.

§ 8

Rozwiązanie umowy

1. Administrator danych może rozwiązać niniejszą umowę ze skutkiem natychmiastowym gdy Podmiot przetwarzający:
   a) pomimo zobowiązania go do usunięcia uchybień stwierdzonych podczas kontroli nie usunie ich w wyznaczonym terminie;
   b) przetwarza dane osobowe w sposób niezgodny z umową;
   c) powierzył przetwarzanie danych osobowych innemu podmiotowi bez zgody Administratora danych.

§ 9

Zasady zachowania poufności

1. Podmiot przetwarzający zobowiązuje się do zachowania w tajemnicy wszelkich informacji, danych, materiałów, dokumentów i danych osobowych otrzymanych od Administratora danych i od współpracujących z nim osób.
2. Podmiot przetwarzający oświadcza, że w związku ze zobowiązaniem do zachowania w tajemnicy danych poufnych nie będą one wykorzystywane, ujawniane ani udostępniane bez pisemnej zgody Administratora w innym celu niż wykonanie umowy, chyba że konieczność ujawnienia posiadanych informacji wynika z obowiązujących przepisów prawa lub umowy.

§ 10

Postanowienia końcowe

1. Zmiana niniejszej umowy może nastąpić tylko w formie pisemnej.
2. Z tytułu wykonywania niniejszej umowy Podmiotowi przetwarzającemu nie przysługuje dodatkowe wynagrodzenie.
3. W sprawach nieuregulowanych niniejszą umową mają zastosowania przepisy kodeksu cywilnego oraz Rozporządzenia.
4. Umowę sporządzono w dwóch jednobrzmiących egzemplarzach, po jednym dla każdej ze Stron.

.....	.....
Administrator	Podmiot przetwarzający

Wykaz podmiotów, którym powierzono dane osobowe do przetwarzania

Lp.	Nazwa podmiotu, któremu powierzono dane osobowe do przetwarzania	Daty/termin obowiązywania umowy	Cel powierzenia danych	Uwagi

REJESTR KATEGORII PRZETWARZANIA

Procesor:

Urząd Gminy
w Bałtowie
Bałtów 32, 27-423 Bałtów
tel. 41 2641008
e-mail: gmina@gminabaltow.pl

Inspektor Ochrony Danych:
……..
e-mail: iod@ gminabaltow.pl

Kategorie przetwarzanych danych	
Ogólny opis technicznych i organizacyjnych środków bezpieczeństwa (jeżeli jest to możliwe)	
Nazwa i dane kontaktowe administratora	
Nazwa i dane kontaktowe współadministratora (jeśli dotyczy)	
Nazwa i dane kontaktowe przedstawiciela administratora (jeśli wyznaczono)	
Inspektor ochrony danych administratora (jeśli powołano)	
Nazwy państw trzecich lub organizacji międzynarodowych, do których dane są przekazywane	
Dokumentacja odpowiednich zabezpieczeń danych osobowych przekazywanych na podstawie art. 49 ust. 1 akapit drugi	
Dodatkowe informacje	

…….
pieczęć administratora

Bałtów, dnia ……. r.

UPOWAŻNIENIE
do przetwarzania danych osobowych

Na podstawie art. 29 rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych) (Dz. U. UE. L. z 2016 r. Nr 119, str. 1 ze zm.)

upoważniam Panią/Pana:

…….
imię, nazwisko i stanowisko upoważnionego

do przetwarzania danych osobowych w zakresie niezbędnym do realizacji zadań wynikających z zakresu obowiązków w ramach następujących czynności:

…….
czynności przetwarzania danych osobowych zgodnie z rejestrem czynności przetwarzania

…….
czynności przetwarzania danych osobowych zgodnie z rejestrem czynności przetwarzania

Niniejsze upoważnienie obowiązuje w okresie ……., może być w każdym czasie zmienione lub odwołane.

Jednocześnie zobowiązuję Panią/Pana do:

- przetwarzania danych osobowych, zgodnie z niniejszym upoważnieniem oraz z przepisami RODO, z ustawą z dnia 10 maja 2018 r. o ochronie danych osobowych oraz z wewnętrznymi politykami i procedurami Urzędu Gminy w Bałtowie dotyczącymi ochrony danych osobowych;
- zachowania w tajemnicy wszelkich informacji związanych z wykonywaną pracą, w szczególności w zakresie danych osobowych i sposobów ich zabezpieczania, również po odwołaniu upoważnienia, a także po ustaniu zatrudnienia.

……
podpis administratora

Niniejsze upoważnienie otrzymałam/em i zobowiązuję się do jego przestrzegania.

……
data i podpis upoważnionego

Uwagi: w przypadku przetwarzania danych szczególnych kategorii należy je wyszczególnić.

…….
pieczęć administratora

Bałtów, dnia ……. r.

ODWOŁANIE UPOWAŻNIENIA
do przetwarzania danych osobowych

Na podstawie art. 29 rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych) (Dz. U. UE. L. z 2016 r. Nr 119, str. 1 ze zm.)

odwołuję Pani/Panu:

…….
imię, nazwisko i stanowisko upoważnionego

upoważnienie do przetwarzania danych osobowych z dnia ……

do następujących czynności:

…….
czynności przetwarzania danych osobowych zgodnie z rejestrem czynności przetwarzania

…….
czynności przetwarzania danych osobowych zgodnie z rejestrem czynności przetwarzania

Jednocześnie zobowiązuję Panią/Pana do zachowania w tajemnicy wszelkich informacji związanych z wykonywaną pracą, w szczególności w zakresie danych osobowych i sposobów ich zabezpieczania.

……
podpis administratora

Potwierdzam odbiór odwołania upoważnienia.

……
data i podpis osoby, której odwołano upoważnienie

Ewidencja upoważnień do przetwarzania danych osobowych

Lp.	Imię i nazwisko upoważnionego	Data udzielenia upoważnienia	Data końcowa obowiązywania lub ustania upoważnienia	Uwagi

REJESTR REALIZACJI ŻĄDAŃ

Administrator Danych Osobowych:

Urząd Gminy
w Bałtowie
Bałtów 32, 27-423 Bałtów
tel. 41 2641008
e-mail: gmina@gminabaltow.pl

Data zgłoszenia żądania	
Sposób zgłoszenia żądania	
Zakres żądania	
Osoba obsługująca żądanie	
Czy na podstawie informacji przekazanych przez żądającego zidentyfikowano podmiot danych	
Czy prowadzono dodatkowe postępowanie dotyczące identyfikacji podmiotu danych	
Proces, w ramach którego przetwarzano dane	
Sposób realizacji żądania	
Opłata, czy pobrano	
Data realizacji żądania	
Inne informacje dotyczące żądania	

OŚWIADCZENIE O ZACHOWANIU POUFNOŚCI

Ja, ... niżej podpisany/a oświadczam, że: zostałem/am zapoznany/a z przepisami dotyczącymi ochrony danych osobowych, w szczególności Rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/676 z dnia 27 kwietnia 2016 roku w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE oraz zobowiązuję się do:

- zachowania w tajemnicy danych osobowych oraz wszelkich informacji o danych osobowych uzyskanych w trakcie dokonywania powierzonych mi operacji związanych z przetwarzaniem danych osobowych przez Urząd Gminy w Bałtowie;
- przetwarzania danych osobowych wyłącznie w zakresie celu przewidzianym w powierzonych przez administratora zadaniach oraz niewykorzystywania danych osobowych w celach niezgodnych z zakresem i celem powierzonych zadań przez administratora;
- zachowania w tajemnicy sposobów zabezpieczenia danych osobowych i informacji;
- ochrony danych osobowych przed przypadkowym lub niezgodnym z prawem zniszczeniem, utratą, modyfikacją danych osobowych, nieuprawnionym ujawnieniem danych osobowych, nieuprawnionym dostępem do danych osobowych oraz przetwarzaniem.

Przyjmuję do wiadomości, iż postępowanie sprzeczne z powyższymi zobowiązaniami może być uznane przez Administratora za naruszenie przepisów o ochronie danych osobowych. Jestem świadoma/y, że naruszenie poufności przetwarzanych danych osobowych może nieść dla mnie konsekwencje dyscyplinarne, w tym skutkować zwolnieniem dyscyplinarnym za ciężkie naruszenie obowiązków pracowniczych, może skutkować odpowiedzialnością karną lub odszkodowawczą na rzecz administratora i/lub pokrzywdzonych na skutek mojego działania osób.

.....

(podpis oświadczającego)

Bałtów, dnia .....

Raport o naruszeniu danych osobowych

Sporządzający raport:

Imię i nazwisko .....

Stanowisko .....

1) miejsce, dokładny czas i data naruszenia bezpieczeństwa informacji w tym ochrony danych osobowych (budynek, piętro, pomieszczenie, godzina itp.):

   .....

   .....

   .....

2) osoby powodujące naruszenie (które swoim działaniem lub zaniechaniem przyczyniły się do naruszenia bezpieczeństwa informacji w tym ochrony danych osobowych):

   .....

   .....

   .....

3) charakter naruszenia (tj. nieuprawnione lub przypadkowe ujawnienie lub udostępnienie danych, wprowadzenie nieuprawnionych zmian podczas odczytu, zapisu, transmisji lub przechowywania, brak możliwości wykorzystania danych na żądanie, w założonym czasie, przez osobę do tego uprawnioną):

   .....

   .....

   .....

4) informacje o danych, które zostały lub mogły zostać ujawnione:

   .....

   .....

   .....

5) zabezpieczone materiały lub inne dowody związane z wydarzeniem:

.....

.....

.....

6) kategorie danych, których dotyczy naruszenie:

.....

.....

.....

7) kategorie osób, których dotyczy naruszenie:

.....

.....

.....

8) środki bezpieczeństwa zastosowane przed naruszeniem:

.....

.....

.....

9) krótki opis wydarzenia związanego z naruszeniem bezpieczeństwa informacji, w tym ochrony danych osobowych (przebieg zdarzenia, opis zachowania uczestników, podjęte działania):

.....

.....

.....

.....

.....

…… ……

data podpis

REJESTR NARUSZEŃ

Administrator Danych Osobowych:

Urząd Gminy
w Bałtowie
Bałtów 32, 27-423 Bałtów
tel. 41 2641008
e-mail: gmina@gminabaltow.pl

Naruszenie (opis naruszenia)	
Data i godzina zgłoszenia podejrzenia naruszenia	
Data oraz godzina stwierdzenia naruszenia	
Data i miejsce naruszenia/okres, którego dotyczy	
Kategoria i ilość osób, których dotyczy naruszenie	
Zakres danych i/lub kategorie danych, których dotyczy naruszenie	
Okoliczności naruszenia	
Opis skutków/konsekwencji naruszenia	
Osoba/jednostka odpowiedzialna za naruszenie	
Podjęte działania - opis środków zastosowanych lub proponowanych do wdrożenia w celu zaradzenia naruszeniu, w tym zastosowane środki w celu zminimalizowania negatywnych skutków	
Rezultat działań naprawczych	
Czy zachodzi obowiązek poinformowania Urzędu Ochrony Danych Osobowych (Jeśli tak - data i godzina zgłoszenia; w przypadku wystąpienia opóźnienia w powiadomieniu - wyjaśnienie przyczyn opóźnienia)	
Czy poinformowano organy ścigania (data zawiadomienia)	
Czy zachodzi obowiązek poinformowania osoby/osób, których naruszenie dotyczy oraz sposób przekazania informacji wraz opisem zaleceń dla podmiotów danych	
Monitoring działań naprawczych	