ZARZĄDZENIE nr 31/2018

Wójta Gminy Naruszewo

z dnia 19 czerwca 2018 roku

w sprawie wprowadzenia Polityki ochrony danych osobowych w Urzędzie Gminy Naruszewo

Działając na podstawie art. 30 ust. 1 ustawy z dnia 8 marca 1990r. o samorządzie gminnym (Dz. U. z 2017r. poz. 1875 ze zm.) oraz Rozporządzenia 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. (Dz. Urz. UE L 119 z 04.05.2016) zarządzam, co następuje:

§ 1

W Urzędzie Gminy Naruszewo w celu zapewnienia ochrony przetwarzania przez Urząd danych osobowych, wprowadza się Politykę ochrony danych osobowych w Urzędzie Gminy Naruszewo (zwaną dalej „Polityką") , stanowiącą załącznik Nr 1 do niniejszego Zarządzenia.

§ 2

Do zapoznania się z treścią Polityki oraz stosowania jej zapisów zobowiązani są wszyscy pracownicy Urzędu Gminy Naruszewo.

§ 3

Polityka została sporządzona w wersji papierowej oraz elektronicznej.

§ 4

Wykonanie zarządzenia powierzam sekretarzowi Gminy

§ 5

1. Traci moc zarządzenie Nr 22/2016 Wójta Gminy Naruszewo z dnia 5 kwietnia 2016 roku w sprawie ochrony danych osobowych w Urzędzie Gminy w Naruszewie.
2. Dokumenty opracowane na podstawie zarządzenia, o którym mowa w ust. 1 zachowują moc chyba, że są sprzeczne z Polityką.

§ 6

Zarządzenie wchodzi w życie z dniem podjęcia z mocą obowiązującą od dnia 25 maja 2018r.

Wójt

mgr inż. Beata Pierścińska

Załącznik nr 1 do Zarządzenia nr 31/2018 Wójta Gminy Naruszewo w sprawie wprowadzenia Polityki ochrony danych osobowych w Urzędzie Gminy Naruszewo

POLITYKA OCHRONY DANYCH OSOBOWYCH
Urzędu Gminy Naruszewo

1. **Polityka ochrony danych osobowych** (dalej także "**Polityka**") Urzędu Gminy Naruszewo stanowi zbiór zasad i regulacji ochrony danych osobowych obowiązujących w Urzędzie Gminy Naruszewo (dalej jako „**Urzędem**").
   Niniejsza Polityka jest polityką ochrony danych osobowych w rozumieniu RODO - rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z 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.Urz. UE L 119, s. 1).

2. **Polityka zawiera:**
   a) opis zasad ochrony danych obowiązujących w Urzędzie,
   b) odwołania do załączników uszczegóławiających (konkretne procedury lub instrukcje dotyczące poszczególnych obszarów z zakresu ochrony danych osobowych wymagających doprecyzowania w odrębnych dokumentach).

3. **Odpowiedzialny za wdrożenie i utrzymanie niniejszej Polityki jest Wójt Gminy Naruszewo, a w ramach Urzędu:**
   a) Sekretarz Gminy, któremu powierzono nadzór nad obszarem ochrony danych osobowych - zarówno dokumentacja w wersji papierowej, jak i sprzęt, w tym sprzęt komputerowy.
   b) Osoba wyznaczona przez Wójta Gminy do zapewnienia zgodności procedur i systemów informatycznych stosowanych w Urzędzie, a związanych w przetwarzaniem danych osobowych.

4. **Za monitorowanie przestrzegania Polityki odpowiada Inspektor Ochrony Danych.**

5. **Urząd zapewnia zgodność przetwarzania danych osobowych z regulacjami RODO oraz krajowymi przepisami dotyczącymi ochrony danych osobowych - szczególnie w odniesieniu do: pracowników i interesantów Urzędu, a ponadto danych osobowych**

powierzonych do przetwarzania podmiotom trzecim.

6. **Skróty i definicje:**
   - **Polityka** oznacza niniejszą Politykę ochrony danych osobowych, o ile co innego nie wynika wyraźnie z kontekstu.
   - **RODO** oznacza rozporządzenie Parlamentu Europejskiego i Rady (UE) 2016/679 z 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.Urz. UE L 119, s. 1).
   - **Dane** oznaczają dane osobowe, o ile co innego nie wynika wyraźnie z kontekstu.
   - **Dane wrażliwe** oznaczają dane osobowe ujawniające pochodzenie rasowe lub etniczne, poglądy polityczne, przekonania religijne lub światopoglądowe, przynależność do związków zawodowych oraz przetwarzania danych genetycznych, danych biometrycznych w celu jednoznacznego zidentyfikowania osoby fizycznej lub danych dotyczących zdrowia, seksualności lub orientacji seksualnej.
   - **Osoba** oznacza osobę, której dane dotyczą, o ile co innego nie wynika wyraźnie z kontekstu.
   - **Podmiot przetwarzający** oznacza podmiot lub osobę, której Urząd powierzył przetwarzanie danych osobowych (np. usługodawca – informatyk)
   - **IOD lub Inspektor** oznacza Inspektora Ochrony Danych Osobowych
   - **RCPD lub Rejestr** oznacza Rejestr Czynności Przetwarzania Danych Osobowych.

7. **Filary ochrony danych osobowych w Urzędzie:**
   1) **Legalność** – Urząd dba o ochronę prywatności i przetwarza dane zgodnie z prawem.
   2) **Bezpieczeństwo** – Urząd zapewnia odpowiedni poziom bezpieczeństwa danych podejmując stale działania w tym zakresie.
   3) **Prawa interesanta (pracownika)** – Urząd umożliwia osobom, których dane przetwarza, wykonywanie swoich praw i prawa te realizuje.
   4) **Rozliczalność** – Urząd dokumentuje to, w jaki sposób spełnia obowiązki, aby w każdej chwili móc wykazać zgodność.

8. **Zasady ochrony danych**

   Urząd działa w oparciu o powszechnie obowiązujące przepisy prawa:
   1) zgodnie z prawem (legalizm),
   2) rzetelnie i uczciwie (rzetelność),

3) w sposób przejrzysty dla osoby, której dane dotyczą (transparentność),
4) w konkretnych celach i nie "na zapas" (minimalizacja),
5) nie więcej niż potrzeba (adekwatność),
6) z dbałością o prawidłowość danych (prawidłowość),
7) nie dłużej niż potrzeba (czasowość),
8) zapewniając odpowiednie bezpieczeństwo danych (bezpieczeństwo).

9. System ochrony danych

System ochrony danych osobowych w Urzędzie składa się z następujących elementów:

1) **Inwentaryzacja danych. Ocena skutków dla ochrony danych. Urząd** w terminie co najmniej do końca stycznia danego roku kalendarzowego (lub każdorazowo w trakcie roku kalendarzowego - jak dodawane (odejmowane) są kolejne kategorie przetwarzanych danych) dokonuje identyfikacji zasobów przetwarzanych danych osobowych, kategorii danych, zależności między zasobami danych, identyfikacji sposobów wykorzystania danych (inwentaryzacja), w tym:
   a) przypadków przetwarzania danych wrażliwych,
   b) przypadków przetwarzania danych osób, których Urząd nie identyfikuje (**dane niezidentyfikowane**);
   c) współadministrowania danymi.
2) **Rejestr.** Urząd opracowuje, prowadzi i utrzymuje Rejestr Czynności Przetwarzania Danych Osobowych w Urzędzie (Rejestr). Rejestr jest narzędziem rozliczania zgodności z ochroną danych w Urzędzie.
3) **Umowy powierzenia przetwarzania danych. Urząd** zawiera z podmiotami lub osobami, którym powierza przetwarzanie danych osobowych (np. usługodawca - informatyk) odpowiednie umowy, stosownie do art. 28 RODO.
4) **Podstawy prawne. Urząd** zapewnia, identyfikuje, weryfikuje podstawy prawne przetwarzania danych i rejestruje je w Rejestrze, w tym:
   a) utrzymuje system zarządzania zgodami na przetwarzanie danych i komunikację na odległość,
   b) inwentaryzuje i uszczegóławia uzasadnienie przypadków, gdy Urząd przetwarza dane na podstawie prawnie uzasadnionego interesu Urzędu
5) **Obsługa praw jednostki.** Urząd spełnia obowiązki informacyjne względem osób, których dane przetwarza, oraz zapewnia obsługę ich praw, realizując otrzymane w tym zakresie żądania, w tym:
   a) **Obowiązki informacyjne. Urząd** przekazuje osobom prawem wymagane

informacje przy zbieraniu danych i w innych sytuacjach oraz organizuje i zapewnia udokumentowanie realizacji tych obowiązków.

b) **Możliwość wykonania żądań. Urząd** weryfikuje i zapewnia możliwość efektywnego wykonania każdego typu żądania przez siebie i swoich przetwarzających.

c) **Obsługa żądań. Urząd** zapewnia odpowiednie nakłady i procedury, aby żądania osób były realizowane w terminach i w sposób wymagany RODO i dokumentowane.

d) **Zawiadamianie o naruszeniach. Urząd** stosuje procedury pozwalające na ustalenie konieczności zawiadomienia osób dotkniętych zidentyfikowanym naruszeniem ochrony danych.

6) **Minimalizacja.** Urząd posiada zasady i metody zarządzania minimalizacją (*privacy by default*), a w tym:

a) zasady zarządzania **adekwatnością** danych;

b) zasady reglamentacji i zarządzania **dostępem** do danych;

c) zasady zarządzania okresem **przechowywania** danych i weryfikacji dalszej przydatności;

7) **Bezpieczeństwo. Urząd** zapewnia odpowiedni poziom bezpieczeństwa danych, w tym:

a) przeprowadza analizy ryzyka dla czynności przetwarzania danych lub ich kategorii;

b) przeprowadza oceny skutków dla ochrony danych tam, gdzie ryzyko naruszenia praw i wolności osób jest wysokie;

c) dostosowuje środki ochrony danych do ustalonego ryzyka;

d) posiada system zarządzania bezpieczeństwem informacji; (w tym systemem informatycznym)

e) stosuje procedury pozwalające na identyfikację, ocenę i zgłoszenie zidentyfikowanego naruszenia ochrony danych Urzędowi Ochrony Danych – zarządza incydentami.

8) ***Privacy by design.*** Urząd zarządza zmianami mającymi wpływ na prywatność. W tym celu procedury uruchamiania nowych projektów lub zadań Urzędu uwzględniają konieczność oceny wpływu zmiany na ochronę danych, zapewnienie prywatności (a w tym zgodności celów przetwarzania, bezpieczeństwa danych i minimalizacji) już w fazie projektowania zmiany, inwestycji czy na początku nowego projektu.

10. Rejestr Czynności Przetwarzania Danych (RCPD).

1) RCPD stanowi formę dokumentowania czynności przetwarzania danych osobowych

w Urzędzie. RCPD pełni rolę mapy przetwarzania danych i jest jednym z kluczowych elementów umożliwiających realizację fundamentalnej zasady, na której opiera się cały system ochrony danych osobowych, czyli zasady rozliczalności.

2) Urząd prowadzi RCPD, w którym inwentaryzuje i monitoruje sposób, w jaki wykorzystuje dane osobowe.
3) RCPD jest jednym z podstawowych narzędzi umożliwiających Urzędowi rozliczanie większości obowiązków ochrony danych.
4) W RCPD, dla każdej czynności przetwarzania danych, którą Urząd uznał za odrębną dla potrzeb RCPD, Urząd odnotowuje co najmniej: (a) nazwę czynności, (b) cel przetwarzania, (c) opis kategorii osób, (d) opis kategorii danych, (e) podstawę prawną przetwarzania, wraz z wyszczególnieniem kategorii uzasadnionego interesu Urzędu, jeśli podstawą jest uzasadniony interes, (f) sposób zbierania danych, (g) opis kategorii odbiorców danych (w tym przetwarzających), (h) informację o przekazaniu poza EU/EOG; (i) ogólny opis technicznych i organizacyjnych środków ochrony danych.
5) Wzór RCPD stanowi **Załącznik nr 1 do Polityki - "Wzór Rejestru Czynności Przetwarzania Danych".** Wzór Rejestru zawiera także kolumny nieobowiązkowe.

W kolumnach nieobowiązkowych Urząd rejestruje informacje w miarę potrzeb i możliwości, z uwzględnieniem tego, że pełniejsza treść RCPD ułatwia zarządzanie zgodnością ochrony danych i rozliczenie się z niej.

11. Podstawy przetwarzania.

1) Urząd dokumentuje w RCPD podstawy prawne przetwarzania danych dla poszczególnych czynności przetwarzania.
2) Wskazując ogólną podstawę prawną (zgoda, umowa, obowiązek prawny, żywotne interesy, zadanie publiczne/władza publiczna, uzasadniony cel Urzędu) Urząd dookreśla podstawę w czytelny sposób, gdy jest to potrzebne. Np. dla zgody pracownika Urzędu wskazując na jej zakres, gdy podstawą jest prawo - wskazując na konkretny przepis i inne dokumenty, np. umowę, porozumienie, żywotne interesy - wskazując na kategorie zdarzeń, w których się zmaterializują, uzasadniony cel - wskazując na konkretny cel, np. marketing własny, dochodzenie roszczeń.
3) Urząd wdraża metody zarządzania zgodami umożliwiające rejestrację i weryfikację posiadania zgody osoby na przetwarzanie jej konkretnych danych w konkretnym celu, zgody na komunikację na odległość (email, telefon, sms, in.) oraz rejestrację odmowy zgody, cofnięcia zgody i podobnych czynności (sprzeciw, ograniczenie itp.).
4) Kierownik komórki organizacyjnej Urzędu ma obowiązek znać podstawy prawne,

na jakich komórka przez niego kierowana dokonuje konkretnych czynności przetwarzania danych osobowych. Jeżeli podstawą jest uzasadniony interes Urzędu, kierownik komórki ma obowiązek znać konkretny realizowany przetwarzaniem interes Urzędu.

12. Zgłaszanie naruszenia ochrony danych osobowych organowi nadzorczemu.

1) W przypadku naruszenia w Urzędzie ochrony danych osobowych, Wójt Gminy bez zbędnej zwłoki - w miarę możliwości, nie później niż w terminie 72 godzin po stwierdzeniu naruszenia - zgłasza je organowi nadzorczemu właściwemu zgodnie z art. 55 RODO, chyba że jest mało prawdopodobne, by naruszenie to skutkowało ryzykiem naruszenia praw lub wolności osób fizycznych. Do zgłoszenia przekazanego organowi nadzorczemu po upływie 72 godzin dołącza się wyjaśnienie przyczyn opóźnienia.
2) Zgłoszenie naruszenia w Urzędzie ochrony danych osobowych musi co najmniej:
   a) opisywać charakter naruszenia ochrony danych osobowych, w tym w miarę możliwości wskazywać kategorie i przybliżoną liczbę osób, których dane dotyczą, oraz kategorie i przybliżoną liczbę wpisów danych osobowych, których dotyczy naruszenie;
   b) zawierać imię i nazwisko oraz dane kontaktowe inspektora ochrony danych lub oznaczenie innego punktu kontaktowego, od którego można uzyskać więcej informacji;
   c) opisywać możliwe konsekwencje naruszenia ochrony danych osobowych;
   d) opisywać środki zastosowane lub proponowane przez Urząd w celu zaradzenia naruszeniu ochrony danych osobowych, w tym w stosownych przypadkach środki w celu zminimalizowania jego ewentualnych negatywnych skutków.
3) Wójt Gminy dokumentuje wszelkie naruszenia ochrony danych osobowych, w tym okoliczności naruszenia ochrony danych osobowych w Urzędzie, jego skutki oraz podjęte działania zaradcze.

13. Wyznaczenie Inspektora ochrony danych w Urzędzie.

1) Status prawny i zadania Inspektora ochrony danych regulują przepisy Rozdziału IV Sekcji 4 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.
2) Inspektor ochrony danych w wykonywaniu swoich zadań podlega bezpośrednio

Wójtowi Gminy.

3) Do zadań Inspektora ochrony danych należy w szczególności:
   a) informowanie Wójta Gminy oraz pracowników Urzędu, którzy przetwarzają dane osobowe o obowiązkach wynikających z rozporządzenia RODO oraz innych przepisów Unii Europejskiej lub państw członkowskich o ochronie danych i doradzanie im w tych sprawach;
   b) monitorowanie przestrzegania rozporządzenia RODO, innych przepisów dotyczących ochrony danych osobowych oraz prowadzenie szkoleń wewnętrznych zwiększających świadomość pracowników Urzędu w zakresie zasad dotyczących ochrony danych,
   c) pełnienie funkcji punktu kontaktowego dla właściwych organów i podmiotów zewnętrznych w kwestiach związanych z przetwarzaniem przez Urząd danych osobowych.

14. Załączniki:

1) Wzór rejestru czynności przetwarzanych danych,
2) Polityka zarządzania ryzykiem,
3) Arkusz analizy ryzyka,
4) Instrukcja zarządzania systemem informatycznym w Urzędzie,
5) Regulamin użytkowania komputerów przenośnych,
6) Polityka zachowania poufności i ochrony danych osobowych,
7) Polityka postępowania w przypadku wystąpienia naruszenia systemu ochrony danych osobowych,
8) Wzór rejestru naruszeń,
9) Polityka kluczy,
10) Polityka szkoleń,
11) Polityka Czystego Biurka,
12) Wzór upoważnienia do przetwarzania danych osobowych,
13) Wzór ewidencji osób upoważnionych,
14) Wzór umowy powierzenia,
15) Wzór rejestr umów powierzenia,
16) Wzór oświadczenia o poufności,
17) Wzór wykazu pomieszczeń, w których przechowywane są dane osobowe,
18) Wzory zgód i klauzul informacyjnych
19) Wzór wykazu zabezpieczeń

*Kolorem czerwonym oznaczono informacje wymagane w rejestrze przez art. 30 ust. 1 RODO

	1	2	3	4
LP.	Nazwa czynności przetwarzania	Jednostka organizacyjna (departament, dział itp.)	Cel przetwarzania	Kategorie osób
			Art.. 30 ust. 1 pkt b	Art.. 30 ust. 1 pkt c
1.				
2.				

Załącznik Nr 1 do Polityki ochrony danych osobowych

5	6	7	8
Kategorie danych	**Podstawa prawna**	**Źródło danych**	**Planowany termin usunięcia kategorii danych** *(jeżeli jest to możliwe)*
Art.. 30 ust. 1 pkt c			**Art.. 30 ust. 1 pkt f**

9	10	11	12
Nazwa współadministratora i dane kontaktowe *(jeśli dotyczy)*	**Nazwa podmiotu przetwarzajacego i dane kontakowe** *(jeśli dotyczy)*	**Kategorie odbiorców** *(innych niż podmiot przetwarzajacy)*	**Nazwa systemu lub oprogramowania**
Art.. 30 ust. 1 pkt a	**Art.. 30 ust. 1 pkt d**	**Art.. 30 ust. 1 pkt d**	

13	14	15
		Transfer do kraju trzeciego
Ogólny opis technicznych i organizacyjnych srodków bezpieczeństwa zgodnie z art. 32 ust. 1 *(jeżeli jest to możliwe)*	**DPIA (jeśli tak, lokalizacja raportu)**	**Transfer do kraju trzeciego lub organizacji międzynarodowej (nazwa kraju i podmiotu)**
Art.. 30 ust. 1 pkt g		**Art. 30 ust. 1 pkt e**

16
lub org. międzynarodowej
Jeśli transfer i art. 49 ust. 1 akapit drugi - dokumentacja odpowiednich zabezpieczeń
Art. 30 ust. 1 pkt e

Załącznik Nr 2 do Polityki Ochrony Danych Osobowych

Polityka Zarządzania Ryzykiem
w procesie przetwarzania danych osobowych
w Urzędzie Gminy Naruszewo

Rozdział 1
Postanowienia ogólne
§ 1.

Celem analizy ryzyka jest zastosowanie środków technicznych i organizacyjnych zapewniających stopień bezpieczeństwa odpowiadający ryzyku wynikającemu z przypadkowego lub niezgodnego z prawem zniszczenia, utraty, modyfikacji, nieuprawnionego ujawnienia lub nieuprawnionego dostępu do danych osobowych.

§ 2.

1. Polityka zarządzania ryzykiem w zakresie ochrony danych osobowych, zwana dalej „polityką zarządzania ryzykiem", obejmuje:

1) zakres zadań i obowiązków podmiotów uczestniczących w procesie zarządzania ryzykiem;
2) zasady i tryb identyfikacji ryzyka;
3) zasady i tryb dokonywania analizy ryzyka;
4) zasady określania właściwej reakcji na ryzyko.

§ 3.

Polityka zarządzania ryzykiem ma zastosowanie dla wszystkich pracowników jednostki.

§ 4.

Zarządzanie ryzykiem jest procesem ciągłym i nie ogranicza się do działań określonych w § 2 ust. 1.

§ 5.

1. Celem zarządzania ryzykiem jest zwiększenie prawdopodobieństwa osiągnięcia wyznaczonych celów i zadań w zakresie ochrony danych osobowych, poprzez ograniczenie prawdopodobieństwa wystąpienia ryzyka oraz zabezpieczanie się przed jego skutkami. Następuje to poprzez:

1) rozpoznanie – czyli identyfikowanie ryzyka, określenie rodzajów ryzyk, które wiążą się z działalnością placówki w zakresie ochrony danych osobowych i dokonywanie ich pomiaru;

2) analiza ryzyka ocenę ryzyka i jego istotności, przy pomocy skali określonej w § 7;

3) zarządzanie ryzykiem, które polega na badaniu efektywności i skuteczności podejmowanych działań, poprzez system kontroli instytucjonalnej i zewnętrznej;

4) kontrolę zarządzania ryzykiem, której istotą podjętych działań jest ocena zastosowanych metod redukcji ryzyka, prowadząca do skutecznego i efektywnego realizowania celów i nałożonych zadań.

Rozdział 2
Zakresy zadań i obowiązków

§ 6.

1. Za realizację polityki zarządzania ryzykiem odpowiada Wójt Gminy poprzez:

1) kształtowanie i wdrażanie polityki zarządzania ryzykiem;
2) nadzór i monitorowanie skuteczności procesu zarządzania ryzykiem;
3) wyznaczanie poziomu akceptowalnego dla każdego ryzyka;
4) podejmowanie decyzji dotyczących sposobu reakcji na poszczególne ryzyka.

2. Pracownicy odpowiadają za zarządzanie ryzykiem poprzez:

1) identyfikację ryzyk związanych z realizacją przydzielonych zadań w zakresie ochrony danych osobowych;
2) wskazywanie właścicieli zidentyfikowanych ryzyk;
3) przeprowadzanie analizy zidentyfikowanego ryzyka we współpracy z IOD;
4) proponowanie sposobu postępowania w odniesieniu do poszczególnych ryzyk;
5) wdrażanie działań zaradczych w stosunku do zidentyfikowanego ryzyka.

3. Pracownicy są zobowiązani do współpracy z Wójtem oraz IOD.

Rozdział 3
Opis metody analizy ryzyka

§ 7.

1. Analizę ryzyka przeprowadza się stosując metodę matematyczną z wykorzystaniem arkusza kalkulacyjnego EXCEL. Celem analizy ryzyka jest zastosowanie środków technicznych i organizacyjnych zapewniających stopień bezpieczeństwa odpowiadający ryzyku wynikającemu z przypadkowego lub niezgodnego z prawem zniszczenia, utraty, modyfikacji, nieuprawnionego ujawnienia lub nieuprawnionego dostępu do danych osobowych.

Definicje

1) Aktywa – środki materialne i niematerialne mające wpływ na przetwarzanie danych osobowych
2) Naruszenie (Incydent) ochrony danych osobowych - to 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
3) Zagrożenie - potencjalne naruszenie (potencjalny incydent)
4) Skutki - rezultaty niepożądanego incydentu (straty w wypadku wystąpienia zagrożenia)

5) Ryzyko - prawdopodobieństwo, że określone zagrożenie wystąpi i spowoduje straty lub zniszczenie zasobów

Wyznaczenie zbiorów do analizy ryzyka z aktywami

6) Analizie ryzyka poddawane są zbiory danych osobowych lub procesy przetwarzania
7) Do analizy wymagane jest zidentyfikowanie aktywów na podstawie rejestrów zbiorów.

Wyznaczenie zagrożeń

8) Administrator z IOD jest odpowiedzialny za określenie listy możliwych zagrożeń, które mogą wystąpić w przetwarzaniu danych w zbiorze lub w procesie przetwarzania

Wyliczenie ryzyka dla zagrożeń

9) Administrator określa Prawdopodobieństwo (**P**) wystąpienia poszczególnych zagrożeń w zbiorze lub w procesie przetwarzania
10) Proponowaną skalę prawdopodobieństwa prezentuje Tabela A
11) Administrator określa Skutki (**S**) wystąpienia incydentów (materializacji zagrożeń), uwzględniając straty finansowe, utratę reputacji, sankcje/skutki karne
12) Proponowaną Skalę skutków prezentuje Tabela B
13) Administrator wylicza Ryzyka (R) dla wszystkich zagrożeń i ich skutków w/g formuły:

14) Administrator porównuje wyliczone ryzyka ze skalą i podejmuje decyzje dotyczące dalszego postępowania z ryzykiem
15) Proponowaną skalę Ryzyka prezentuje Tabela C

Tabela C POZIOM RYZYKA	**WARTOŚĆ [R = P*S]**
ryzyko pomijalne i akceptowalne (akceptujemy)	1-2
ryzyko jest opcjonalne (akceptujemy albo obniżamy)	3-6
ryzyko jest nieakceptowalne (musimy obniżyć)	9

Reakcja na wartość ryzyka

16) Akceptacja ryzyka – zabezpieczenia są właściwe – brak potrzeby stosowania dodatkowych zabezpieczeń
17) Działania obniżające ryzyko, które może zastosować Administrator:
    a) Przeniesienie –przerzucenie ryzyka (outsourcing, ubezpieczenie)
    b) Unikanie – eliminacja działań powodujących ryzyko (np. zakaz wynoszenia komputerów przenośnych poza obszar organizacji)
    c) Redukcja – zastosowanie zabezpieczeń w celu obniżenia ryzyka (np. zaszyfrowanie pendrivów z danymi wynoszonych poza firmę)

PLAN POSTĘPOWANIA Z RYZYKIEM

18) Wszędzie, gdzie Administrator decyduje się obniżyć ryzyko, wyznacza listę zabezpieczeń do wdrożenia, termin realizacji i osoby odpowiedzialne
19) Administrator zobowiązany jest do monitorowania wdrożenia zabezpieczeń

PONOWNA ANALIZA RYZYKA

20) Ponowna analiza ryzyka przeprowadzana jest cyklicznie lub po znaczących zmianach w przetwarzaniu danych (np. przetwarzanie nowych zbiorów, nowych procesów przetwarzania, zmiany prawne)

21) W przypadku, gdy analiza ryzyka prowadzona jest w ramach Oceny skutków, wymagana jest do przeprowadzenia przynajmniej raz na 3 lata.

Rozdział 5
Reakcja na ryzyko
§ 9.

1. Dla każdego istotnego zidentyfikowanego ryzyka właściciel ryzyka wskazuje optymalną reakcję. Przyjmuje się niżej wymienione reakcje na ryzyko:

1) tolerowanie – będzie to miało miejsce w przypadkach, kiedy koszty skutecznego przeciwdziałania ryzyku mogą przekraczać jego potencjalne korzyści, z zdolności do skutecznego przeciwdziałania są ograniczone lub wykraczające poza decyzje i działania wewnętrzne;

2) przeniesienie – dotyczyć to będzie kategorii ryzyk w odniesieniu do których nastąpi przeniesienie ich na inna instytucję, między innymi poprzez ubezpieczenie lub zlecenie usług na zewnątrz;

3) wycofanie się – dotyczyć to będzie grypy ryzyk dla których mimo podejmowanych działań nie udało się zmniejszyć ich istotności do akceptowanego poziomu;

4) przeciwdziałanie – dotyczyć to będzie kategorii ryzyk, które wymagać będą podjęcia zdecydowanych, przemyślanych i zaplanowanych działań prowadzących do ich likwidacji, lub znacznego ograniczenia.

§ 6

Identyfikacja zagrożeń i określenie ich poziomu

Dla środowiska budynków rozważano następujące zagrożenia:

Zagrożenie	Opis	Rodzaj zagrożeń
Phishing	Mail z prośbą o zalogowanie się do „podróbki" strony, np. bankowej, lub pseudo konta gmail i w rezultacie przejęcie hasła.	Ataki socjotechniczne
cybersquatting	Zachęcanie do zalogowania się do podrobionej strony o „wiarygodnym" adresie	Ataki socjotechniczne

	www. Zamiastlogować się do www.mbank.pl logowanie byłoby w www.mbank.pl	
wyłudzanie informacji	• Maile od „przełożonych" do księgowego z dyspozycją wykonania przelewu • Faxy, w których intruz podszywa się pod dostawcę i informuje o zmianie numeru konta bankowego. • Maile lub rozmowy tel., w których intruz podaje się np. za pracownika firmy dostarczającej oprogramowanie i prosi o hasło w celu „przetestowania uprawnień"	Ataki socjotechniczne
nakłanianie do wykonania czynności	Maile, które zachęcają lub „zmuszają" do otwarcia załączników lub kliknięcia na hiperilnk, wpisywanie komend	Ataki socjotechniczne
podrzucone nośniki danych	Pen drive pozostawiony w biurze	Ataki socjotechniczne
ataki telefoniczne	• Intruz przedstawia się jako pracownik dostawcy łącza naprawiający usterkę i prosi o uruchomienie określonej strony internetowej. • Intruz przedstawia się jako inżynier Microsoftu lub programista dostawcy oprogramowania. Podsyła „aktualizację" lub prosi o udostępnienie pulpitu	Ataki socjotechniczne
łamanie i pozyskiwanie haseł	• Łamanie metodami słownikowymi i siłowymi • Ujawnianie haseł • Nieprawidłowe przechowywanie (karteczki, pliki) • Odgadywanie zbyt słabych, najpopularniejszych haseł • Stosowanie domyślnych haseł producenta • Stosowanie słownikowych haseł (np. 8 znaków z 3 grup: „Grażynka1") • Stosowanie jednego hasła do wielu (często wszystkich) systemów	Ataki na infrastrukturę
Ataki na sprzęt	• Włamania do urządzeń nieaktualizowanych *Urządzenia sieciowe (routery, access pointy, firewalle) oraz inne np. macierze, dyski NAS działają dzięki umieszczonemu na nich oprogramowaniu. To oprogramowanie, jak każde inne podlega testom*	Ataki na infrastrukturę

	bezpieczeństwa i znajdowane są w nim dziury. Brak aktualizacji tego oprogramowania skutkuje podatnością na włamania, kradzież danych, zakłócanie pracy... • Włamania do urządzeń nieodpowiednio skonfigurowanych *Błędy konfiguracyjne popełniane przez administratorów mogą ułatwiać hackerom włamanie się do sieci lub urządzenia. Powodem jest najczęściej brak profesjonalnej wiedzy u osób konfigurujących urządzenia. Przykładem może być pozostawienie domyślnych haseł lub dostępu do strony konfiguracyjnej z poziomu Internetu.* • • Włamania z użyciem niezabezpieczonych interfejsów lokalnych *Urządzenia takie jak routery, switche, firewalle posiadają często porty konfiguracyjne (USB, Ethernet lub COM - szeregowe), które podłącza się do komputera aby skonfigurować urządzenie. Dostęp do tych portów powinien być odpowiednio zabezpieczonych hasłem, aby przypadkowa osoba, która podłączy do nich swój komputer nie mogła zmienić konfiguracji. Administratorzy często jednak pozostawiają te porty niezabezpieczone.* • Włamania za pośrednictwem niepotrzebnych usług (np. telnet na routerze) *Urządzenia sieciowe posiadają często włączone wszystkie możliwe usługi sieciowe (DHCP, DNS, SSH, HTTP, telnet, FTP), mimo iż nie wszystkie z nich są potrzebne w danym środowisku. Każda z tych usług jest obsługiwana przez oprogramowanie, które może zawierać błędy. Wyłączenie niepotrzebnych serwisów ogranicza ilość dziur i możliwość przechwycenia / podsłuchania ruchu lub haseł. Włączone powinny być tylko te usługi, które są niezbędne do działania danego*	

	środowiska.	
Ataki na oprogramowanie	• Wykorzystanie znanych dziur w nieaktualizowanym oprogramowaniu *W każdym oprogramowaniu (przeglądarki, pakiety biurowe, systemy operacyjne, systemy serwerowe...) prędzej czy później znajdowane są błędy pozwalające na przełamania zabezpieczeń i uzyskanie zdalnego dostępu lub zdalne wykonanie kodu. Informacje o tych błędach są upubliczniane po tym, jak producent oprogramowania przygotuje odpowiednią latę lub aktualizację. Jeżeli nie zainstalujemy tych aktualizacji, narażamy się na ryzyko, że ktoś wykorzysta ogólnodostępne informacje o znanych błędach aby włamać się, wykraść dane, lub w inny sposób nam zaszkodzić. (nieaktualizowany Windows 7)* • Włamania z wykorzystaniem luk typu zero day *Zero-day to błędy w oprogramowaniu, o których informacje zostają upublicznione zanim jeszcze autor oprogramowania zdąży wypuścić aktualizację. Często pojawiają się narzędzia umożliwiające wykorzystanie tych błędów (exploity) i przełamanie zabezpieczeń skutkujące włamaniem, kradzieżą danych itp. Innymi słowy - Zero day – podatność sprzętu lub oprogramowania znana wąskiej grupie osób i pozwalająca na przełamanie zabezpieczeń, na którą producent nie dostarczył jeszcze odpowiedniej aktualizacji* • Włamania z wykorzystaniem domyślnych haseł *Włamania będące wynikiem tego, że administrator po uruchomieniu oprogramowania lub urządzenia nie zmienił domyślnego hasła. Intruz, któremu uda się rozpoznać model urządzenia w pierwszej kolejności próbuje się do niego zalogować hasłem podanym w instrukcji obsługi przez*	Ataki na infrastrukturę

	producenta. Często się to niestety udaje. • Włamania z wykorzystaniem najczęstszych błędów *Programiści pisząc oprogramowanie często popełniają te same znane błędy. Istnieje zestawienie takich błędów, np. dla aplikacji webowych - OWASP TOP 10. Wiele programów i stron internetowych pada ofiarą ataków właśnie za pośrednictwem tych najczęstszych błędów.* • Włamania z wykorzystaniem API (interfejsów programistycznych) *Niektóre aplikacje, systemy ale też serwisy internetowe (np. Allegro) posiadają specjalne interfejsy, dzięki którym programiści używając odpowiednich bibliotek mogą odwoływać się do nich z poziomu oprogramowania, Możliwe jest np. wystawienie aukcji na allegro bez konieczności logowania się na swoje konto przeglądarką internetową. Błędy w tych bibliotekach powodowały często, że programista mógł np. uzyskać szerszy dostęp do bazy danych i wyciągnąć dane wszystkich klientów.* • Namierzanie wersji testowych (np. strona www) *Niektóre portale lub aplikacje webowe posiadają swoje kopie utrzymywane do celów testowych lub rozwojowych. Programiści zamieszczają na nich zmiany w kodzie zanim trafią one na główne serwery. Strony te są często gorzej zabezpieczone i latwiej jest się do nich włamać, a mogą zawierać również krytyczne dane. Często udaje się je namierzyć wpisując np. zamiast adresu www.strona.pl adres test.strona.pl .*	
Skanowanie sieci i usług	Atakujący poznaje wersję systemu operacyjnego lub wersję serwera www a przez to potem może dobrać skuteczny atak	Ataki na infrastrukturę
Podsłuchanie transmisji (okablowanie, wifi, telefonia, internet)	Łatwo dostępne gniazdka sieciowe, gdzie atakujący może się podłączyć np. z własnym urządzeniem i za jego pomocą podsłuchiwać naszą sieć (możliwość podpięcia się pod drukarkę na korytarzu lub do gniazdka w	Ataki na infrastrukturę

	salce konferencyjnej)	
ATAKI MAN-IN-THE-MIDDLE	Przejęcie komputera w firmie w celu podsłuchiwania w sieci firmowej (w rezultacie możliwość podsłuchu haseł)	Ataki na infrastrukturę
Eskalacja uprawnień	• Zwiększenie uprawnień użytkownika przez wykorzystanie błędów programistycznych • Przejęcie uprawnień użytkownika zaawansowanego • Przejęcie uprawnień administratora • Przejęcie uprawnień systemowych • Przejęcie innych poświadczeń (certyfikaty elektroniczne, pliki cookies z identyfikatorami sesji)	Ataki na infrastrukturę
DOS	Zmasowany atak pojedynczego atakującego na jakąś stronę www lub na portal, aby ją przeciążyć i „zakorkować"	Ataki na infrastrukturę
DDOS	Zmasowany atak komputerów-zombie na zlecenie atakującego na jakąś stronę www lub na portal, aby ją przeciążyć i „zakorkować"	Ataki na infrastrukturę
Wirusy i trojany	Trojany – instalują się często z nielegalnym oprogramowaniem. Zawierają ukrytą funkcjonalność, działają na szkodę użytkownika.	Złośliwe oprogramowanie
Backdoory	Instalują się z maili lub z linków w mailach. Po uruchomieniu umożliwiają intruzowi ponowny dostęp i stałą kontrolę nad komputerem. Taki komputer-zombie może być użyty do wszelkich zachcianek intruza.	Złośliwe oprogramowanie
Keyloggery	Programy przechwytujące hasła wpisywane na klawiaturze przez użytkownika i oddające je intruzowi.	Złośliwe oprogramowanie
Ransomeware	Program do szyfrowania plików. Odszyfrowanie wymaga zapłaty 500 USD. Bardzo groźny	Złośliwe oprogramowanie
Exploity / exploitpaki	Oprogramowanie wykorzystujące znane luki w systemach. Uruchomiony pozwala na przejęcie systemu przez intruza.	Złośliwe oprogramowanie
Włamanie do obiektów	Może skutkować zainstalowaniem nieautoryzowanych urządzeń, np. keyloggerów, podsłuchów	Zagrożenia dla sprzętu
Kradzież / zniszczenie sprzętu	kradzież komputerów w organizacji i laptopów poza nią, uszkodzenie sprzętu na skutek przepięcia, czy upadku	Zagrożenia dla sprzętu
Pożar / eksplozja	– pożar serwerowni, wybuch gazów technicznych	Zagrożenia dla sprzętu
Zalanie	– np. powódź, pęknięta rura kanalizacyjna, zalanie kawą	Zagrożenia dla sprzętu

Przegrzanie	– wysoka temperatura w serwerowni	Zagrożenia dla sprzętu
Awaria zasilania	– skoki napięcia / przerwy w dostawie	Zagrożenia dla sprzętu
Awaria sprzętu	– awaria dysków, modułów, płyty głównej, sterowników, routerów	Zagrożenia dla sprzętu
Nieuprawniony dostęp	– nadane zbyt wysokie uprawnienia użytkownikom lub brak kontroli nad dostępem do plików, baz, komputerów	Zagrożenia dla danych
Kradzież tożsamości	przejęcie poczty, np. mailowej, pozyskanie danych z dowodu osobistego i w rezultacie no. założenie firmy „słupa", wzięcie kredytu, zakup na allegro na cudze konto	
Nieuprawniona modyfikacja / usunięcie	– może mieć również charakter niezamierzony lub być efektem pomyłki - sfałszowanie danych przez osoby z wewnątrz lub zewnątrz organizacji	Zagrożenia dla danych
Nieuprawnione kopiowanie danych	- kopiowanie danych z katalogów, dysków, baz, programów, kserowanie i robienie zdjęć przez pracownika lub przez osobę obcą	Zagrożenia dla danych
Kradzież danych lub nośników	Na zewnątrz i wewnątrz organizacji	Zagrożenia dla danych
Utrata / kradzież danych dostępowych	haseł, kluczy, certyfikatów	Zagrożenia dla danych
Błąd / awaria oprogramowania	– uszkodzenie bazy danych, programu kadrowo-płacowego	Zagrożenia dla danych
Brak / błędy w wykonywaniu kopii bezpieczeństwa	– doraźne lub za rzadkie wykonywanie kopii, błędy podczas procesu wykonywania kopii, kopie dostępne w sieci bez zabezpieczeń	Zagrożenia dla danych
Udostępnianie danych osobom nieupoważnionym	– upublicznienie danych w przestrzeni publicznej, dostęp przez internet, przesłanie lub wydawanie informacji osobie nieupoważnionej, wyrzucanie na śmietnik, wynoszenie na wolne powietrze	Zagrożenia dla danych
Nieprawidłowe / brak procedur niszczenia nośników z danymi –	wyrzucenie uszkodzonych nośników bez ich zniszczenia, wyrzucenie niezniszczonych pendrive, DVD	Zagrożenia dla danych
Nieprawidłowe / brak procedur napraw w serwisach zewnętrznych	– naprawa sprzętu z nośnikami w serwisie bez standardu bezpiecznej naprawy i bez umowy bezpieczeństwa	Zagrożenia dla danych
Nieprzestrzeganie procedur	– świadome naruszenie pisemnych lub ustnych procedur, np. niewylogowywanie się z systemu, przekazywanie haseł koledze	Błędy ludzkie
Pomyłki administratorów, użytkowników	pomyłkowe udostępnienie, wysłanie do złego odbiorcy, błędne zabezpieczenia	Błędy ludzkie
Brak świadomości / wiedzy	braki w inteligencji, nieprzeszkolony personel	Błędy ludzkie

Błędy projektowe / konfiguracyjne	– błędy programistów prowadzące do niewłaściwego przetwarzania danych, niezabezpieczenie danych w bazie www przed indeksacją robotów google	Błędy ludzkie
Brak aktualnej dokumentacji	Brak instrukcji, opisów, dokumentacji technicznej sprzętu i oprogramowania utrudnia przywracanie środowiska i zarządzanie nim gdy np. odejdzie pracownik IT	Zagrożenia ciągłości działania
Nieprawidłowe / brak umowy o współpracy	brak odpowiedzialności stwarza ryzyko braku staranności	Zagrożenia ciągłości działania
Nieprawidłowe / brak umowy gwarancyjnej lub wsparcia serwisowego	– umowy wymagają przedłużania, czas reakcji nie oznacza czasu naprawy	Zagrożenia ciągłości działania
Upadek firmy outsourcingowej lub dostawczej –	ryzyko braku zastępstw, np. dla hostingodawcy poczty, dla wsparcia do zakupionej aplikacji	Zagrożenia ciągłości działania
Awaria łączy telekomunikacyjnych –	krytyczna w przypadku usług chmurowych oraz platform SaaS	Zagrożenia ciągłości działania

Rozdział 7
Postanowienia końcowe.

§ 10.

1. Strategia zarządzania ryzykiem obowiązuje od 25 maja 2018 roku.

2. Pracownicy jednostki obowiązani są do systematycznej analizy wystąpienia ryzyk na stanowiskach pracy i zgłaszania ich Wójtowi i/lub IOD.

Załącznik Nr 3 do Polityki Ochrony Danych Osobowych

ARKUSZ ANALIZY RYZYKA

P-Prawdopodobieństwo incydentu (skala od 1 do 3) **S-Skutki wystąpienia incydentu (skala od 1 do 3)** **R-Ryzyko wystąpienia incydentu (skala od 1 do 9)** **Formuła: R=P*S**	Informacje P / S / R	Programy, systemy operacyjne P / S / R	Infrastruktura IT P / S / R	Infrastruktura P / S / R	Pracownicy i współpracownicy P / S / R	Outsourcing P / S / R
phishing						
cybersquatting						
wyłudzanie informacji						
nakłanianie do wykonania czynności						
podrzucanie nośników danych						
ataki telefoniczne						
łamanie haseł (słownikowe, siłowe)						
ataki na sprzęt						
ataki na oprogramowanie						
skanowanie sieci i usług						
podsłuchiwanie transmisji (okablowanie, wifi, telefonia, internet)						
ataki man-in-the-middle						
eskalacja uprawnień						
DOS						
DDOS						

wirusy / trojany	
backdoory	
keyloggery	
ransomeware	
exploity / exploitpacki	
kradzież / zniszczenie sprzętu	
pożar / eksplozja	
zalanie	
przegrzanie	
awaria zasilania	
awaria sprzętu	
nieuprawniony dostęp	
kradzież tożsamości	
nieuprawniona modyfikacja / usunięcie	
nieuprawnione kopiowanie danych	
kradzież danych lub nośników	
utrata / kradzież danych dostępowych (hasła, klucze, certyfikaty)	
błąd / awaria oprogramowania	
brak / błędy w wykonywaniu kopii bezpieczeństwa	
udostępnienie danych osobom nieupoważnionym	
fałszowanie danych	

nieprawidlowe / brak procedur niszczenia nośników z danymi																								
nieprawidłowe / brak procedur napraw w serwisach zewnętrznych																								
nieprzestrzeganie procedur																								
pomyłki																								
brak świadomości / wiedzy																								
błędy projektowe / konfiguracyjne																								
brak aktualnej dokumentacji																								
nieprawidłowe / brak umowy o współpracy																								
nieprawidłowe / brak umowy gwarancyjnej lub wsparcia serwisowego																								
upadek firmy outsourcingowej lub dostawczej																								
awaria łączy telekomunikacyjnych																								

Załącznik Nr 5 do Polityki Ochrony Danych Osobowych

Regulamin użytkowania komputerów przenośnych

1. Pracownicy upoważnieni do przetwarzania danych osobowych i pracujący na komputerach przenośnych muszą zapoznać się z Regulaminem użytkowania komputera przenośnego oraz pisemnego zobowiązania się do jego przestrzegania.
2. Dane osobowe muszą zostać zaszyfrowane na dysku i zabezpieczone co najmniej 8 znakowym hasłem (duże, małe litery i cyfry).
3. Komputery przenośne są wykorzystywane do prac służbowych. W przypadku konieczności korzystania z komputera przenośnego w innym celu wszystkie dane osobowe muszą być zabezpieczone hasłem.
4. W przypadku kradzieży / zgubienia lub naruszenia ochrony danych osobowych osoba upoważniona zobowiązana jest zgłosić zdarzenie / problem Inspektorowi Ochrony Danych.
5. Osoba upoważniona zobowiązana jest do zabezpieczenia komputera przenośnego w czasie transportu, a przede wszystkim:

    1) zaleca się przenoszenie komputera przenośnego w zwykłej teczce, aktówce,
    2) zabrania się pozostawiania komputera przenośnego w samochodzie podczas nieobecności osoby upoważnionej.

6. Gdy komputer przenośny jest pozostawiony w miejscu dostępnym dla osób nieupoważnionych, konieczne jest zabezpieczenie hasłem. Dotyczy to przede wszystkim zabezpieczenia komputera przenośnego na stanowisku pracy, podczas przedstawiania prezentacji, szkolenia.
7. Użytkownik komputera przenośnego jest zobowiązany do regularnego tworzenia kopii bezpieczeństwa danych na serwerze. Nośniki z takimi kopiami powinny być przechowywane w miejscu zabezpieczonym przed dostępem osób nieupoważnionych.
8. Pracując na komputerze przenośnym w miejscach publicznych osoba upoważniona zobowiązana jest do chronienia wyświetlanych danych osobowych na monitorze przed wglądem osób nieupoważnionych.

Załącznik Nr 6 do Polityki Ochrony Danych Osobowych

POLITYKA ZACHOWANIA POUFNOŚCI I OCHRONY DANYCH OSOBOWYCH

1. Każda z osób dopuszczona do przetwarzania danych osobowych jest zobowiązana do:
    a. przetwarzania danych osobowych wyłącznie w zakresie i celu przewidzianym w powierzonych przez Pracodawcę zadaniach,
    b. zachowania w tajemnicy danych osobowych do których ma dostęp w związku z wykonywaniem zadań powierzonych przez Pracodawcę,
    c. niewykorzystywania danych osobowych w celach niezgodnych z zakresem i celem powierzonych zadań przez Pracodawcę,
    d. zachowania w tajemnicy sposobów zabezpieczenia danych osobowych,
    e. 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,
2. osoba przed dopuszczeniem do przetwarzania odbywa szkolenie z zasad ochrony danych osobowych
3. Osoby zapoznane z treścią niniejszego Regulaminu ODO lub przeszkolone zobowiązane są podpisać Oświadczenie o poufności.
4. Zabrania się przekazywania bezpośrednio lub przez telefon danych osobowych osobom nieupoważnionym lub osobom których tożsamości nie można zweryfikować lub osobom podszywającym się pod kogoś innego.
5. Zabrania się przekazywania lub ujawniania danych osobom lub instytucjom, które nie mogą wykazać się podstawą prawną do dostępu do takich danych.
6. Zabrania się ujawniania na grupach dyskusyjnych, forach internetowych itp. jakichkolwiek szczegółów dotyczących funkcjonowania jednostki, w tym informacji na temat sprzętu i oprogramowania, z jakiego korzysta jednostka, oraz informacji kontaktowych innych, niż ogólnodostępne w materiałach zewnętrznych.

Załącznik Nr 7 do Polityki Ochrony Danych Osobowych

POLITYKA POSTĘPOWANIA W PRZYPADKU WYSTĄPIENIA NARUSZENIA SYSTEMU OCHRONY DANYCH OSOBOWYCH

§ 1

W przypadku stwierdzenia naruszenia lub zaistnienia okoliczności wskazujących na naruszenie systemu ochrony danych osobowych użytkownik zobowiązany jest do bezzwłocznego powiadomienia o tym fakcie Administratora oraz IOD.

§ 2

1. Użytkownik do momentu przybycia IOD powinien:

a) zabezpieczyć dostęp do pomieszczenia lub urządzenia;

b) powstrzymać się od rozpoczęcia lub kontynuowania jakichkolwiek czynności mogących spowodować zatarcie śladów, bądź dowodów naruszenia ochrony;

c) zatrzymać pracę na komputerze, na którym zaistniało naruszenie ochrony oraz nie uruchamiać innych urządzeń, które mogą mieć związek z naruszeniem ochrony;

d) podjąć stosownie do zaistniałej sytuacji działania, które zapobiegną ewentualnej utracie danych osobowych.

§ 3

1. IOD po otrzymaniu informacji o naruszeniu lub próby naruszenia zabezpieczenia systemu przetwarzającego dane osobowe, podejmuje działania zmierzające do usunięcia powstałego zagrożenia.

2. Po przybyciu na miejsce, o którym mowa w ust. 1, IOD realizuje czynności w kolejności:

a) ocenia sytuację, uwzględniając stan pomieszczenia, w którym przetwarzane są dane, stan urządzenia i zbioru oraz identyfikuje zakres negatywnych następstw naruszenia ochrony danych osobowych;

b) wysłuchuje relacji użytkownika lub osoby, która dokonała powiadomienia;

c) podejmuje działania mające na celu ustalenie sprawcy, miejsca, czasu i sposobu dokonania naruszenia ochrony;

d) w zależności od zakresu naruszenia ochrony podejmuje decyzje o dalszym postępowaniu, wydając użytkownikowi stosowne polecenia i wskazówki do obsługi urządzeń;

e) biorąc pod uwagę skalę oraz skutki naruszenia ochrony, IOD decyduje o powołaniu doraźnego zespołu i powiadomieniu o zdarzeniu Administratora lub osobę upoważnioną przez niego.

§ 4

1. IOD z przebiegu zdarzenia sporządza notatkę, która obejmuje:

a) dane osoby stwierdzającej naruszenie ochrony;

b) datę, godzinę i miejsce naruszenia ochrony;

c) rodzaj naruszenia ochrony;

d) czas powiadomienia o zdarzeniu;

e) opis podjętych czynności;

f) wnioski do realizacji.

2. Notatkę, o której mowa w ust. 1, IOD przekazuje Administratorowi.

§ 5

Zgodę na ponowne uruchomienie komputera lub innych urządzeń oraz kontynuowanie przetwarzania danych, wyraża IOD.

§ 6

Dokonywanie zmian w miejscu naruszenia ochrony bez zgody, o której mowa w § 5 jest dopuszczalne tylko w wypadku konieczność ratowania osób, mienia albo zapobiegania powstaniu innego niebezpieczeństwa.

§ 7

1. W przypadku powołania doraźnego zespołu, o którym mowa w § 3 ust. 2 lit. e) pracą jego kieruje IOD.

2. Zespół z przeprowadzonych czynności sporządza protokół, w którym ujmuje skalę stwierdzonych naruszeń ochrony, przyczyny ich powstania oraz skutki, jakie wpłynęły lub wpłynąć mogą na stan zabezpieczenia i ochrony danych osobowych.

3. Protokół zawierać powinien wnioski określające zakres działań organizacyjnych i technicznych, zapobiegających w przyszłości naruszeniom ochrony danych osobowych.

4. Protokół przekazywany jest Administratorowi w celu akceptacji wniosków i zaleceń usprawniających zabezpieczenia ochrony danych.

§ 8

W przypadku stwierdzenia:

a) błędu użytkownika systemu – IOD przeprowadza dodatkowe szkolenie osób zatrudnionych przy przetwarzaniu danych w komórce organizacyjnej;

b) uaktywnienia wirusa – należy zgłosić IOD, który ustali źródło jego pochodzenia oraz uaktualni zabezpieczenia antywirusowe;

c) zaniedbania ze strony użytkownika – należy w stosunku do niego zastosować konsekwencje wynikające z właściwych przepisów prawa;

d) włamania, w celu nielegalnego pozyskania danych – należy dokonać szczegółowej analizy wdrożonych środków zabezpieczenia i zapewnić skuteczniejszą ochronę

e) złego stanu urządzenia lub złego działania programu – należy niezwłocznie powiadomić IOD i przeprowadzić kontrolę czynności serwisowo-programowych.

§ 9

W przypadku naruszenia ochrony danych osobowych skutkującego ryzykiem naruszenia praw lub wolności osób fizycznych, Administrator bez zbędnej zwłoki – w miarę możliwości, nie później niż w terminie 72 godzin po stwierdzeniu naruszenia – zgłasza je organowi nadzorczemu.

Załącznik Nr 8 do Polityki Ochrony Danych Osobowych

Rejestr naruszeń ochrony danych osobowych

Rodzaj naruszenia	Obowiązek zgłoszenia organowi nadzorczemu	Obowiązek zawiadomienia osoby, której dane dotyczą	Okoliczności naruszenia	Skutki naruszenia	Podjęte działania zaradcze

Załącznik Nr 9 do Polityki Ochrony Danych Osobowych

POLITYKA KLUCZY
oraz zabezpieczeń pomieszczeń i obiektu

Rozdział I.
Założenia i postanowienia ogólne

§ 1

Ilekroć w niniejszej polityce jest mowa o:

1) Urzędzie - należy przez to rozumieć Urząd Gminy Naruszewo
2) pracownikach - należy przez to rozumieć pracowników Urzędu Gminy Naruszewo
3) ochronie i dozorze - należy przez to rozumieć fizyczną całodobową ochronę obiektu przez pracowników firmy ochroniarskiej

Rozdział II.
Ochrona i dozór obiektu

§ 2

1. Budynek podlega ochronie i dozorowi całodobowo przez pracowników firmy ochroniarskiej.
2. Ochrona pełniona jest w formie stacjonarnej, w razie potrzeby wzywany jest patrol interwencyjny.
3. Szczegółowy zakres obowiązków i ustaleń w zakresie ochrony i dozoru obiektu reguluje umowa zawarta pomiędzy Urzędem, a firmą ochroniarską.

Rozdział III.
Zabezpieczenie pomieszczeń i procedura postępowania z kluczami.

§ 3

1. Wszystkie pokoje, i pomieszczenia pracowników oraz pomieszczenia gospodarcze i techniczne zamykane są na klucz.
2. Miejscem deponowania kluczy w Urzędzie jest w metalowej szafie pok. nr 5
3. Wykaz osób uprawnionych do pobierania kluczy do poszczególnych pomieszczeń znajduje się w sekretariacie

§ 4.

1. Pracownik, który pobrał klucz do danego pomieszczenia przed otwarciem zamków powinien sprawdzić od strony wizualnej, stan tych zamków i ewentualnych zabezpieczeń (np. plomb) zastosowanych przy zamykaniu pomieszczeń.
2. Po otwarciu pomieszczeń biurowych, jeszcze przed przystąpieniem do pracy, pracownicy powinni sprawdzić stan zastosowanych zabezpieczeń sprzętu biurowego i komputerowego, a także składowanej w tych pomieszczeniach dokumentacji i innego wyposażenia.
3. W przypadku stwierdzenia zmian lub naruszenia stanu zabezpieczeń, o których mowa w ust. 1 i 2 , pracownik, który to stwierdził, natychmiast powinien powiadomić o tym swojego bezpośredniego przełożonego.
4. Od momentu pobrania kluczy do momentu ich zdania, na pracowniku tego pomieszczenia, w którym usytuowane jest jego miejsce pracy, spoczywa pełna odpowiedzialność za ochronę pomieszczenia, sprzętu i dokumentów.

§ 5

1. Po zakończeniu dnia pracy, pracownicy zobowiązani są do uporządkowania swoich stanowisk pracy, wykonania czynności zabezpieczających adekwatnych do zastosowanych rozwiązań technicznych i organizacyjnych, głównie polegających na:
1) zabezpieczeniu dokumentacji (tzn. zasada czystego biurka),
2) zabezpieczeniu komputerów, dyskietek, pendrive'ów, płyt CD oraz innych przenośnych nośników pamięci,
3) wyłączeniu wszystkich urządzeń zasilanych energią elektryczną, (czajniki, wentylatory, niszczarki , itp.) zgodnie z zasadami bhp.,
4) zamknięciu szaf, okien i drzwi na klucz,
5) zdaniu kluczy od pomieszczenia na portiernię.

2. Za zabezpieczenie kluczy od magazynów, szaf pancernych, kasetek metalowych, biurek stanowiskowych i szaf biurowych odpowiedzialni są pracownicy, którzy ponoszą pełną odpowiedzialność za powierzone mienie.

Rozdział IV.
Procedury postępowania z kluczami zapasowymi

§ 6

1. Ze względu na bezpieczeństwo Urzędu, zapewniony jest awaryjny, całodobowy dostęp do wszystkich pomieszczeń pracowniczych, gospodarczych i technicznych w budynku.
2. W tym celu ustalony jest obowiązek przechowywania zapasowych kluczy do wszystkich pomieszczeń, w sposób umożliwiający awaryjne korzystanie z nich przez uprawnione osoby.
3. Pełen komplet kluczy zapasowych znajduje się w pokoju nr 5 w metalowych kasetkach.
4. Użycie kluczy zapasowych możliwe jest tylko za zgodą Wójta lub osoby przez niego upoważnionej. Użycie kluczy bez takiej zgody jest uzasadnione tylko w nagłych awaryjnych sytuacjach takich jak pożar, zalanie lub inne zagrożenia.
5. Użycie kluczy zapasowych powinno być udokumentowane każdorazowo w rejestrze, który znajduje się w kasetce metalowej w pomieszczeniu nr 5 razem z zapasowymi kluczami.

Rozdział V.
Postanowienia końcowe

§ 7

1. Zabrania się:
l) dorabiania kluczy do pomieszczeń i budynków Urzędu bez zgody Wójta Gminy,
2) udostępniania kluczy osobom nieupoważnionym,
3) pozostawiania kluczy bez dozoru.
2. Utrzymanie skutecznego zabezpieczenia technicznego budynku Urzędu podlega nadzorowi i kontroli sekretarza gminy.

Załącznik Nr 10 do Polityki Ochrony Danych Osobowych

POLITYKA SZKOLEŃ

1. Każdy Pracownik przed dopuszczeniem do pracy z danymi osobowymi winien być poddany przeszkoleniu i zapoznaniu z przepisami RODO oraz procedur obowiązujących u Pracodawcy związanych z ochroną danych osobowych.
2. Za przeprowadzenie szkolenia odpowiada IOD.
3. W przypadku przeprowadzenia szkolenia wewnętrznego z zasad ochrony danych osobowych jest realizowane udokumentowanie odbycia tego szkolenia.

Załącznik Nr 11 do Polityki Ochrony Danych Osobowych

POLITYKA CZYSTEGO BIURKA

1. Polityka czystego biurka jest częścią Polityki Ochrony Danych Osobowych w Urzędzie i obowiązuje wszystkich pracowników Urzędu.
2. Pracownik:
   a. zobowiązany jest do przechowywania na biurku tylko tych dokumentów, które są mu potrzebne do wykonywania w danym momencie pracy,
   b. nie może przetrzymywać na biurku jedzenia oraz picia,
   c. po zakończonej pracy pracownik zobowiązany jest do zabezpieczenia dokumentów w zamykanej na klucz szafie,
   d. zobowiązany jest do niszczenia dokumentów niepotrzebnych w taki sposób, aby nie było możliwe odtworzenie zawartych w nich informacji, np. w niszczarce.

Załącznik Nr 12 do Polityki Ochrony Danych Osobowych

....., dn. ..... 20..... r.

UPOWAŻNIENIE
DO PRZETWARZANIA DANYCH OSOBOWYCH

Na podstawie art. 29 rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z 27.04.2016 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.Urz. UE L 119, s. 1) – dalej **RODO** – nadaję upoważnienie Pani/Panu:

.....
(imię i nazwisko)

.....
(stanowisko)

do przetwarzania danych osobowych w zakresie pełnionych obowiązków służbowych na zajmowanym stanowisku, tj. uzyskuje Pani/Pan upoważnienie do przetwarzania danych osobowych w zakresie ..... (zakres przetwarzanych danych)

Jednocześnie zobowiązuję Panią/Pana do przetwarzania danych osobowych, zgodnie z udzielonym upoważnieniem oraz z przepisami RODO, ustawy o ochronie danych osobowych, Kodeksu pracy, a także z Polityką ochrony danych osobowych Pracodawcy.

Jednocześnie upoważniam Panią/Pana do tworzenia/posiadania dla potrzeb wykonywanej pracy zestawień, ewidencji oraz rejestrów z danymi osobowymi, z zachowaniem pełnej ich ochrony przy zastosowaniu środków technicznych i organizacyjnych wdrożonych w [.....].

Okres ważności
od:
do:

.....
podpis osoby uprawnionej do nadania upoważnienia

Data wygaśnięcia* .....

Odwołano, dnia .....

.....
podpis osoby uprawnionej do odwołania
upoważnienia

* Data rozwiązania stosunku pracy/umowy cywilnoprawnej

Załącznik Nr 13 do Polityki Ochrony Danych Osobowych

EWIDENCJA OSÓB UPOWAŻNIONYCH DO PRZETWARZANIA DANYCH OSOBOWYCH

L.p.	Imię i nazwisko	Stanowisko/komórka organizacyjna	Zakres przetwarzanych danych	Data nadania upoważnienia	Data ustania upoważnienia
1.					
2.					
3.					
4.					
5.					
6.					
7.					

8.					
9.					
10.					
11.					
12.					
13.					
14.					
15.					

16.					

Załącznik Nr 14 do Polityki Ochrony Danych Osobowych

Umowa powierzenia przetwarzania danych osobowych

zwana dalej „Umową", zawarta w ..... w dniu ....., pomiędzy:

.....
zwanym dalej **„Administratorem"**
a
(pełne dane podmiotu który umowę zawiera, w szczególności: firma spółki, siedziba, adres, oznaczenie sądu rejestrowego, w którym przechowywana jest dokumentacja spółki oraz numer pod którym spółka jest wpisana do rejestru; NIP, wysokość kapitału zakładowego i kapitału wpłaconego – art. 206 lub 374 ksh. W przypadku podmiotów prowadzących działalność gospodarczą imię nazwisko adres zamieszkania osoby fizyczne, PESEL, firma pod jaką działalność jest prowadzona oraz adres głównego miejsca wykonywania działalności),np.:
....., z siedzibą .....,
ul. ....., wpisaną do rejestru przedsiębiorców Krajowego Rejestru Sądowego prowadzonego przez Sąd Rejonowy w ..... Wydział ..... Gospodarczy, pod numerem KRS ....., REGON: ....., NIP: .....,
reprezentowaną przez .....

/

....., prowadzącym/ą działalność gospodarczą w .....,
pod nazwą ....., wpisanym/ą do Centralnej Ewidencji i Informacji o Działalności Gospodarczej Rzeczypospolitej Polskiej, posiadającym/ą NIP: .....
REGON: .....,

/

....., zam. ....., PESEL:
....., dow. os.: .....,
zwanym dalej **„Przetwarzającym",**
lub
*(zwanymi dalej odpowiednio **„Stronami" bądź „Stroną").***

W przypadku, gdy umowa powierzenia danych związana jest z inną umową (Umową Podstawową), można wprowadzić następujący wstęp:

Preambuła

Mając na uwadze, że:

1. *Strony zawarły umowę ..... („**Umowa Podstawowa**"), w związku, z wykonywaniem której Administrator powierzy Przetwarzającemu przetwarzanie danych osobowych zakresie określonym Umową;*
2. *Celem Umowy jest ustalenie warunków, na jakich Przetwarzający wykonuje operacje przetwarzania danych osobowych w imieniu Administratora;*
3. *Strony zawierając Umowę dążą do takiego uregulowania zasad przetwarzania powierzonych danych osobowych, aby odpowiadały one w pełni postanowieniom rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z 27.04.2016 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. Urz. UE L 119, s. 1) – dalej „**Rozporządzenie**",*

Strony postanowiły zawrzeć Umowę o następującej treści:

§ 1
Powierzenie przetwarzania danych osobowych

1. Administrator, w trybie art. 28 rozporządzenia 2016/679 z 27.04.2016 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. Urz. UE L 119 z 04.05.2016 r.) - dalej jako „**Rozporządzenie**", powierza Przetwarzającemu dane osobowe do przetwarzania, na zasadach i w celu określonym w niniejszej Umowie.
2. Przetwarzający zobowiązuje się przetwarzać powierzone mu dane osobowe zgodnie z niniejszą Umową, Rozporządzeniem oraz innymi przepisami prawa powszechnie obowiązującego, chroniącymi prawa osób, których dotyczą przekazywane dane.
3. Przetwarzający oświadcza, że stosuje środki bezpieczeństwa spełniające wymogi Rozporządzenia oraz innych przepisów, o których mowa w ust. 2.

§ 2
Zakres i cel przetwarzania danych

1. Przetwarzający będzie przetwarzał powierzone na podstawie umowy następujące rodzaje danych osobowych: ..... (*należy podać rodzaj danych np. dane zwykłe*) oraz dane dotyczące następujących kategorii osób ..... *(należy podać kategorię osób, których dane dotyczą np. pracowników administratora, lokatorów itp.)* w postaci .....*(np. imion i nazwisk, adresu zamieszkania, nr PESEL itp.).*
2. Powierzone przez Administratora dane osobowe będą przetwarzane przez Przetwarzającego wyłącznie w celu.....*(należy podać cel przetwarzania danych przez podmiot przetwarzający, np. realizacji umowy z dnia .....nr .....w zakresie dowozu dzieci niepełnosprawnych do szkół, organizacji zajęć rekreacyjnych itp.).*

§ 3
Sposób wykonania umowy w zakresie przetwarzania danych osobowych

1. Przetwarzający zobowiązuje się przy przetwarzaniu powierzonych danych, wskazanych w §2, do ich zabezpieczenia poprzez stosowanie odpowiednich środków technicznych

i organizacyjnych, zapewniających adekwatny stopień bezpieczeństwa, odpowiadający ryzyku związanemu z przetwarzaniem danych osobowych, o którym mowa w art. 32 Rozporządzenia.

2. Przetwarzający zobowiązuje się dołożyć należytej staranności przy przetwarzaniu powierzonych danych osobowych.
3. Przetwarzający zobowiązuje się do nadania stosownych upoważnień do przetwarzania danych osobowych wszystkim osobom, które będą przetwarzały powierzone dane w celu realizacji niniejszej Umowy oraz będzie prowadził i aktualizował ich rejestr.
4. Przetwarzający zobowiązuje się zapewnić zachowanie w tajemnicy, o której mowa w art. 28 ust. 3 lit. b Rozporządzenia, przetwarzanych danych przez osoby, które upoważnione zostaną do przetwarzania danych osobowych w celu realizacji niniejszej Umowy, zarówno w trakcie trwania zatrudnienia ich u Przetwarzającego, jak i po jego ustaniu.
5. Przetwarzający po zakończeniu Umowy usuwa/zwraca Administratorowi *(należy wybrać, czy Przetwarzający ma usunąć, czy zwrócić dane)* wszelkie dane osobowe uzyskane na podstawie regulacji Umowy, oraz usuwa wszelkie ich istniejące kopie w ciągu .... (*np. 7 dni)*. Po wykonaniu zobowiązania, o którym mowa w zdaniu poprzedzającym, Przetwarzający złoży Administratorowi pisemne oświadczenie potwierdzające trwałe usunięcie wszystkich danych.
6. Przetwarzający zobowiązuje się pomagać, w miarę możliwości, Administratorowi w niezbędnym zakresie w wywiązywaniu się przez niego z:
    a) obowiązku odpowiadania na żądania osoby, której dane dotyczą, w zakresie wykonywania praw określonych w rozdziale III Rozporządzenia;
    b) obowiązków określonych w art. 32 - 36 Rozporządzenia.
7. Przetwarzający powiadamia Administratora danych o każdym podejrzeniu naruszenia ochrony danych osobowych, powierzonych Umową, niezwłocznie, nie później niż w..... *(np. 24 godziny)* od chwili uzyskania informacji o potencjalnym naruszeniu, oraz umożliwia Administratorowi uczestnictwo w czynnościach wyjaśniających i informuje Administratora o ustaleniach z chwilą ich dokonania, w szczególności o stwierdzeniu faktycznego naruszenia.
8. Planując dokonanie zmian w sposobie przetwarzania powierzonych danych, Przetwarzający ma obowiązek zastosować się do wymogu projektowania prywatności, o którym mowa w art. 25 ust. 1 Rozporządzenia i ma obowiązek z wyprzedzeniem informować Administratora o planowanych zmianach w taki sposób i terminach, aby zapewnić Administratorowi realną możliwość reagowania, jeżeli planowane przez Przetwarzającego zmiany w opinii Administratora grożą bezpieczeństwu danych lub zwiększają ryzyko naruszenia praw lub wolności osób, wskutek przetwarzania danych przez Przetwarzającego.

§ 4
Prawo kontroli

1. Zgodnie z art. 28 ust. 3 lit. h Rozporządzenia Administrator ma prawo kontroli, czy środki zastosowane przez Przetwarzającego przy przetwarzaniu i zabezpieczeniu powierzonych danych osobowych spełniają postanowienia Umowy i Rozporządzenia.
2. Administrator realizować będzie prawo kontroli poprzez....., w godzinach pracy Powierzającego i z minimum .....*(należy wpisać, z jakim wyprzedzeniem Administrator informuje o kontroli)* jego uprzedzeniem.

3. Przetwarzający zobowiązuje się do usunięcia uchybień stwierdzonych podczas kontroli, o której mowa w ust. 1, w terminie wskazanym przez Administratora, nie dłuższym niż .....dni.
4. Przetwarzający zobowiązuje się do udostępnienia Administratorowi wszelkich informacji niezbędnych do kontroli spełnienia przez siebie obowiązków określonych w art. 28 Rozporządzenia.

§ 5

Odpowiedzialność Przetwarzającego

1. Przetwarzający jest odpowiedzialny za przetwarzanie danych osobowych niezgodnie z treścią Umowy, przepisami Rozporządzenia lub innymi przepisami, o których mowa w § 1 ust. 2, a w szczególności za udostępnienie powierzonych do przetwarzania danych osobowych osobom nieupoważnionym.
2. Przetwarzający zobowiązuje się do niezwłocznego poinformowania Administratora o wszelkich wiadomych mu:
   a) postępowaniach, w szczególności sądowych lub administracyjnych,
   b) decyzjach administracyjnych i orzeczeniach sądowych,
   c) planowanych lub realizowanych kontrolach i inspekcjach, w szczególności prowadzonych przez inspektorów upoważnionych przez GIODO lub inny podmiot powołany odpowiednimi przepisami do pełnienia tożsamej funkcji,

dotyczących danych, o których mowa w § 2 Umowy, powierzonych przez Administratora.

§ 6

Podpowierzenie

1. Przetwarzający może powierzyć dane osobowe, wskazane w § 2 Umowy, do dalszego przetwarzania podwykonawcom jedynie w celu wykonania Umowy oraz po uzyskaniu uprzedniej zgody Administratora. Zgoda Administratora musi mieć formę pisemną pod rygorem nieważności.

   Ewentualnie, gdy podwykonawcy są już znani na etapie zawierania umowy powierzenia:

   1. *Przetwarzający może powierzyć dane osobowe, wskazane w § 2 Umowy, do dalszego przetwarzania podwykonawcom, pod warunkiem ich uprzedniej, pisemnej akceptacji przez Administratora lub braku sprzeciwu.*
   2. *Lista podwykonawców zaakceptowanych przez Administratora stanowi Załącznik nr 1 do Umowy.*
   3. *Powierzenie przetwarzania danych podwykonawcom spoza listy, o której mowa w ust. 1, wymaga uprzedniego zgłoszenia ich Administratorowi w celu umożliwienia wyrażenia sprzeciwu. Administrator może z uzasadnionych przyczyn zgłosić udokumentowany sprzeciw względem powierzenia danych konkretnemu podwykonawcy. W razie zgłoszenia sprzeciwu Przetwarzający nie ma prawa powierzyć danych podwykonawcy objętemu sprzeciwem, a jeżeli sprzeciw dotyczy aktualnego podwykonawcy, musi niezwłocznie zakończyć podpowierzenie temu podwykonawcy. Wątpliwości co do zasadności sprzeciwu i ewentualnych negatywnych konsekwencji Przetwarzający zgłosi Administratorowi w czasie umożliwiającym zapewnienie ciągłości przetwarzania.*
2. Przekazanie powierzonych danych do państwa trzeciego może nastąpić jedynie na pisemne polecenie Administratora, chyba, że obowiązek taki nakłada na Przetwarzającego prawo Unii

lub prawo państwa członkowskiego, któremu podlega Przetwarzający. W takim przypadku przed rozpoczęciem przetwarzania Przetwarzający informuje Administratora 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 ust. 1, winien spełniać te same wymogi i obowiązki, jakie zostały nałożone na Przetwarzającego w niniejszej Umowie, w szczególności w zakresie gwarancji ochrony powierzonych danych osobowych.
4. Przetwarzający ponosi wobec Administratora pełną odpowiedzialność za niewywiązywanie przez podwykonawcę ze spoczywających na nim obowiązków ochrony danych.

§ 7

Czas obowiązywania Umowy

1. Niniejsza Umowa obowiązuje od dnia jej zawarcia na czas nieokreślony/określony do dnia.....
2. Każda ze Stron może wypowiedzieć niniejszą Umowę z zachowaniem..... okresu wypowiedzenia.

§ 8

Rozwiązanie Umowy

1. Administrator może rozwiązać niniejszą Umowę ze skutkiem natychmiastowym, w sytuacji, gdy 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, Rozporządzeniem lub innymi przepisami, o których mowa w § 1 ust. 2;
   c) powierzył przetwarzanie danych osobowych innemu podmiotowi bez pisemnej zgody Administratora.

(Umowa może zawierać dodatkowe postanowienia dotyczące kar umownych)

§ 9

Zasady zachowania poufności

(zapisy § 9 można stosować w przypadku zaistnienia odpowiednich okoliczności)

1. *Przetwarzający zobowiązuje się do zachowania w tajemnicy wszelkich informacji, danych, materiałów, dokumentów i danych osobowych otrzymanych w związku z realizacją Umowy od Administratora i współpracujących z nim osób oraz danych uzyskanych w jakikolwiek inny sposób, zamierzony czy przypadkowy, w formie ustnej, pisemnej i elektronicznej („dane poufne").*
2. *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.*
3. *Strony zobowiązują się do dołożenia wszelkich starań w celu zapewnienia, aby środki łączności wykorzystywane do odbioru, przekazywania oraz przechowywania danych poufnych gwarantowały zabezpieczenie danych poufnych, w tym w szczególności danych*

osobowych powierzonych do przetwarzania, przed dostępem osób trzecich nieupoważnionych do zapoznania się z ich treścią.

(Umowa może zawierać dodatkowe postanowienia dotyczące kar umownych za naruszenia poufności)

§ 10

Postanowienia końcowe

1. Umowa została sporządzona w ..... jednobrzmiących egzemplarzach.
2. W sprawach nieuregulowanych zastosowanie będą miały przepisy Kodeksu cywilnego, Rozporządzenia oraz innych przepisów prawa, o których mowa w § 1 ust. 2.
3. Sądem właściwym dla rozpatrzenia sporów wynikających z niniejszej Umowy będzie sąd powszechny właściwy miejscowo dla Administratora *(lub Przetwarzającego, w zależności od postanowień Stron).*
4. Przetwarzający oświadcza, że znany jest mu fakt, iż treść niniejszej umowy, a w szczególności jej przedmiot, stanowią informację publiczną w rozumieniu art. 1 ust. 1 ustawy z dnia 6 września 2001 r. o dostępie do informacji publicznej (Dz.U. z 2016 r. poz. 1764, z późn. zm.), która podlega udostępnianiu w trybie przedmiotowej ustawy.
   ew. gdy Przetwarzającym jest osoba fizyczna, w tym prowadząca działalność gospodarczą:
   Przetwarzający oświadcza, że znany jest mu fakt, iż treść Umowy, a w szczególności jego przedmiot, stanowią informację publiczną w rozumieniu art. 1 ust. 1 ustawy z dnia 6 września 2001 r. o dostępie do informacji publicznej (Dz.U. z 2016 r. poz. 1764, z późn. zm.), która podlega udostępnianiu w trybie przedmiotowej ustawy. Przetwarzający wyraża zgodę na udostępnianie w trybie ustawy, o której mowa powyżej, zawartych w niniejszej Umowie dotyczących go danych osobowych w zakresie obejmującym imię i nazwisko.
5. Wszelkie zmiany niniejszej Umowy wymagają formy pisemnej pod rygorem nieważności.

.....	.....
Administrator	**Przetwarzający**

Załącznik Nr 15 do Polityki Ochrony Danych Osobowych

REJESTR UMÓW POWIERZENIA

L.p.	Nazwa podmiotu, któremu powierzono dane	Data powierzenia	Cel powierzenia oraz numer umowy powierzenia	Zakres powierzonych danych *(jakie dane zostały powierzone)*
1.				
2.				
3.				
4.				
5.				
6.				
7.				

Załącznik Nr 16 do Polityki Ochrony Danych Osobowych

WZÓR OŚWIADCZENIA

....

(imię i nazwisko) *(miejscowość, data)*

OŚWIADCZENIE O POUFNOŚCI

Oświadczam, iż zapoznano mnie z przepisami dotyczącymi ochrony danych osobowych, w szczególności ogólnego Rozporządzenia o ochronie danych UE z dnia 27 kwietnia 2016 r. oraz procedurami obowiązującymi w Urzędzie Gminy dotyczącymi przetwarzania danych osobowych.

W szczególności zobowiązuję się do:

- przetwarzania danych osobowych wyłącznie w zakresie i celu przewidzianym w powierzonych przez Administratora zadaniach,
- zachowania w tajemnicy danych osobowych do których mam lub będę mieć dostęp w związku z wykonywaniem zadań powierzonych przez Administratora,
- niewykorzystywania danych osobowych w celach niezgodnych z zakresem i celem powierzonych zadań przez Administratora,
- zachowania w tajemnicy sposobów zabezpieczenia danych osobowych,
- 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 Rozporządzenia o ochronie danych UE z dnia 27 kwietnia 2016 r.

.....

podpis oświadczającego

Załącznik Nr 17 do Polityki Ochrony Danych Osobowych

WYKAZ POMIESZCZEŃ W KTÓRYCH PRZETWARZANE SĄ DANE OSOBOWE

(wszystkie miejsca, pomieszczenia, pokoje, w których dokonuje się operacji na danych osobowych)

L.p.	Nazwa czynności	Precyzyjne określenie pomieszczenia	Osoba upoważniona do przetwarzania zbioru danych osobowych	Zabezpieczenie pomieszczenia
1.				
2.				
3.				
4.				
5.				
6.				

Załącznik Nr 18 do Polityki ochrony danych osobowych

WZORY ZGÓD I KLAUZUL INFORMACYJNYCH

OGÓLNA KLAUZULA INFORMACYJNA

Zgodnie z art. 13 ogólnego rozporządzenia o ochronie danych osobowych z dnia 27 kwietnia 2016 r.(Dz. Urz. UE L 119 z 04.05.2016) informuję, że:

1.Administratorem Pani/Pana danych osobowych jest .....(dalej: „ADMINISTRATOR"), z siedzibą: ..... Z Administratorem można się kontaktować pisemnie, za pomocą poczty tradycyjnej na adres: ..... lub drogą e-mailową pod adresem: .....

2. Administrator wyznaczył Inspektora Ochrony Danych, z którym można się skontaktować pod adresem mailowym: .....

3.Pani/Pana dane osobowe są przetwarzane na podstawie art. 6 ust. 1 lit. a i b dyrektywy Parlamentu Europejskiego i Rady (UE) 2016/680 z dnia 27 kwietnia 2016r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych przez właściwe organy do celów zapobiegania przestępczości, prowadzenia postępowań przygotowawczych, wykrywania i ścigania czynów zabronionych i wykonywania kar, w sprawie swobodnego przepływu takich danych oraz uchylająca decyzję ramową Rady 2008/977/WSiSW.tj.w oparciu o zgodę osoby, której dane dotyczą oraz ustawy z dnia 8 marca 1990 r. o samorządzie gminnym; ustawy z dnia 21 listopada 2008 r. o pracownikach samorządowych, ustawy z dnia 14 czerwca 1960 r. Kodeks postępowania administracyjnego i innych nakładających na samorząd gminny obowiązek ustawowy.

4. Przetwarzanie odbywa się w związku realizacja obowiązków lub uprawnień gminy wynikających z przepisów prawa, jeśli jest to konieczne do realizacji umowy, gdy osoba, której dane dotyczą, jest jej stroną lub gdy jest to niezbędne do podjęcia działań przed zawarciem umowy na żądanie osoby, której dane dotyczą, jest niezbędne do wykonania określonych prawem zadań realizowanych dla dobra publicznego, jest to niezbędne do wypełnienia prawnie usprawiedliwionych celów realizowanych przez administratorów danych albo odbiorców danych, a przetwarzanie nie narusza praw i wolności osoby, której dane dotyczą, a także jest konieczne do prowadzenia postępowań administracyjnych oraz w urzędzie stanu cywilnego, ewidencji ludności.

5.Dane osobowe mogą pochodzić od stron trzecich, tj. urzędów gmin, Policji, urzędów pracy, placówek oświatowych, jednostek podległych, placówek pomocy społecznej, ministerstw, sądów oraz innych organów administracji publicznej.

6.Administrator nie zamierza przekazywać danych do państwa trzeciego lub organizacji międzynarodowej.

7. Administrator będzie przekazywał dane osobowe innym podmiotom, tylko na podstawie przepisów prawa, w tym w szczególności do: Policji, urzędów pracy, placówek oświatowych, placówek pomocy społecznej, innych urzędów gminy, sądów, instytucji publicznych, jednostek podległych, ministerstw, Mazowieckiego Urzędu Wojewódzkiego w Warszawie oraz innych organów administracji publicznej.

8.Dane osobowe będą przetwarzane tak długo jak wynika to z przepisów prawa (w szczególności dotyczących archiwizacji). Dane, których nie ma obowiązku przechowywać, będą niszczone niezwłocznie po zakończeniu działania, którego dotyczą.

9.Osoba,której dane dotyczą ma prawo do żądania od administratora dostępu do danych osobowych, ich sprostowania, usunięcia lub ograniczenia przetwarzania oraz prawo do wniesienia sprzeciwu wobec przetwarzania, a także prawo do przenoszenia danych.

10.Skargę na działania Administratora można wnieść do Prezesa Urzędu Ochrony Danych Osobowych.

11. Podanie danych osobowych wynikających z przepisu prawa jest wymogiem ustawowym, koniecznym do wykonania obowiązków Administratora.

12. Administrator nie przewiduje zautomatyzowanego podejmowania decyzji.

Obowiązek informacyjny radnych w związku z przetwarzaniem danych osobowych:

Zgodnie z art. 13 ogólnego rozporządzenia o ochronie danych osobowych z dnia 27 kwietnia 2016 r.(Dz. Urz. UE L 119 z 04.05.2016) informuję, że:

1.Administratorem Pani/Pana danych osobowych jest .....(dalej: „ADMINISTRATOR"), z siedzibą: ..... Z Administratorem można się kontaktować pisemnie, za pomocą poczty tradycyjnej na adres: ..... lub drogą e-mailową pod adresem: .....

2. Administrator wyznaczył Inspektora Ochrony Danych, z którym można się skontaktować pod adresem mailowym: .....

3.Pani/Pana dane osobowe są przetwarzane na podstawie art. 6 ust. 1 lit. a i b dyrektywy Parlamentu Europejskiego i Rady (UE) 2016/680 z dnia 27 kwietnia 2016r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych przez właściwe organy do celów zapobiegania przestępczości, prowadzenia postępowań przygotowawczych, wykrywania i ścigania czynów zabronionych. i wykonywania kar, w sprawie swobodnego przepływu takich danych oraz uchylająca decyzję ramową Rady 2008/977/WSiSW,tj. w oparciu o zgodę osoby, której dane dotyczą oraz ustawy z dnia 8 marca 1990 r. o samorządzie gminnym

4. Przetwarzanie danych osobowych odbywa się w celu wykonywania obowiązków radnego wyznaczonych na podstawie ustawy o samorządzie gminnym.

5. Dane osobowe pochodzą od Komisarza Wyborczego.

6.Administrator nie zamierza przekazywać danych do państwa trzeciego lub organizacji międzynarodowej.

7. Administrator będzie przekazywał dane osobowe innym podmiotom, tylko na podstawie przepisów prawa, w tym w szczególności do: Zakładu Ubezpieczeń Społecznych. Urzędu Skarbowego.

8.Dane osobowe będą przetwarzane przez Administratora tak długo jak wynika to z przepisów prawa.

9.Osoba,której dane dotyczą ma prawo do żądania od administratora dostępu do danych osobowych, ich sprostowania, usunięcia lub ograniczenia przetwarzania oraz prawo do wniesienia sprzeciwu wobec przetwarzania, a także prawo do przenoszenia danych.

10.Skargę na działania Administratora można wnieść do Prezesa Urzędu Ochrony Danych Osobowych.

11. Podanie danych osobowych jest wymogiem do wykonania obowiązków radnego.

12. Administrator nie przewiduje zautomatyzowanego podejmowania decyzji.

.....

(miejscowość, data)

.....

(imię i nazwisko)

.....

.....

(adres)

ZGODA

na przetwarzanie danych osobowych pracownika

Ja niżej podpisany/a wyrażam zgodę na przetwarzanie następujących danych osobowych:

1) .....

2) .....

3) .....

w celach związanych z przebiegiem zatrudnienia .....z siedzibą w przy ulicy ..... w ..... .

(dokładny adres)

Rozumiem, że moje dane osobowe będą przechowywane przez .....

(wskazać administratora danych)

przez okres ..... . Po upływie tego okresu dane zostaną zniszczone.

(wskazać okres przechowywania)

Zgodnie z przekazaną mi informacją z dnia ..... wyrażam zgodę, aby:

odbiorcą moich danych osobowych był .....;

(wskazać odbiorców danych osobowych lub ich grupy, jeżeli istnieją)

Rozumiem, że przysługuje mi prawo dostępu do treści swoich danych oraz prawo ich sprostowania, usunięcia, ograniczenia przetwarzania, jak również prawo do przenoszenia danych, prawo wniesienia sprzeciwu, prawo do cofnięcia zgody na ich przetwarzanie w

dowolnym momencie bez wpływu na zgodność z prawem przetwarzania, którego dokonano na podstawie zgody wyrażonej przed jej cofnięciem.

.....

(data i podpis pracownika)

Wzór klauzuli informacyjnej dla pracownika

Zgodnie z art. 13 ust. 1 i 2 ogólnego rozporządzenia o ochronie danych osobowych z dnia 27 kwietnia 2016 r.(Dz. Urz. UE L 119 z 04.05.2016) informuję, iż:

1) administratorem Pani/Pana danych osobowych jest ..... z siedzibą w .....

2) inspektorem ochrony danych w ..... jest Pan/Pani..... (*e-mail służbowy lub nr tel. służbowego) .....

3) administrator będzie przetwarzał Państwa dane w celu związanym z nawiązaniem i przebiegiem procesu zatrudnienia na podstawie dobrowolnej zgody - art. 6 ust. 1 lit. a RODO oraz na podstawie art. 6 ust. 1 lit. c i art. 9 ust. 2 lit. b RODO tj. przetwarzanie jest niezbędne do wypełnienia obowiązków i szczególnych praw przez administratora w dziedzinie prawa pracy, zabezpieczenia społecznego i ochrony socjalnej

4) dane osobowe mogą być udostępnione innym uprawionym podmiotom na podstawie przepisów prawa, a także na rzecz podmiotów, z którymi administrator zawarł umowę powierzenia przetwarzania danych w związku z realizacją usług na rzecz administratora (np. kancelarią prawną, dostawcą oprogramowania, zleceniobiorcą świadczącym usługę z zakresu ochrony danych osobowych)

5) Państwa dane osobowe będą przechowywane do momentu upływu okresu przewidzianego w ustawie dnia 17 grudnia 1998r. o emeryturach i rentach z Funduszu Ubezpieczeń Społecznych, w ustawie z dnia 14 lipca 1983r. o narodowym zasobie archiwalnym i archiwach oraz w Rozporządzeniu Ministra Kultury i Dziedzictwa Narodowego z dnia 20 października 2015r. w sprawie klasyfikowania i kwalifikowania dokumentacji, przekazywania materiałów archiwalnych do archiwów państwowych i brakowania dokumentacji niearchiwalnej

6) administrator nie zamierza przekazywać Państwa danych osobowych do państwa trzeciego lub organizacji międzynarodowej

7) posiada Pani/Pan prawo dostępu do treści swoich danych oraz prawo ich sprostowania, usunięcia, ograniczenia przetwarzania, prawo wniesienia sprzeciwu, prawo do przenoszenia danych, prawo do cofnięcia zgody z wyłączeniem sytuacji, kiedy podanie danych osobowych jest obowiązkowe

8) ma Pan/Pani prawo wniesienia skargi do Prezesa Urzędu Ochrony Danych Osobowych, gdy uzna Pani/Pan, iż przetwarzanie danych osobowych Pani/Pana dotyczących narusza przepisy RODO

9) podanie przez Pana/Panią danych osobowych jest dobrowolne, ale konieczne dla celów związanych z nawiązaniem i przebiegiem Pani/Pana zatrudnienia, z wyjątkiem danych osobowych pobieranych na podstawie przepisów prawa w przypadku których konsekwencją niepodania danych osobowych jest brak możliwości realizacji umowy o pracę

10) administrator nie podejmuje decyzji w sposób zautomatyzowany w oparciu o Państwa dane osobowe.

.....

(miejscowość, data)

.....

(imię i nazwisko)

.....

.....

(adres)

ZGODA

na przetwarzanie danych osobowych kandydatów do pracy

Zgodnie z art.6 ust.1 lit. a ogólnego rozporządzenia o ochronie danych osobowych z dnia 27 kwietnia 2016 r.(Dz. Urz. UE L 119 z 04.05.2016) wyrażam zgodę na przetwarzanie moich danych osobowych dla potrzeb rekrutacji.

Wzór klauzuli informacyjnej dla kandydatów do pracy

Zgodnie z art. 13 ogólnego rozporządzenia o ochronie danych osobowych z dnia 27 kwietnia 2016 r.(Dz. Urz. UE L 119 z 04.05.2016) informuję, że:

1)administratorem Pani/Pana danych osobowych jest .....

2) inspektorem ochrony danych w ..... jest Pan/Pani..... (*e-mail służbowy lub nr tel. służbowego) .....

3) administrator będzie przetwarzał Państwa dane dla potrzeb rekrutacji na podstawie art. 6 ust. 1 lit. a RODO

4) Pani/Pana dane osobowe przechowywane będą przez okres rekrutacji

5)dane osobowe mogą być udostępnione innym uprawionym podmiotom na podstawie przepisów prawa, a także na rzecz podmiotów, z którymi administrator zawarł umowę powierzenia przetwarzania danych w związku z realizacją usług na rzecz administratora (np. kancelarią prawną, dostawcą oprogramowania, zleceniobiorcą świadczącym usługę z zakresu ochrony danych osobowych)

6) administrator nie zamierza przekazywać Państwa danych osobowych do państwa trzeciego lub organizacji międzynarodowej

7) posiada Pani/Pan prawo dostępu do treści swoich danych oraz prawo ich sprostowania, usunięcia, ograniczenia przetwarzania, prawo wniesienia sprzeciwu, prawo do przenoszenia danych, prawo do cofnięcia zgody na ich przetwarzanie w dowolnym momencie bez wpływu na zgodność z prawem przetwarzania, którego dokonano na podstawie zgody wyrażonej przed jej cofnięciem

8) ma Pan/Pani prawo wniesienia skargi do Prezesa Urzędu Ochrony Danych Osobowych, gdy uzna Pani/Pan, iż przetwarzanie danych osobowych Pani/Pana dotyczących narusza przepisy RODO

9) podanie przez Pana/Panią danych osobowych jest dobrowolne, ale konieczne dla celów rekrutacji

10) administrator nie podejmuje decyzji w sposób zautomatyzowany w oparciu o Państwa dane osobowe

.....

(miejscowość, data)

.....

(imię i nazwisko)

.....

.....

(adres)

Zgoda Pracownika na publikację wizerunku

Zgodnie z art. 6 ust. 1 lit. a ogólnego rozporządzenia o ochronie danych osobowych z dnia 27 kwietnia 2016 r. wyrażam zgodę na przetwarzanie oraz bezpłatne rozpowszechnianie moich danych osobowych - wizerunkowych na stronie internetowej, na profilu na portalu społecznościowym, a także zamieszczenie w materiałach promocyjnych i informacyjnych w celu budowania pozytywnego wizerunku ....

Administratorem danych osobowych jest .....

Rozumiem, że przysługuje mi prawo dostępu do treści swoich danych oraz prawo ich sprostowania, usunięcia, ograniczenia przetwarzania, jak również prawo do przenoszenia danych, prawo wniesienia sprzeciwu, prawo do cofnięcia zgody na ich przetwarzanie w dowolnym momencie bez wpływu na zgodność z prawem przetwarzania, którego dokonano na podstawie zgody wyrażonej przed jej cofnięciem.

.....

(data i podpis Pracownika)

Wzór klauzuli informacyjnej dla Zleceniobiorców/ Przyjmujących zamówienie (wykonawców dzieła)

Zgodnie z art. 13 ust. 1 i 2 ogólnego rozporządzenia o ochronie danych osobowych z dnia 27 kwietnia 2016 r.(Dz. Urz. UE L 119 z 04.05.2016) informuję, iż:

1. administratorem danych osobowych Zleceniobiorców / Przyjmujących zamówienie (wykonawców dzieła) jest ..... z siedzibą w .....
2. inspektorem ochrony danych w ..... jest Pan/Pani..... (*e-mail służbowy lub nr tel. służbowego) .....
3. Administrator będzie przetwarzał Państwa dane osobowe na podstawie art. 6 ust. 1 lit. b) RODO tj. przetwarzanie jest niezbędne w celu wykonania umowy, której stroną jest osoba, której dane dotyczą lub do podjęcia działań na żądanie osoby, której dane dotyczą, przed zawarciem umowy
4. dane osobowe mogą być udostępnione innym uprawionym podmiotom na podstawie przepisów prawa, a także na rzecz podmiotów, z którymi administrator zawarł umowę powierzenia przetwarzania danych w związku z realizacją usług na rzecz administratora (np. kancelarią prawną, dostawcą oprogramowania, zleceniobiorcą świadczącym usługę z zakresu ochrony danych osobowych)
5. administrator nie zamierza przekazywać Państwa danych osobowych do państwa trzeciego lub organizacji międzynarodowej
6. posiada Pani/Pan prawo dostępu do treści swoich danych oraz prawo ich sprostowania, usunięcia, ograniczenia przetwarzania, prawo wniesienia sprzeciwu, prawo do przenoszenia danych, prawo do cofnięcia zgody na ich przetwarzanie w dowolnym momencie bez wpływu na zgodność z prawem przetwarzania, którego dokonano na podstawie zgody wyrażonej przed jej cofnięciem
7. ma Pan/Pani prawo wniesienia skargi do Prezesa Urzędu Ochrony Danych Osobowych, gdy uzna Pani/Pan, iż przetwarzanie danych osobowych Pani/Pana dotyczących narusza przepisy RODO

8. Państwa dane osobowe będą przechowywane przez okres .....
9. podanie przez Pana/Panią danych osobowych jest dobrowolne, ale konieczne do zawarcia umowy. Konsekwencją niepodania danych będzie brak realizacji umowy.
10. administrator nie podejmuje decyzji w sposób zautomatyzowany w oparciu o Państwa dane osobowe.

Wzór klauzuli informacyjnej dla osób ubiegających się o przyznanie świadczeń z Zakładowego Funduszu Świadczeń Socjalnych

Zgodnie z art. 13 ust. 1 i 2 i ogólnego rozporządzenia o ochronie danych osobowych z dnia 27 kwietnia 2016 r.(Dz. Urz. UE L 119 z 04.05.2016) informuję, iż:

1. administratorem danych osobowych osób ubiegających się o świadczenie z Zakładowego Funduszu Świadczeń Socjalnych jest ..... z siedzibą w . .....

2. inspektorem ochrony danych w ..... jest Pan/Pani..... (*e-mail służbowy lub nr tel. służbowego) .....

3. Administrator będzie przetwarzał Państwa dane osobowe w celu związanym z rozpatrzeniem i realizacją wniosku o przyznanie świadczenia z Zakładowego Funduszu Świadczeń Socjalnych na podstawie art. 6 ust. 1 lit. c) RODO tj. przetwarzanie jest niezbędne do wypełnienia obowiązku prawnego ciążącego na administratorze wynikającego z ustawy z dnia 4 marca 1994r. o zakładowym funduszu świadczeń socjalnych

4. dane osobowe mogą być udostępnione innym uprawionym podmiotom na podstawie przepisów prawa, a także na rzecz podmiotów, z którymi administrator zawarł umowę powierzenia przetwarzania danych w związku z realizacją usług na rzecz administratora (np. kancelarią prawną, dostawcą oprogramowania, zleceniobiorcą świadczącym usługę z zakresu ochrony danych osobowych)

5. administrator nie zamierza przekazywać Państwa danych osobowych do państwa trzeciego lub organizacji międzynarodowej

6. posiada Pani/Pan prawo dostępu do treści swoich danych oraz prawo ich sprostowania, usunięcia, ograniczenia przetwarzania, prawo wniesienia sprzeciwu, prawo do przenoszenia danych, prawo do cofnięcia zgody na ich przetwarzanie w dowolnym momencie bez wpływu na zgodność z prawem przetwarzania, którego dokonano na podstawie zgody wyrażonej przed jej cofnięciem

7. Państwa dane osobowe będą przechowywane do momentu upływu okresu przewidzianego zgodnie z ustawą z dnia 14 lipca 1983r. o narodowym zasobie archiwalnym i archiwach oraz Rozporządzeniu Ministra Kultury i Dziedzictwa Narodowego z dnia 20 października 2015r. w sprawie klasyfikowania i klasyfikowania dokumentacji przekazywania materiałów archiwalnych do archiwów państwowych i brakowania dokumentacji niearchiwalnej

8. podanie przez Pana/Panią danych osobowych jest dobrowolne, ale konieczne do przyznania świadczeń z Zakładowego Funduszu Świadczeń Socjalnych. Konsekwencją niepodania danych jest brak możliwości rozpatrzenia wniosku o świadczenie z Zakładowego Funduszu Świadczeń Socjalnych

9. ma Pan/Pani prawo wniesienia skargi do Prezesa Urzędu Ochrony Danych Osobowych, gdy uzna Pani/Pan, iż przetwarzanie danych osobowych Pani/Pana dotyczących narusza przepisy RODO

10. administrator nie podejmuje decyzji w sposób zautomatyzowany w oparciu o Państwa dane osobowe.

.....

(miejscowość, data)

.....

(imię i nazwisko)

.....

.....

(adres)

ZGODA

byłego pracownika korzystającego z Zakładowego Funduszu Świadczeń Socjalnych

Zgodnie z art.6 ust.1 lit. a ogólnego rozporządzenia o ochronie danych osobowych z dnia 27 kwietnia 2016 r.(Dz. Urz. UE L 119 z 04.05.2016)wyrażam zgodę na przetwarzanie moich danych osobowych dla potrzeb korzystania z Zakładowego Funduszu Świadczeń Socjalnych.

Wzór klauzuli informacyjnej dla byłego pracownika korzystającego z Zakładowego Funduszu Świadczeń Socjalnych

Zgodnie z art. 13 ogólnego rozporządzenia o ochronie danych osobowych z dnia 27 kwietnia 2016 r.(Dz. Urz. UE L 119 z 04.05.2016) informuję, że:

1)administratorem Pani/Pana danych osobowych jest .....

2) inspektorem ochrony danych w ..... jest Pan/Pani..... (*e-mail służbowy lub nr tel. służbowego) .....

3) Administrator będzie przetwarzał Państwa dane na podstawie Art. 6 ust. 1 lit. a RODO, tj. na podstawie zgody na przetwarzanie danych osobowych oraz na podstawie art. 6 ust. 1 lit. c RODO tj. przetwarzanie danych jest niezbędne do wypełnienia obowiązku prawnego ciążącego na administratorze,

4) Pani/Pana dane osobowe przechowywane będą przez okres .....

5) dane osobowe mogą być udostępnione innym uprawionym podmiotom na podstawie przepisów prawa, a także na rzecz podmiotów, z którymi administrator zawarł umowę powierzenia przetwarzania danych w związku z realizacją usług na rzecz administratora (np. kancelarią prawną, dostawcą oprogramowania, zleceniobiorcą świadczącym usługę z zakresu ochrony danych osobowych)

6) administrator nie zamierza przekazywać Państwa danych osobowych do państwa trzeciego lub organizacji międzynarodowej

7) posiada Pani/Pan prawo dostępu do treści swoich danych oraz prawo ich sprostowania, usunięcia, ograniczenia przetwarzania, prawo wniesienia sprzeciwu, prawo do przenoszenia danych, prawo do cofnięcia zgody, z wyjątkiem danych których podanie jest obowiązkowe

8) ma Pan/Pani prawo wniesienia skargi do Prezesa Urzędu Ochrony Danych Osobowych, gdy uzna Pani/Pan, iż przetwarzanie danych osobowych Pani/Pana dotyczących narusza przepisy RODO

9) podanie przez Pana/Panią danych osobowych jest dobrowolne, ale konieczne dla przyznania świadczeń z Zakładowego Funduszu Świadczeń Socjalnych, z wyjątkiem danych których podanie jest obowiązkowe

10) administrator nie podejmuje decyzji w sposób zautomatyzowany w oparciu o Państwa dane osobowe.

Wzór klauzuli informacyjnej dla kontrahentów – osób fizycznych oraz osób fizycznych prowadzących działalność gospodarczą

Zgodnie z art. 13 ust. 1 i 2 ogólnego rozporządzenia o ochronie danych osobowych z dnia 27 kwietnia 2016 r.(Dz. Urz. UE L 119 z 04.05.2016) informuję, iż:

1. administratorem danych osobowych Wykonawców lub Zleceniobiorców jest ..... z siedzibą w .....

2. inspektorem ochrony danych w ..... jest Pan/Pani..... (*e-mail służbowy lub nr tel. służbowego) .....

3. Administrator będzie przetwarzał Państwa dane osobowe na podstawie art. 6 ust. 1 lit. b) RODO tj. przetwarzanie jest niezbędne w celu wykonania umowy, której stroną jest osoba, której dane dotyczą lub do podjęcia działań na żądanie osoby, której dane dotyczą, przed zawarciem umowy,

4. dane osobowe mogą być udostępnione innym uprawionym podmiotom na podstawie przepisów prawa, a także na rzecz podmiotów, z którymi administrator zawarł umowę powierzenia przetwarzania danych w związku z realizacją usług na rzecz administratora (np. kancelarią prawną, dostawcą oprogramowania, zleceniobiorcą świadczącym usługę z zakresu ochrony danych osobowych)

5. administrator nie zamierza przekazywać Państwa danych osobowych do państwa trzeciego lub organizacji międzynarodowej

6. posiada Pani/Pan prawo dostępu do treści swoich danych oraz prawo ich sprostowania, usunięcia, ograniczenia przetwarzania, prawo wniesienia sprzeciwu, prawo do przenoszenia danych, prawo do cofnięcia zgody na ich przetwarzanie w dowolnym momencie bez wpływu na zgodność z prawem przetwarzania, którego dokonano na podstawie zgody wyrażonej przed jej cofnięciem

7. ma Pan/Pani prawo wniesienia skargi do Prezesa Urzędu Ochrony Danych Osobowych, gdy uzna Pani/Pan, iż przetwarzanie danych osobowych Pani/Pana dotyczących narusza przepisy RODO

8. Państwa dane osobowe będą przechowywane do momentu upływu terminu przedawnienia, zgodnie z kodeksem cywilnym

9. podanie przez Pana/Panią danych osobowych jest dobrowolne, ale konieczne do zawarcia umowy. Konsekwencją niepodania danych jest brak realizacji umowy.

10. administrator nie podejmuje decyzji w sposób zautomatyzowany w oparciu o Państwa dane osobowe.

Wzór klauzuli informacyjnej dla Wolontariuszy

Zgodnie z art. 13 ust. 1 i 2 ogólnego rozporządzenia o ochronie danych osobowych z dnia 27 kwietnia 2016 r.(Dz. Urz. UE L 119 z 04.05.2016) informuję, iż:

1. administratorem danych osobowych jest .....

2. inspektorem ochrony danych w ..... jest Pan/Pani..... (*e-mail służbowy lub nr tel. służbowego) .....

3. Administrator będzie przetwarzał Państwa dane osobowe na podstawie art. 6 ust. 1 lit. b) RODO tj. przetwarzanie jest niezbędne w celu wykonania umowy, której stroną jest osoba, której dane dotyczą lub do podjęcia działań na żądanie osoby, której dane dotyczą, przed zawarciem umowy

4. dane osobowe mogą być udostępnione innym uprawionym podmiotom na podstawie przepisów prawa, a także na rzecz podmiotów, z którymi administrator zawarł umowę powierzenia przetwarzania danych w związku z realizacją usług na rzecz administratora (np. kancelarią prawną, dostawcą oprogramowania, zleceniobiorcą świadczącym usługę z zakresu ochrony danych osobowych)

5. administrator nie zamierza przekazywać Państwa danych osobowych do państwa trzeciego lub organizacji międzynarodowej

6. posiada Pani/Pan prawo dostępu do treści swoich danych oraz prawo ich sprostowania, usunięcia, ograniczenia przetwarzania, prawo wniesienia sprzeciwu, prawo do przenoszenia danych, prawo do cofnięcia zgody na ich przetwarzanie w dowolnym momencie bez wpływu na zgodność z prawem przetwarzania, którego dokonano na podstawie zgody wyrażonej przed jej cofnięciem

7. Państwa dane osobowe będą przechowywane do czasu .....

8. podanie przez Pana/Panią danych osobowych jest dobrowolne, ale konieczne do zawarcia umowy. Konsekwencją niepodania danych jest brak realizacji umowy

9. ma Pan/Pani prawo wniesienia skargi do Prezesa Urzędu Ochrony Danych Osobowych, gdy uzna Pani/Pan, iż przetwarzanie danych osobowych Pani/Pana dotyczących narusza przepisy RODO

10. administrator nie podejmuje decyzji w sposób zautomatyzowany w oparciu o Państwa dane osobowe.

Wzór klauzuli informacyjnej dla darczyńców

Zgodnie z art. 13 ust. 1 i 2 ogólnego rozporządzenia o ochronie danych osobowych z dnia 27 kwietnia 2016 r.(Dz. Urz. UE L 119 z 04.05.2016) informuję, iż:

1. administratorem danych osobowych jest .....

2. inspektorem ochrony danych w ..... jest Pan/Pani..... (*e-mail służbowy lub nr tel. służbowego) .....

3. Administrator będzie przetwarzał Państwa dane osobowe na podstawie art. 6 ust. 1 lit. b) RODO tj. przetwarzanie jest niezbędne w celu wykonania umowy, której stroną jest osoba, której dane dotyczą lub do podjęcia działań na żądanie osoby, której dane dotyczą, przed zawarciem umowy

4. dane osobowe mogą być udostępnione innym uprawionym podmiotom na podstawie przepisów prawa, a także na rzecz podmiotów, z którymi administrator zawarł umowę powierzenia przetwarzania danych w związku z realizacją usług na rzecz administratora (np. kancelarią prawną, dostawcą oprogramowania, zleceniobiorcą świadczącym usługę z zakresu ochrony danych osobowych)

5. administrator nie zamierza przekazywać Państwa danych osobowych do państwa trzeciego lub organizacji międzynarodowej

6. posiada Pani/Pan prawo dostępu do treści swoich danych oraz prawo ich sprostowania, usunięcia, ograniczenia przetwarzania, prawo wniesienia sprzeciwu, prawo do przenoszenia danych, prawo do cofnięcia zgody na ich przetwarzanie w dowolnym momencie bez wpływu na zgodność z prawem przetwarzania, którego dokonano na podstawie zgody wyrażonej przed jej cofnięciem

7. ma Pan/Pani prawo wniesienia skargi do Prezesa Urzędu Ochrony Danych Osobowych, gdy uzna Pani/Pan, iż przetwarzanie Pani/Pana danych osobowych narusza przepisy

8. Państwa dane osobowe będą przechowywane do czasu wniesienia sprzeciwu

9. podanie przez Pana/Panią danych osobowych jest dobrowolne, ale konieczne do zawarcia umowy. Konsekwencją niepodania danych jest brak realizacji umowy.

10. administrator nie podejmuje decyzji w sposób zautomatyzowany w oparciu o Państwa dane osobowe.

Wzór klauzuli informacyjnej dla osoby wykonującej pracę społecznie użyteczne

Zgodnie z art. 13 ogólnego rozporządzenia o ochronie danych osobowych z dnia 27 kwietnia 2016 r.(Dz. Urz. UE L 119 z 04.05.2016) informuję, że:

1)administratorem Pani/Pana danych osobowych jest .....

2) inspektorem ochrony danych w ..... jest Pan/Pani..... (*e-mail służbowy lub nr tel. służbowego) .....

3) Administrator będzie przetwarzał Państwa dane na podstawie art. 6 ust. 1 lit. c RODO tj. przetwarzanie danych jest niezbędne do wypełnienia obowiązku prawnego ciążącego na administratorze

4) Pani/Pana dane osobowe przechowywane będą przez okres .....

5) dane osobowe mogą być udostępnione innym uprawionym podmiotom na podstawie przepisów prawa, a także na rzecz podmiotów, z którymi administrator zawarł umowę powierzenia przetwarzania danych w związku z realizacją usług na rzecz administratora (np. kancelarią prawną, dostawcą oprogramowania, zleceniobiorcą świadczącym usługę z zakresu ochrony danych osobowych)

6) administrator nie zamierza przekazywać Państwa danych osobowych do państwa trzeciego lub organizacji międzynarodowej

7) posiada Pani/Pan prawo dostępu do treści swoich danych oraz prawo ich sprostowania, usunięcia, ograniczenia przetwarzania, prawo wniesienia sprzeciwu, prawo do przenoszenia danych, prawo do cofnięcia zgody, z wyjątkiem danych których podanie jest obowiązkowe

8)ma Pan/Pani prawo wniesienia skargi do Prezesa Urzędu Ochrony Danych Osobowych, gdy uzna Pani/Pan, iż przetwarzanie danych osobowych Pani/Pana dotyczących narusza przepisy RODO;

9) administrator nie podejmuje decyzji w sposób zautomatyzowany w oparciu o Państwa dane osobowe.

Wzór klauzuli informacyjnej dla osoby wykonującej nieodpłatną, kontrolowaną pracę na cele społeczne

Zgodnie z art. 13 ogólnego rozporządzenia o ochronie danych osobowych z dnia 27 kwietnia 2016 r.(Dz. Urz. UE L 119 z 04.05.2016) informuję, że:

1)administratorem Pani/Pana danych osobowych jest .....

2) inspektorem ochrony danych w ..... jest Pan/Pani..... (*e-mail służbowy lub nr tel. służbowego) .....

3) Administrator będzie przetwarzał Państwa dane na podstawie art. 6 ust. 1 lit. c RODO tj. przetwarzanie danych jest niezbędne do wypełnienia obowiązku prawnego ciążącego na administratorze

4) Pani/Pana dane osobowe przechowywane będą przez okres .....

5) dane osobowe mogą być udostępnione innym uprawionym podmiotom na podstawie przepisów prawa, a także na rzecz podmiotów, z którymi administrator zawarł umowę powierzenia przetwarzania danych w związku z realizacją usług na rzecz administratora (np. kancelarią prawną, dostawcą oprogramowania, zleceniobiorcą świadczącym usługę z zakresu ochrony danych osobowych)

6) administrator nie zamierza przekazywać Państwa danych osobowych do państwa trzeciego lub organizacji międzynarodowej

7) posiada Pani/Pan prawo dostępu do treści swoich danych oraz prawo ich sprostowania, usunięcia, ograniczenia przetwarzania, prawo wniesienia sprzeciwu, prawo do przenoszenia danych, prawo do cofnięcia zgody, z wyjątkiem danych których podanie jest obowiązkowe

8)ma Pan/Pani prawo wniesienia skargi do Prezesa Urzędu Ochrony Danych Osobowych, gdy uzna Pani/Pan, iż przetwarzanie danych osobowych Pani/Pana dotyczących narusza przepisy RODO;

9) podanie przez Pana/Panią danych osobowych jest obowiązkowe

10) administrator nie podejmuje decyzji w sposób zautomatyzowany w oparciu o Państwa dane osobowe.

Wzór klauzuli informacyjnej dla osób składających skargę lub wniosek

Zgodnie z art. 13 ogólnego rozporządzenia o ochronie danych osobowych z dnia 27 kwietnia 2016 r.(Dz. Urz. UE L 119 z 04.05.2016) informuję, że:

1) administratorem Pani/Pana danych osobowych jest .....

2) inspektorem ochrony danych w ..... jest Pan/Pani..... (*e-mail służbowy lub nr tel. służbowego) .....

3) Administrator będzie przetwarzał Państwa dane na podstawie art. 6 ust. 1 lit. c RODO tj. przetwarzanie danych jest niezbędne do wypełnienia obowiązku prawnego ciążącego na administratorze,

4) Pani/Pana dane osobowe przechowywane będą przez okres .....

5)dane osobowe mogą być udostępnione innym uprawionym podmiotom na podstawie przepisów prawa, a także na rzecz podmiotów, z którymi administrator zawarł umowę powierzenia przetwarzania danych w związku z realizacją usług na rzecz administratora (np. kancelarią prawną, dostawcą oprogramowania, zleceniobiorcą świadczącym usługę z zakresu ochrony danych osobowych)

6) administrator nie zamierza przekazywać Państwa danych osobowych do państwa trzeciego lub organizacji międzynarodowej

7) posiada Pani/Pan prawo dostępu do treści swoich danych oraz prawo ich sprostowania, usunięcia, ograniczenia przetwarzania, prawo wniesienia sprzeciwu, prawo do przenoszenia danych, prawo do cofnięcia zgody

8)ma Pan/Pani prawo wniesienia skargi do Prezesa Urzędu Ochrony Danych Osobowych, gdy uzna Pani/Pan, iż przetwarzanie danych osobowych Pani/Pana dotyczących narusza przepisy RODO

9) podanie przez Pana/Panią danych osobowych jest dobrowolne, jednakże brak ich podania skutkuje niemożnością należytego wykonania obowiązku Domu Pomocy Społecznej w zakresie rozpoznania skarg i wniosków

10) administrator nie podejmuje decyzji w sposób zautomatyzowany w oparciu o Państwa dane osobowe.

Zgoda uczestnika imprezy na przetwarzanie danych osobowych

Ja niżej podpisany wyrażam zgodę na przetwarzanie moich danych osobowych, prezentacje moich wypowiedzi, wizerunku oraz nagrywanie, fotografowanie, publikację w mediach, gazetach, na stronach internetowych w celu upamiętnienia i popularyzacji..... organizowanego przez .....

KLAUZULA INFORMACJNA- MONITORING

1. Administratorem systemu monitoringu jest ....w ..... tel: ....., mail: .....

2. Kontakt z Inspektorem Ochrony Danych w .....możliwy jest pod numerem tel. nr. ..... lub adresem email (adres email): .....

3. Monitoring stosowany jest celu ochrony mienia oraz zapewnienia bezpieczeństwa na terenie monitorowanym.

4. Podstawą przetwarzania jest prawnie usprawiedliwiony interes administratora / przepis prawa.

5. Zapisy z monitoringu przechowywane będą w okresie 30 dni.

6. Osoba zarejestrowana przez system monitoringu ma prawo do dostępu do danych osobowych oraz ograniczenia przetwarzania.

7. Osobie zarejestrowanej przez system monitoringu przysługuje prawo wniesienia skargi do organu nadzorczego – Prezesa Urzędu Ochrony Danych.

Załącznik Nr 19 do Polityki Ochrony Danych Osobowych

LISTA POTENCJALNYCH ZABEZPIECZEŃ

L.p.	Zabezpieczenie	Opis	Rodzaj zabezpieczenia
1			
2			
3			
4			
5			
6			
7			
8			
9			