

Zarządzenie Nr 11 /2018
Kierownika Ośrodka Pomocy Społecznej w Górze Kalwarii
z dnia 01.08.2018 r.

w sprawie wprowadzenia Polityki bezpieczeństwa danych osobowych w Ośrodku
Pomocy Społecznej w Górze Kalwarii

Na podstawie art. 24 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 oraz § 3-5 Rozporządzenia Ministra Spraw Wewnętrznych i Administracji z 29 kwietnia 2004 r. w sprawie dokumentacji przetwarzania danych osobowych oraz warunków technicznych i organizacyjnych, jakim powinny odpowiadać urządzenia i systemy informatyczne służące do przetwarzania danych osobowych (Dz. U. Nr 100, poz. 1024), zarządza się, co następuje:

§ 1

Wprowadza się Politykę bezpieczeństwa danych osobowych w Ośrodku Pomocy Społecznej w Górze Kalwarii, zwaną dalej „Polityką bezpieczeństwa”, która stanowi załącznik do niniejszego zarządzenia.

§ 2

Zobowiązuje się pracowników Ośrodka Pomocy Społecznej w Górze Kalwarii do stosowania zasad określonych w Polityce bezpieczeństwa.

§ 3

Wykonanie zarządzenia powierza się Inspektorowi Ochrony Danych.

§ 4

Traci moc zarządzenie Kierownika Ośrodka Pomocy Społecznej w Górze Kalwarii nr 10/2018 z dnia 25.08.2018 r. w części dotyczącej polityki bezpieczeństwa. W pozostałej części Zarządzenie powyższe nie ulega zmianie.

§ 5

Zarządzenie wchodzi w życie z dniem podpisania

Kierownik
Ośrodka Pomocy Społecznej
w Górze Kalwarii

mgr Katarzyna Łagowska



ZATWIERDZAM

Egz. nr.....

.....
Kierownik Ośrodka Pomocy
Społecznej w Górze Kalwarii
mgr Katarzyna Łagowska

**POLITYKA
BEZPIECZEŃSTWA DANYCH OSOBOWYCH
OŚRODKA POMOCY SPOŁECZNEJ
GÓRA KALWARIA**

Góra Kalwaria sierpień 2018 r

SPIS TREŚCI

Strona

ROZDZIAŁ I	Postanowienia ogólne	3
ROZDZIAŁ II	Cel oraz główne założenia ochrony danych	4
ROZDZIAŁ III	Zadania Inspektora Ochrony Danych	4
ROZDZIAŁ IV	Przedsięwzięcia zabezpieczające przed naruszeniem systemu ochrony danych osobowych	5
ROZDZIAŁ V	Zasady bezpiecznego przetwarzania danych osobowych.....	7
ROZDZIAŁ VI	Postępowanie w przypadku naruszenia lub podejrzenia naruszenia ochrony danych osobowych	7
ROZDZIAŁ VII	Postanowienia końcowe	9

ZAŁĄCZNIKI

1. Wykaz budynków i pomieszczeń w których przetwarzane są dane osobowe.....	12
2. Wykaz zbiorów danych osobowych	13
3. Struktura zbiorów danych osobowych.....	14

ROZDZIAŁ I

Postanowienia ogólne

1. Polityka bezpieczeństwa danych osobowych, zwana dalej Polityką, określa środki techniczne i organizacyjne zastosowane przez Administratora Danych dla zapewnienia ochrony danych osobowych oraz tryb postępowania w przypadku stwierdzenia naruszenia zabezpieczenia danych osobowych w systemie informatycznym lub kartotekach, albo w sytuacji powzięcia podejrzenia o takim naruszeniu.
2. Politykę opracowano zgodnie z wymogami 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.
3. Ilekoć w Polityce jest mowa o:
 1. **zbiorze danych** - rozumie się przez to oznacza uporządkowany zestaw danych osobowych dostępnych według określonych kryteriów, niezależnie od tego, czy zestaw ten jest scentralizowany, zdecentralizowany czy rozproszony funkcjonalnie lub geograficznie;
 2. **przetwarzaniu danych** - rozumie się przez to operację lub zestaw operacji wykonywanych na danych osobowych lub zestawach danych osobowych w sposób zautomatyzowany lub nieautomatyzowany, taką jak zbieranie, utrwalanie, organizowanie, porządkowanie, przechowywanie, adaptowanie lub modyfikowanie, pobieranie, przeglądanie, wykorzystywanie, ujawnianie poprzez przesłanie, rozpowszechnianie lub innego rodzaju udostępnianie, dopasowywanie lub łączenie, ograniczanie, usuwanie lub niszczenie;
 3. **systemie informatycznym** - rozumie się przez to zespół współpracujących ze sobą urządzeń, programów, procedur przetwarzania informacji i narzędzi programowych zastosowanych w celu przetwarzania danych;
 4. **kartotece** - rozumie się przez to zewidencjonowany, usystematyzowany zbiór wykazów, skróty, wydruków komputerowych i innej dokumentacji gromadzonej w formie papierowej, zawierającej dane osobowe;
 5. **Administratorze Danych Osobowych (ADO)** - rozumie się przez to Ośrodek Pomocy Społecznej,
 6. **Kierownik** - rozumie się przez to Kierownika Ośrodka Pomocy Społecznej,
 7. **Inspektorze Ochrony Danych (IOD)** - rozumie się przez to osobę odpowiedzialną za stosowanie środków technicznych i organizacyjnych zapewniających ochronę przetwarzanych danych osobowych, odpowiednich do zagrożeń oraz kategorii danych objętych ochroną, a w szczególności za zabezpieczenie danych osobowych przed ich udostępnieniem osobom nieupoważnionym, zabranie przez osobę nieuprawnioną, przetwarzaniem z naruszeniem ustawy oraz zmianą, utratą, uszkodzeniem lub zniszczeniem, oraz za podejmowanie odpowiednich działań w przypadku wykrycia naruszeń w systemie zabezpieczeń, upoważnioną do nadzoru i kontroli w zakresie określonym przepisami o ochronie danych osobowych oraz regulacjami wewnętrznymi Administratora Danych;
 8. **osobie odpowiedzialnej za prawidłowe funkcjonowanie sprzętu, oprogramowania i jego konserwacji** - rozumie się przez to informatyka odpowiedzialnego za powyższe zadania;
 9. **użytkownika** - rozumie się przez to osobę wyznaczoną przez Kierownika lub osobę przez niego upoważnioną, uprawnioną do bezpośredniego dostępu do danych osobowych przetwarzanych w systemie informatycznym oraz kartotekach, posiadających ustalony identyfikator i hasło;
 10. **pracownika ochrony** - rozumie się przez to osobę wykonującą zadania z zakresu ochrony osób i mienia na rzecz Administratora Danych;
 11. **pomieszczeniach** - rozumie się przez to budynki, pomieszczenia lub części pomieszczeń określone przez Administratora Danych, tworzące obszar, w którym przetwarzane są dane osobowe z użyciem stacjonarnego sprzętu komputerowego oraz gromadzone w kartotekach;
 12. **polityce bezpieczeństwa** - należy rozumieć określenie zadań, które należy realizować dla zapewnienia spójności wszystkich zabezpieczeń danych osobowych.

ROZDZIAŁ II

Cel oraz główne założenia ochrony danych osobowych

1. Celem zabezpieczenia ochrony danych osobowych jest zapewnienie:

- a) przetwarzania zgodnie z prawem, rzetelnie i w sposób przejrzysty dla osoby, której dane dotyczą;
- b) zbierania w konkretnych, wyraźnych i prawnie uzasadnionych celach i nieprzetwarzania dalej w sposób niezgodny z tymi celami;
- c) przetwarzania danych adekwatnego, stosownego oraz ograniczonego do tego, co niezbędne do celów, w których są przetwarzane ;
- d) przetwarzania prawidłowego i w razie potrzeby uaktualniania; podejmowania wszelkich rozsądnych działań, aby dane osobowe, które są nieprawidłowe w świetle celów ich przetwarzania, zostały niezwłocznie usunięte lub sprostowane;
- e) przechowywania w formie umożliwiającej identyfikację osoby, której dane dotyczą, przez okres nie dłuższy, niż jest to niezbędne do celów, w których dane te są przetwarzane; dane osobowe można przechowywać przez okres dłuższy, o ile będą one przetwarzane wyłącznie do celów archiwalnych w interesie publicznym, do celów badań naukowych lub historycznych lub do celów statystycznych na mocy art. 89 ust. 1, z zastrzeżeniem że wdrożone zostaną odpowiednie środki techniczne i organizacyjne wymagane na mocy niniejszego rozporządzenia w celu ochrony praw i wolności osób, których dane dotyczą;
- f) przetwarzania w sposób zapewniający odpowiednie bezpieczeństwo danych osobowych, w tym ochrony przed niedozwolonym lub niezgodnym z prawem przetwarzaniem oraz przypadkową utratą, zniszczeniem lub uszkodzeniem, za pomocą odpowiednich środków technicznych lub organizacyjnych

2. Realizację powyższych celów powinny zagwarantować następujące przedsięwzięcia:

- 1) wdrożenie procedur określających postępowanie osób zatrudnionych przy przetwarzaniu danych osobowych oraz ich odpowiedzialność za ochronę tych danych,
- 2) przeszkolenie użytkowników w zakresie bezpieczeństwa i ochrony danych osobowych,
- 3) przypisanie użytkownikom określonych atrybutów pozwalających na ich identyfikację (hasła, identyfikatory) oraz zapewniających dostęp użytkownikom do różnych poziomów baz danych osobowych - stosownie do indywidualnego zakresu upoważnienia,
- 4) podejmowanie niezbędnych działań w celu likwidacji słabych ogniw w systemie zabezpieczeń,
- 5) okresowe sprawdzanie przestrzegania przez użytkowników wdrożonych metod postępowania przy przetwarzaniu danych osobowych,
- 6) opracowanie procedur odtwarzania systemu w przypadku wystąpienia awarii,
- 7) śledzenie osiągnięć w dziedzinie zabezpieczania systemów informatycznych i w miarę możliwości organizacyjnych i techniczno-finansowych - wdrażanie nowych narzędzi i metod pracy oraz sposobów zarządzania systemem informatycznym, które będą służyły wzmocnieniu bezpieczeństwa danych osobowych.

3. Za przestrzeganie zasad ochrony i bezpieczeństwa danych w komórkach organizacyjnych odpowiedzialni są kierownicy tych komórek.

ROZDZIAŁ III

Zadania Inspektora Ochrony Danych

1. Inspektor ochrony danych ma następujące zadania:

- a) informowanie administratora oraz pracowników, którzy przetwarzają dane osobowe, o

obowiązkach spoczywających na nich na mocy Rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. oraz innych przepisów Unii lub państw członkowskich o ochronie danych i doradzanie im w tej sprawie;

b) monitorowanie przestrzegania opisanego rozporządzenia, innych przepisów Unii lub państw członkowskich o ochronie danych oraz polityk administratora lub podmiotu przetwarzającego w dziedzinie ochrony danych osobowych, w tym podział obowiązków, działania zwiększające świadomość, szkolenia personelu uczestniczącego w operacjach przetwarzania oraz powiązane z tym audyty;

c) udzielanie na żądanie zaleceń co do oceny skutków dla ochrony danych oraz monitorowanie jej wykonania zgodnie z art. 35 rozporządzenia;

d) współpraca z organem nadzorczym;

e) pełnienie funkcji punktu kontaktowego dla organu nadzorczego w kwestiach związanych z przetwarzaniem, w tym z uprzednimi konsultacjami, o których mowa w art. 36 rozporządzenia, oraz w stosownych przypadkach prowadzenie konsultacji we wszelkich innych sprawach.

2. Inspektor ochrony danych wypełnia swoje zadania z należyтым uwzględnieniem ryzyka związanego z operacjami przetwarzania, mając na uwadze charakter, zakres, kontekst i cele przetwarzania.

Administrator wspiera inspektora ochrony danych w wypełnianiu przez niego zadań, o których mowa powyżej, zapewniając mu zasoby niezbędne do wykonania tych zadań oraz dostęp do danych osobowych i operacji przetwarzania, a także zasoby niezbędne do utrzymania jego wiedzy fachowej.

Administrator Bezpieczeństwa Informacji ma prawo:

1. wyznaczania, rekomendowania i egzekwowania wykonania zadań związanych z ochroną danych osobowych w całej organizacji
2. wstępu do pomieszczeń w których zlokalizowane są zbiory danych i przeprowadzenia niezbędnych badań lub innych czynności kontrolnych w celu oceny zgodności przetwarzania danych z ustawą,
3. żądać złożenia pisemnych lub ustnych wyjaśnień w zakresie niezbędnym do ustalenia stanu faktycznego,
4. żądać okazania dokumentów i wszelkich danych mających bezpośredni związek z problematyką kontroli,
5. żądać udostępnienia do kontroli urządzeń, nośników oraz systemów informatycznych służących do przetwarzania danych,

ROZDZIAŁ IV

Przedsięwzięcia zabezpieczające przed naruszeniem systemu ochrony danych osobowych

Przedsięwzięcia ochrony fizycznej

1. Do podstawowych zabezpieczeń przed naruszeniem ochrony danych osobowych należą:

- 1) wydzielenie pomieszczeń w których będą przetwarzane dane osobowe,
- 2) wyposażenie pomieszczeń w odpowiednie szafy,
- 3) zabezpieczenie wejść do pomieszczeń zamkami,
- 4) zainstalowanie systemu alarmowego,
- 5) objęcie siedziby Działu Pomocy Środowiskowej opieką agencji ochrony

2. Dostęp do pomieszczeń:

- 1) stały dostęp do pomieszczeń mają tylko użytkownicy,
- 2) dostęp do sprzętu komputerowego mają wyłącznie użytkownicy oraz osoby posiadające

aktualne upoważnienia,

- 3) sprzątaczkę, w celu wykonania prac porządkowych, mają dostęp do pomieszczeń tylko w obecności osób tam pracujących,
 - 4) pozostałe osoby mogą przebywać w pomieszczeniach tylko w obecności użytkowników.
3. Klucze do pomieszczeń w budynku mieszczącym Dział Pomocy Środowiskowej posiada Kierownik OPS, Koordynator Działu Pomocy Środowiskowej oraz jeden, wyznaczony na stałe, pracownik socjalny, natomiast w budynku mieszczącym Dział Świadczeń Rodzinnych oraz Księgowość – Główny Księgowy, księgowy i inspektor ds świadczeń rodzinnych.
4. Główny Księgowy, księgowy i inspektor ds świadczeń rodzinnych mają też obowiązek otwierania i zamykania budynku OPS, w którym mieści się Dział Świadczeń Rodzinnych oraz Księgowość.
5. W budynkach świetlicy środowiskowej klucze do pomieszczeń ma każda z wychowawczyń (3 osoby w Czersku i 3 osoby w Górze Kalwarii) i każda wychowawczyni odpowiada za bezpieczne ich przechowywanie.

Przedsięwzięcia organizacyjne

1. Został powołany Inspektor Ochrony Danych nadzorujący przestrzeganie zasad ochrony przetwarzania danych osobowych.
2. Każdy nowo zatrudniany pracownik - przed dopuszczeniem do dostępu do danych osobowych podlega przeszkoleniu z przepisów o ochronie danych osobowych oraz wynikających z nich zadań oraz obowiązków.
3. Wszyscy użytkownicy podlegają okresowym szkoleniom, stosownie do potrzeb wynikających ze zmian w systemie informatycznym (wymiana sprzętu na nowszej generacji, zmiana oprogramowania) oraz w związku ze zmianą przepisów o ochronie danych osobowych lub zmianą wewnętrznych regulacji.
4. Za organizację i prowadzenie szkoleń, odpowiedzialny jest Inspektor Ochrony Danych.
5. Użytkownicy powinni mieć świadomość możliwości zaistnienia sytuacji naruszenia ochrony danych osobowych, w tym celu powinni:
 - 1) zwracać szczególną uwagę przy wchodzeniu i wychodzeniu z obiektu na podejrzane osoby.
 - 2) przestrzegać procedur związanych z otwieraniem i zamykaniem pomieszczeń, a także z wejściem do obszarów przetwarzania danych osobowych osób nieupoważnionych,
 - 3) informować Inspektora Ochrony Danych o podejrzanych osobach, tj.:
 - a) osobach przebywających w pomieszczeniach bez wyraźnego celu;
 - b) osobach posiadających przy sobie podejrzane bagaże, w których mogą być ukryte niebezpieczne przedmioty;
 - 4) przestrzegać zasad i procedur ochrony danych osobowych, w czasie pracy a także po jej zakończeniu.
6. Użytkownicy zobowiązani są, na podstawie dokonanej identyfikacji ewentualnych zagrożeń, przedkładać Inspektorowi Ochrony Danych projekty i propozycje stosownych rozwiązań, których celem jest zabezpieczenie przed naruszeniem ochrony danych osobowych.
7. Użytkownicy zobowiązani są do przestrzegania przepisów o ochronie danych osobowych, a także do ścisłej współpracy z Inspektorem Ochrony Danych. W tym celu zobowiązani są do:
 - 1) pisemnego wnioskowania o rejestrację nowych zbiorów danych osobowych,
 - 2) okresowego składania informacji o funkcjonowaniu mechanizmów zabezpieczeń i ochrony,
 - 3) występowania z wnioskami w sprawie wprowadzenia niezbędnych zmian w zakresie ochrony danych osobowych.

ROZDZIAŁ V

Zasady bezpiecznego przetwarzania danych osobowych

1. Przetwarzać dane osobowe mogą tylko użytkownicy (pracownicy posiadający imienne upoważnienie wydane przez Administratora Danych)
2. Przetwarzanie danych osobowych z użyciem stacjonarnego sprzętu komputerowego i kartotek odbywa się wyłącznie w obszarze przetwarzania danych, pomieszczeniach Ośrodka Pomocy Społecznej.
3. Przetwarzanie danych osobowych w urządzeniach przenośnych może odbywać się poza obszarem przetwarzania danych, wyłącznie za zgodą Kierownika lub Inspektora Ochrony Danych.
4. Wykaz budynków tworzących obszar w którym przetwarzane są dane osobowe zawiera załącznik nr 1 do niniejszej Polityki.
5. Przebywanie osób trzecich w pomieszczeniach gdzie przetwarzane są dane osobowe może odbywać się wyłącznie w obecności użytkowników.
6. Stały dostęp do pomieszczeń, w których przetwarzane są dane osobowe, mają tylko osoby upoważnione przez administratora danych.
7. Przebywanie użytkownika po godzinach pracy w pomieszczeniach, w których przetwarzane są dane osobowe jest dopuszczalne jedynie za zgodą Kierownika.
8. W trakcie prac technicznych wykonywanych przez osoby trzecie w pomieszczeniach, przetwarzanie danych jest zabronione.

ROZDZIAŁ VI

Postępowanie w przypadku naruszenia lub podejrzenia naruszenia ochrony danych osobowych

1. Przed przystąpieniem do pracy użytkownik obowiązany jest dokonać sprawdzenia stanu urządzeń komputerowych oraz oględzin swojego stanowiska pracy, ze zwróceniem szczególnej uwagi, czy nie zaszły okoliczności wskazujące na naruszenie lub próby naruszenia ochrony danych osobowych.
2. W przypadku stwierdzenia naruszenia lub zaistnienia okoliczności wskazujących na naruszenia ochrony danych osobowych, użytkownik zobowiązany jest do bezzwłocznego powiadomienia o tym fakcie Inspektora Ochrony Danych.
3. Obowiązek określony w ust. 2 ciąży również na pozostałych pracownikach Administratora Danych.
4. Postanowienia ust. 2 i 3 mają zastosowanie zarówno w przypadku naruszenia lub podejrzenia naruszenia ochrony danych osobowych gromadzonych w systemie informatycznym, jak i w kartotekach.
5. Do czasu przybycia Inspektora Ochrony Danych, zgłaszający:
 - 1) powstrzymuje się od rozpoczęcia lub kontynuowania pracy, jak również od podejmowania jakichkolwiek czynności, mogących spowodować zatarcie śladów naruszenia bądź innych dowodów,
 - 2) zabezpiecza elementy systemu informatycznego lub kartotek, przede wszystkim poprzez uniemożliwienie dostępu do nich osób nieupoważnionych,
 - 3) podejmuje, stosownie do zaistniałej sytuacji, wszelkie niezbędne działania celem zapobieżenia dalszym zagrożeniom, które mogą skutkować utratą danych osobowych.
6. W przypadku stwierdzenia naruszenia lub zaistnienia okoliczności wskazujących na naruszenia ochrony danych osobowych, Inspektor Ochrony Danych, po przybyciu na miejsce:
 - 1) ocenia zaistniałą sytuację, biorąc pod uwagę w szczególności stan pomieszczeń, w których przetwarzane są dane oraz stan urządzeń, a także identyfikuje wielkość negatywnych

następstw incydentu,

2) wysłuchuje relacji osoby, która dokonała powiadomienia,

3) podejmuje decyzje o toku dalszego postępowania, stosownie do zakresu naruszenia lub zasadności podejrzenia naruszenia ochrony danych osobowych.

7. 1) W przypadku naruszenia ochrony danych osobowych, administrator 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 Rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r., 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) Podmiot przetwarzający po stwierdzeniu naruszenia ochrony danych osobowych bez zbędnej zwłoki zgłasza je administratorowi.

3) Zgłoszenie, o którym mowa w ust. 1, 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 administratora w celu zaradzenia naruszeniu ochrony danych osobowych, w tym w stosownych przypadkach środki w celu zminimalizowania jego ewentualnych negatywnych skutków.

4) Jeżeli – i w zakresie, w jakim – informacji nie da się udzielić w tym samym czasie, można je udzielać sukcesywnie bez zbędnej zwłoki.

5) Administrator dokumentuje wszelkie naruszenia ochrony danych osobowych, w tym okoliczności naruszenia ochrony danych osobowych, jego skutki oraz podjęte działania zaradcze. Dokumentacja ta musi pozwolić organowi nadzorczemu weryfikowanie przestrzegania postanowień Rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r.

8. Administrator Bezpieczeństwa Informacji podejmuje kroki zmierzające do likwidacji naruszeń zabezpieczeń danych osobowych i zapobieżenia wystąpieniu ich w przyszłości. W tym celu:

1) w miarę możliwości przywraca stan zgodny z zasadami zabezpieczenia systemu,

2) relacjonuje Kierownikowi przedsiębiorstwa czynności

3) o ile taka potrzeba zachodzi, postuluje wprowadzenie nowych form zabezpieczenia, a w razie ich wprowadzenia nadzoruje zaznajamianie z nimi osób zatrudnionych przy przetwarzaniu danych osobowych.

9. W przypadku, gdy naruszenie ochrony danych osobowych jest wynikiem uchybienia obowiązującej u Administratora Danych dyscypliny pracy, Administrator Bezpieczeństwa Informacji wnioskuję do Kierownika o wyjaśnienie wszystkich okoliczności incydentu i o podjęcie stosownych działań wobec sprawcy / sprawców.

10. W przypadku zaginięcia komputera lub nośników magnetycznych, na których były zgromadzone dane osobowe, użytkownik posługujący się komputerem niezwłocznie powiadamia Inspektora Ochrony Danych lub upoważnioną przez niego osobę, a w przypadku kradzieży występuje o

powiadomienie jednostki policji.

11. Osoba zatrudniona przy przetwarzaniu danych osobowych za naruszenie obowiązków wynikających z niniejszej Polityki oraz przepisów o ochronie danych osobowych ponosi odpowiedzialność przewidzianą w Regulaminie Pracy, Kodeksie Pracy oraz wynikającą z Rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. a także z ustawy o ochronie danych osobowych (Dz. U. z 2018 r., poz. 1000).

12.1) Jeżeli naruszenie ochrony danych osobowych może powodować wysokie ryzyko naruszenia praw lub wolności osób fizycznych, administrator bez zbędnej zwłoki zawiadamia osobę, której dane dotyczą, o takim naruszeniu.

2) Zawiadomienie, o którym mowa w ust. 1, jasnym i prostym językiem opisuje charakter naruszenia ochrony danych osobowych oraz zawiera przynajmniej informacje i środki, o których mowa w pkt. 7 niniejszego rozdziału ust. 3 lit. b), c) i d).

3) Zawiadomienie, o którym mowa w ust. 1, nie jest wymagane, w następujących przypadkach:

a) administrator wdrożył odpowiednie techniczne i organizacyjne środki ochrony i środki te zostały zastosowane do danych osobowych, których dotyczy naruszenie, w szczególności środki takie jak szyfrowanie, uniemożliwiające odczyt osobom nieuprawnionym do dostępu do tych danych osobowych;

b) administrator zastosował następnie środki eliminujące prawdopodobieństwo wysokiego ryzyka naruszenia praw lub wolności osoby, której dane dotyczą, o którym mowa w ust. 1;

c) wymagałoby ono niewspółmiernie dużego wysiłku. W takim przypadku wydany zostaje publiczny komunikat lub zastosowany zostaje podobny środek, za pomocą którego osoby, których dane dotyczą, zostają poinformowane w równie skutecznym sposób.

4) Jeżeli administrator nie zawiadomił jeszcze osoby, której dane dotyczą, o naruszeniu ochrony danych osobowych, organ nadzorczy – biorąc pod uwagę prawdopodobieństwo, że to naruszenie ochrony danych osobowych spowoduje wysokie ryzyko – może od niego tego zażądać lub może stwierdzić, że spełniony został jeden z warunków, o których mowa w ust. 3.

ROZDZIAŁ VII

Postanowienia końcowe

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

2. Użytkownicy obowiązani są zapoznać się z treścią niniejszej Polityki.

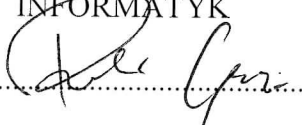
3. Użytkownicy składają oświadczenie, iż zostali zaznajomiony z przepisami ustawy o ochronie danych osobowych oraz wydanymi na jej podstawie aktami wykonawczymi oraz instrukcjami obowiązującymi u Administratora Danych, a także o zobowiązaniu się do ich przestrzegania.

4. Wzór oświadczenia o którym mowa w ust. 3 stanowi załącznik nr 2 do Instrukcji zarządzania systemem informatycznym.

5. Oświadczenie przechowywane jest w aktach personalnych pracownika.

6. W sprawach nieuregulowanych w niniejszej Instrukcji mają zastosowanie przepisy Rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. oraz ustawy z dnia 24 maja 2018, o ochronie danych osobowych (Dz.U. z 2018 r. poz. 1000) oraz wydanych na jej podstawie aktów wykonawczych.

INFORMATYK

.....


INSPEKTOR
OCHRONY DANYCH

.....


*Załącznik nr 1 do Polityki bezpieczeństwa danych osobowych***WYKAZ
BUDYNKÓW I POMIESZCZEŃ W KTÓRYCH PRZETWARZANE SĄ DANE OSOBOWE**

L.p.	Adres budynku	Pomieszczenie	Uwagi
1.	Góra Kalwaria ul. Pijarska 40	parter – wszystkie pokoje	
2.	Góra Kalwaria ul. Rotmistrza Pileckiego 10	Parter budynku – część przeznaczona dla Działu Pomocy Środowiskowej	
3.	Czersk, Plac Tysiąclecia 14 A 05-530 Góra Kalwaria	Parter – dwa pokoje	
4.	Góra Kalwaria ul. Ks. Sajny 4	Parter – pokój	

Załącznik nr 2 do Polityki bezpieczeństwa danych osobowych

WYKAZ
ZBIORÓW DANYCH OSOBOWYCH

L.p.	Nazwa zbioru	Postać zbioru	Program komputerowy wykorzystywany do przetwarzania danych w zbiorze	Uwagi
1	2	3	4	5
1.	Osoby korzystające z pomocy społecznej.	papierowo-elektroniczna	- TT Pomoc - Pakiet biurowy MS Office - Płatnik	
2.	Świadczenia rodzinne.	papierowo-elektroniczna	- Świadczenia Rodzinne - Płatnik - Pakiet biurowy MS Office	
3.	Dodatki mieszkaniowe.	papierowo-elektroniczna	- TT Dodatki Mieszkaniowe	
4.	Osoby świadczące usługi na podstawie umów cywilnoprawnych.	papierowo-elektroniczna	- PERSON - PŁATNIK - DOS	
5.	Akta osobowe oraz wynagrodzenie pracowników.	papierowo-elektroniczna	- PERSON - PŁATNIK - DOS	
6.	Kandydaci do pracy w Ośrodku Pomocy Społecznej	papierowa		
7.	Sprawy alimentacyjne	papierowo-elektroniczna	- TT Alimony - Pakiet biurowy MS Office	
8.	Przemoc w rodzinie	papierowa		
9.	Stypendia i zasiłki szkolne	papierowo-elektroniczna	TT Stypendia - Pakiet biurowy MS Office	
10.	Wolontariat	papierowa		
11.	Obieg dokumentów w OPS	Papierowo-elektroniczna	E-kancelaria	
12.	Świetlica środowiskowa	papierowa		
13.	Za życiem	Papierowo-elektroniczna	- Świadczenia rodzinne - Pakiet biurowy MS Office	
14.	Program „Dobry start”	Papierowo-elektroniczna	- Świadczenia rodzinne - Pakiet biurowy MS Office	

STRUKTURA ZBIORÓW DANYCH OSOBOWYCH

L.p.	Nazwa zbioru	Opis zbioru	Pola powiązane
1	2	3	4
1.	Osoby korzystające z pomocy społecznej.	nazwisko i imię, imiona rodziców, obywatelstwo, data urodzenia, stan cywilny, numer ewidencyjny PESEL, miejsce zameldowania, wykształcenie, wykonywany zawód, miejsce pracy lub nauki, pozycja na rynku pracy, sytuacja zdrowotna, źródła dochodu i ich wysokość, sytuacja mieszkaniowa w tym standard i utrzymanie mieszkania, stosunki rodzinne, kwalifikacje, umiejętności oraz doświadczenie zawodowe, stan rodzinny (imiona i daty urodzenia dzieci, seria i numer dowodu potwierdzającego tożsamość, stan zdrowia, nałogi, stan rodzinny, stan majątkowy, numer telefonu.	brak
2.	Świadczenia rodzinne.	nazwisko i imię, obywatelstwo, data urodzenia, stan cywilny, numer ewidencyjny PESEL, miejsce zamieszkania, NIP, źródła dochodu i ich wysokość, stan rodzinny, stan zdrowia, numer telefonu.	brak
3.	Dodatki mieszkaniowe.	nazwisko i imię, data urodzenia, adres zamieszkania, sytuacja mieszkaniowa, dochodu i ich wysokość, niepełnosprawność, stan rodzinny,	brak
4.	Osoby świadczące usługi na podstawie umów cywilnoprawnych.	nazwiska, nazwiska rodowe, imiona, data urodzenia, wykształcenie, obywatelstwo, okresy zatrudnienia, konta bankowe, dane o ubezpieczeniu, adres zameldowania, adres zamieszkania, adres do korespondencji.	brak

1	2	3	4
5.	Akta osobowe oraz wynagrodzenie pracowników.	nazwisko i imiona,nazwisko rodowe,imiona rodziców,nazwisko rodowe matki, data urodzenia, miejsce urodzenia, obywatelstwo, numer ewidencyjny PESEL, NIP, miejsce zameldowania, wykształcenie,zawód,specjalność,stopień, tytuł zawodowy (naukowy), wykształcenie uzupełniające,przebieg zatrudnienia, znajomość języków obcych,prawo jazdy, stan rodzinny (imiona i daty urodzenia dzieci, stosunek do powszechnego obowiązku obrony, stopień wojskowy, numer specjalności wojskowej, przynależność do WKU,numer książeczki wojskowej, przydział mobilizacyjny, nazwisko imię oraz adres osoby którą należy powiadomić w razie wypadku, seria i numer dowodu osobistego oraz przez kogo wydany, stan zdrowia.	brak
6.	Kandydaci do pracy w Ośrodku Pomocy Społecznej	nazwiska i imiona,imiona rodziców,data urodzenia, miejsce urodzenia, adres zamieszkania lub pobytu, numer ewidencyjny PESEL, miejsce pracy,zawód, wykształcenie, seria i numer dowodu osobistego,numer telefonu,dane dotyczące dodatkowych umiejętności, zainteresowania, stan cywilny,dane dotyczące skazań, stosunek do powszechnego obowiązku obrony RP	
7.	Sprawy alimentacyjne	nazwisko i imię (imiona) ,nazwisko rodowe,imiona rodziców, nazwisko rodowe matki, obywatelstwo, data i miejsce urodzenia,stan cywilny, numer ewidencyjny PESEL, miejsce zamieszkania, NIP,wykształcenie, zawód wyuczony, zawód wykonywany, dodatkowe kwalifikacje, seria i nr prawa jazdy, źródła dochodu i ich wysokość, sytuacja mieszkaniowa, stan majątkowy, sytuacja rodzinna, seria i numer dowodu osobistego, stan zdrowia, numer telefonu.	

1	2	3	4
8	Przemoc w rodzinie	nazwiska i imiona, imiona rodziców, data urodzenia, miejsce urodzenia, adres zamieszkania lub pobytu, numer ewidencyjny PESEL, miejsce pracy, zawód, wykształcenie, seria i numer dowodu osobistego, numer telefonu, stan zdrowia, nałogi, skazania, orzeczenia o ukaraniu, inne orzeczenia wydane w postępowaniu sądowym lub administracyjnym, obywatelstwo, stan cywilny, dodatkowe kwalifikacje, źródła dochodu i ich wysokość, sytuacja mieszkaniowa, stan majątkowy, stan rodzinny.	
9	Stypendia i zasiłki szkolne	nazwiska, imiona, imiona rodziców, data i miejsce urodzenia, adres zamieszkania lub pobytu, nr ewidencyjny PESEL, źródła dochodów i ich wysokość, miejsce pracy, numer telefonu, obywatelstwo, nr konta bankowego.	
10	Wolontariat	nazwiska, imiona, adres zamieszkania, adres zameldowania, telefon, data i miejsce urodzenia, e-mail, telefon do rodzica, data urodzenia, PESEL, wykształcenie, stopień aktywności zawodowej, nazwa szkoły, uczelni, wykształcenie	
11	Obieg dokumentów w OPS	Nazwiska, imiona, adres zamieszkania, adres zameldowania, telefon, e-mail, PESEL	
12	Świetlica środowiskowa	Nazwiska, imiona, adres zamieszkania, adres zameldowania, data urodzenia, PESEL	
13	Za życiem	Nazwiska i imiona, imiona rodziców, data urodzenia, miejsce urodzenia, adres zamieszkania lub pobytu, numer ewidencyjny PESEL, seria i numer dowodu osobistego numer telefonu, stan zdrowia, inne orzeczenia wydane w postępowaniu sądowym lub administracyjnym	
14	Program „Dobry start”	Nazwiska i imiona, imiona rodziców, data urodzenia, miejsce zamieszkania, adres zamieszkania lub pobytu, numer ewidencyjny PESEL, seria i numer dowodu osobistego, numer telefonu, stan zdrowia, inne orzeczenia wydane w postępowaniu sądowym lub administracyjnym.	