Załącznik nr 1 do zarządzenia nr 11/2016

Kierownika Gminnego Ośrodka Pomocy Społecznej w Książkach

z dnia 08 grudnia 2016

POLITYKA BEZPIECZEŃSTWA INFORMACJI

W GMINNYM OŚRODKU POMOCY SPOŁECZNEJ W KSIĄŻKACH

SPIS TREŚCI

§ 1

Postanowienia ogólne

1. Polityka Bezpieczeństwa Informacji określa zbiór zasad przetwarzania danych osobowych w Gminnym Ośrodku Pomocy Społecznej w Książkach oraz ich zabezpieczenia jako zestaw praw, reguł i zaleceń regulujących sposób ich zarządzania, ochrony i dystrybucji w Gminnym Ośrodku Pomocy Społecznej.
2. Celem Polityki jest wdrożenie i realizacja działań przy wykorzystaniu środków technicznych i organizacyjnych, które zapewnią maksymalny poziom bezpieczeństwa w zakresie przetwarzania danych osobowych, chroniąc je przed nieautoryzowanym dostępem, przetwarzaniem z naruszeniem przepisów określających zasady postępowania przy przetwarzaniu danych osobowych oraz przed zmianą, uszkodzeniem lub zniszczeniem.
3. Cele Polityki realizowane są poprzez zapewnienie danym osobowym następujących cech osobowych:
   1) poufności – właściwości zapewniającej, ze dane nie są udostępniane nieupoważnionym podmiotom;
   2) integralności – właściwości zapewniającej, że dane osobowe nie zostały zmienione lub zniszczone w sposób nieautoryzowany;
   3) rozliczalności – właściwości zapewniającej, ze działania podmiotu mogą być przypisane w sposób jednoznaczny tylko temu podmiotowi;
   4) zgodności z prawem – właściwości zapewniającej, że gromadzone są wyłącznie dane niezbędne do właściwego funkcjonowania danego podmiotu.
4. Niniejsza Polityka oraz dokumenty z nią powiązane powinny być aktualizowane wraz ze zmieniającymi się przepisami prawa oraz w związku ze zmianami, które powodują że określone zasady przestają być aktualne.

§ 2

Podstawa prawna

1. Polityka opracowana została w oparciu o następujące przepis prawa:
   1) Ustawa o ochronie danych osobowych z dnia 29 sierpnia 1997 r. (Dz. U. 2016.poz. 922 z późn. zm.);
   2) Ustawa z dnia 8 marca 1990r. o samorządzie gminny (Dz. U. z 2016 r. poz. 446);
   3) Rozporządzenie Prezydenta Rzeczypospolitej Polskiej z dnia 3 listopada 2006r. w sprawie nadania statutu Biuru Generalnego Inspektora Ochrony Danych Osobowych (Dz. U. z 2006, Nr 203, poz. 1494) – art. 13.3 ustawy;
   4) Rozporządzenie Prezydenta Rzeczypospolitej Polskiej z dnia 19 listopada 2015 r. zmieniające rozporządzenie w sprawie nadania statutu Biuru Generalnego Inspektora Ochrony Danych Osobowych (Dz. U. 2015, poz. 2020);
   5) Rozporządzenie Ministra Spraw Wewnętrznych i Administracji z dnia 22 kwietnia 2004 r. w sprawie wzorów imiennego upoważnienia i legitymacji służbowej inspektora Biura Generalnego Inspektora Ochrony Danych Osobowych (Dz. U. z 2004 r. Nr 94, poz. 923) – art. 22a ustawy;
   6) Rozporządzenie Ministra Spraw Wewnętrznych i Administracji z dnia 11 maja 2011 r. zmieniające rozporządzenie w sprawie wzorów imiennego upoważnienia i legitymacji służbowej

inspektora Biura Generalnego Inspektora Ochrony Danych Osobowych (Dz. U. z 2011 r. Nr 103, poz. 601);

7) Rozporządzenie Ministra Spraw Wewnętrznych i Administracji z dnia 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. z 2004 r. Nr 100, poz. 1024) – art. 39a ustawy;
8) Rozporządzenie Ministra Spraw Wewnętrznych i Administracji z dnia 11 grudnia 2008 r. w sprawie wzoru zgłoszenia zbioru danych do rejestracji Generalnemu Inspektorowi Ochrony Danych Osobowych (Dz. U. nr 229, poz. 1536) – art. 46a ustawy;
9) Rozporządzenie Ministra Administracji i Cyfryzacji z dnia 10 grudnia 2014 r. w sprawie wzorów zgłoszeń powołania i odwołania administratora bezpieczeństwa informacji (Dz. U. 2014, poz. 1934);
10) Rozporządzenie Ministra Administracji i Cyfryzacji z dnia 11 maja 2015r. w sprawie sposobu prowadzenia przez administratora bezpieczeństwa informacji rejestru zbiorów danych (Dz.U. 2015 poz. 719);
11) Rozporządzenie Ministra Administracji i Cyfryzacji z dnia 11 maja 2015r. w sprawie trybu i sposobu realizacji zadań w celu zapewnienia przestrzegania przepisów o ochronie danych osobowych przez administratora bezpieczeństwa informacji (Dz.U. 2015 poz. 745).

2. Przetwarzanie danych osobowych w Gminnym Ośrodku Pomocy Społecznej w Książkach jest dopuszczalne wyłącznie pod warunkiem przestrzegania ustawy z dnia 29 sierpnia 1997 r. o ochronie danych osobowych i wydanych na jej podstawie przepisów wykonawczych, w tym niniejszej polityki i instrukcji zarządzania systemem informatycznym.
3. Administrator Danych Osobowych zobowiązuje się do podjęcia odpowiednich kroków mających na celu zapewnienie prawidłowej ochrony danych osobowych, a w szczególności dane osobowe są przetwarzane zgodnie z prawem, zbierane dla oznaczonych, zgodnych z prawem celów i nie poddawane dalszemu przetwarzaniu niezgodnie z tymi celami, zabezpieczone środkami technicznymi i organizacyjnymi.

§ 3

Słownik pojęć

1. Określenia i skróty użyte w Polityce Bezpieczeństwa Informacji oznaczają:

1) **Administrator Danych Osobowych** – osoba decydująca o celach i środkach przetwarzania danych osobowych – Kierownik Gminnego Ośrodka Pomocy Społecznej w Książkach, zwany dalej ADO;
2) **Administrator Bezpieczeństwa Informacji** – osoba powołana przez Administratora Danych Osobowych, odpowiedzialna za nadzorowanie stosowania środków technicznych i organizacyjnych, zapewniających ochronę przetwarzanych danych osobowych, w tym w szczególności za przeciwdziałanie dostępowi osób trzecich do systemu, w którym przetwarzane są dane osobowe oraz za podejmowanie odpowiednich działań w przypadku wykrycia naruszeń w systemie ochrony danych osobowych, zwany dalej ABI;
3) **Administrator Systemów Informatycznych/Informatyk** – osoba powołana przez Administratora Danych Osobowych, zwany dalej ASI;
4) **Dane osobowe** – każda informacja dotycząca osoby fizycznej, która w sposób pośredni lub bezpośredni pozwala ją zidentyfikować, w szczególności poprzez podanie jednego lub kilku specyficznych czynników ją określających;
5) **GIODO** – Generalny Inspektor Ochrony Danych Osobowych;

6) **Naruszenie ochrony danych osobowych –** zamierzone lub przypadkowe działanie lub zaniechanie działania, powodujące zagrożenie bezpieczeństwa danych osobowych , przetwarzanych tradycyjnie, jak również z wykorzystaniem systemów informatycznych;
7) **Osoba upoważniona** – osoba posiadająca imienne upoważnienie wydane przez Administratora Danych Osobowych lub Administratora Bezpieczeństwa Informacji i dopuszczona jako użytkownik do przetwarzania danych osobowych w zakresie wskazanym w upoważnieniu;
8) **Osoba trzecia** – należy przez to rozumieć, osobę nie będącą pracownikiem i współpracownikiem Gminnego Ośrodka Pomocy Społecznej w Książkach, dla której nie istnieją podstawy prawne do nadania jej upoważnienia do przetwarzania danych osobowych;
9) **Przetwarzanie danych osobowych** – jakiekolwiek operacje wykonywane na danych osobowych, takie jak zbieranie, utrwalanie, przechowywanie, opracowywanie, zmienianie, udostępnianie i usuwanie, a zwłaszcza te, które wykonuje się w systemach informatycznych;
10) **Ustawa** – ustawa z dnia 29 sierpnia 1997r. o ochronie danych osobowych (tekst jednolity Dz. U. z 2016 r. poz. 922);
11) **System informatyczny** – zespół współpracujących urządzeń, programów, procedur przetwarzania informacji i narzędzi programowych zastosowanych w celu przetwarzania danych;
12) **Zbiór danych osobowych** – każdy posiadający strukturę zestaw danych o charakterze osobowym, dostępnych według określonych kryteriów, niezależnie od tego, czy zestaw ten jest rozproszony lub podzielony funkcjonalnie;
13) **Właściciel zasobów** – osoba odpowiedzialna za gromadzenie i przetwarzanie danych osobowych w komórce organizacyjnej;
14) **Zbiór nieinformatyczny** – zbiór danych osobowych prowadzony poza systemem informatycznym, w szczególności w postaci papierowej;
15) **Identyfikator** – rozumie się przez to ciąg znaków literowych, cyfrowych lub innych, jednoznacznie identyfikujący osobę upoważnioną do przetwarzania danych osobowych w systemie informatycznym;
16) **Hasło –** rozumie się przez to ciąg znaków literowych, cyfrowych lub innych, znany jedynie użytkownikowi.

§4

Odpowiedzialność Administratora Danych Osobowych

1. Administrator Danych Osobowych jest odpowiedzialny za przetwarzanie danych osobowych oraz za ich ochronę zgodnie z przepisami prawa. W tym celu zobowiązany jest do wprowadzenia do stosowania procedur postępowania zapewniających prawidłowe przetwarzanie danych osobowych, rozumiane jako ochronę danych przed ich udostępnieniem osobom upoważnionym, zmianą lub zabraniem przez osobę nieuprawnioną, przetwarzaniem z naruszeniem Ustawy oraz utratą, uszkodzeniem lub zniszczeniem.
2. Do kompetencji Administratora Danych należy w szczególności:
   1) wyznaczanie ABI/ASI;
   2) wskazanie Właścicieli zasobów danych osobowych;
   3) określenie celów i procedur ochrony danych osobowych;
   4) podział zadań i obowiązków związanych z organizacją obszaru ochrony danych osobowych.
3. Do obowiązków Administratora Danych Osobowych należy:

1) zapewnienie poufności, integralności, dostępności i rozliczalności danych przetwarzanych w systemach informatycznych;
2) zapewnienie szkoleń dla pracowników w zakresie przepisów o ochronie danych osobowych oraz informowanie o zagrożeniach związanych z ich przetwarzaniem;
3) przyjmowanie i zatwierdzanie niezbędnych, wymaganych przez przepisy prawa dokumentów regulujących ochronę danych osobowych;
4) nadawanie pracownikom upoważnień do przetwarzania danych osobowych;
5) zapewnienie środków finansowych na ochronę fizyczną pomieszczeń, w których przetwarzane są dane osobowe oraz środków niezbędnych do zapewnienia możliwie najwyższego poziomu bezpieczeństwa danych przetwarzanych w systemach informatycznych;
6) zapewnienie realizacji obowiązku zgłoszenia i aktualizacji zbiorów danych osobowych do rejestracji GIODO;
7) prowadzenie ewidencji osób upoważnionych do ich przetwarzania.

§ 5

Odpowiedzialność Administratora Bezpieczeństwa Informacji

1. Administrator Bezpieczeństwa Informacji jest odpowiedzialny za nadzorowanie stosowania środków technicznych i organizacyjnych zapewniających ochronę przetwarzanych danych osobowych oraz za podejmowanie odpowiednich działań w przypadku wykrycia naruszeń w systemie ochrony danych osobowych.
2. Do kompetencji Administratora Bezpieczeństwa Informacji należy:
   1) dokonywanie sprawdzeń zgodności przetwarzania danych osobowych z przepisami o ochronie danych osobowych oraz opracowania sprawozdania w tym zakresie;
   2) nadzorowanie opracowania i aktualizowania dokumentacji opisującej sposób przetwarzania danych osobowych oraz środki techniczne i organizacyjne zapewniające ochronę przetwarzania danych osobowych odpowiednią do zagrożeń oraz kategorii objętych ochroną;
   3) nadzorowanie przestrzegania zasad określonych w dokumentacji ochrony danych osobowych;
   4) żądanie od wszystkich pracowników GOPS – u wyjaśnień w sytuacjach naruszenia bezpieczeństwa danych osobowych.
3. Do zadań Administratora Bezpieczeństwa Informacji należy:
   1) zapewnienie przestrzegania przepisów o ochronie danych osobowych, w szczególności poprzez:
   a) sprawdzanie zgodności przetwarzania danych osobowych z przepisami o ochronie danych osobowych oraz opracowanie w tym zakresie sprawozdania dla administratora danych;
   b) nadzorowanie opracowania i aktualizowania dokumentacji, o której mowa w art. 36 ust. 2 ustawy oraz przestrzegania zasad w niej określonych;
   c) zapewnienie zapoznania osób upoważnionych do przetwarzania danych osobowych z przepisami o ochronie danych osobowych;
   2) prowadzenie rejestru zbiorów danych przetwarzanych przez administratora danych zgodnie z obowiązującymi przepisami prawa;

3) nadzór nad wdrożeniem stosownych środków organizacyjnych i technicznych w celu ochrony przetwarzanych danych osobowych;

4) nadawanie, zmienianie oraz cofanie uprawnień do przetwarzania danych osobowych na wniosek ADO;

5) prowadzenie dokumentacji opisującej zastosowaną ochronę danych osobowych;

6) reprezentowanie Administratora Danych Osobowych w kontaktach z Biurem GIODO,

7) przygotowywanie zgłoszeń zbiorów danych osobowych do rejestracji w Biurze GIODO;

8) reagowanie na zgłaszane incydenty (zdarzenia, zajścia lub wypadki nie będące częścią standardowych operacji lub usług, które powodują lub mogą spowodować spadek poziomu ochrony danych osobowych) związane z naruszeniem ochrony danych osobowych oraz analizowanie ich przyczyn i kierowanie wniosków dotyczących ukarania winnych naruszeń.

4. Na podstawie art. 36 a ust. 1 ustawy, Administrator Danych może powołać Administratora Bezpieczeństwa Informacji, zgodnie z załącznikiem nr 1 do niniejszej Polityki. Odwołanie ABI następuje w formie pisemnej zgodnie z załącznikiem nr 2 do niniejszej Polityki.
5. W przypadku niewyznaczenia Administratora Bezpieczeństwa Informacji wymienione powyżej obowiązki pełni Administrator Danych Osobowych.

§6

Odpowiedzialność Administratora Systemów Informatycznych

1. Funkcję Administratora Systemów Informatycznych pełni osoba wyznaczona przez Administratora Danych Osobowych.
2. Do obowiązków Administratora Systemów Informatycznych/Informatyka należy:
   1) zabezpieczenie systemów przetwarzania danych osobowych;
   2) nadzór oraz zapewnianie ciągłości działania systemu informatycznego;
   3) reagowanie na przypadki naruszenia bądź powstania zagrożenia bezpieczeństwa danych osobowych;
   4) przeciwdziałanie próbom naruszenia bezpieczeństwa danych osobowych;
   5) zapewnienie zgodności wszystkich wdrażanych systemów przetwarzania danych osobowych z Ustawą oraz z niniejszą Polityką bezpieczeństwa i Instrukcją Zarządzania Systemem Informatycznym;
   6) instalację oraz konfigurację oprogramowania, sprzętu sieciowego i serwerowego używanego do przetwarzania danych osobowych;
   7) konfigurację i administrację oprogramowaniem systemowym i sieciowym zabezpieczającym dane osobowe przed nieupoważnionym dostępem;
   8) nadzór nad czynnościami związanymi ze sprawdzaniem systemu pod kątem obecności szkodliwego oprogramowania;
   9) nadzór nad systemem komunikacji w sieci komputerowej;
   10) nadzór nad naprawami, konserwacją oraz likwidacją urządzeń komputerowych, na których zapisane są dane osobowe;
   11) przyznawanie na wniosek Właściciela zasobów, za zgodą Administratora Danych Osobowych, ściśle określonych praw dostępu do danych osobowych w danym systemie;

12) świadczenie pomocy technicznej w ramach oprogramowania a także serwis sprzętu komputerowego będącego na stanie GOPS, służącego do przetwarzania danych osobowych;

13) diagnozowanie i usuwanie awarii sprzętu komputerowego;

14) wykonywanie i zarządzanie kopiami zapasowymi oprogramowania systemowego (w tym danych osobowych oraz zasobów umożliwiających ich przetwarzanie) i sieciowego;

15) nadzór nad wdrożeniem i zarządzanie systemami Informatycznymi (przeglądanie, nadawanie i odbieranie uprawnień użytkownikom, itp.), w których przetwarza się dane osobowe;

16) umożliwienie przeprowadzenia kontroli systemu informatycznego przez służby Biura Generalnego Inspektora Ochrony Danych Osobowych.

3. W przypadku niepowołania ASI, funkcję i jego zadania wykonuje informatyk Urzędu Gminy zgodnie z zakresem obowiązków.
4. Wsparcie techniczne w użytkowaniu i rozwoju programu do obsługi świadczeń rodzinnych, świadczenia wychowawczego, funduszu alimentacyjnego oraz świadczeń z pomocy społecznej świadczy firma, z którą Gminny Ośrodek Pomocy Społecznej w Książkach podpisuje umowę o opiekę nad systemem informatycznym. Projekt umowy jest przedkładany ASI/informatykowi do zapoznania się.

§7

Odpowiedzialność pracowników i użytkowników systemu

1. W celu zapewnienia wysokiego poziomu bezpieczeństwa danych osobowych konieczne jest zaangażowanie każdego pracownika w procesie ochrony danych osobowych.
2. Pracownicy odpowiedzialni są za bezpieczeństwo danych, do których mają dostęp zgodnie z przyznanymi upoważnieniami.
3. Do obowiązków pracowników należy:
   1) informowanie o wszelkich podejrzeniach naruszenia lub zauważonych naruszeniach Ustawy;
   2) postępowania zgodnie z przyjętą Polityką;
   3) zachowania w tajemnicy danych osobowych oraz informacji o sposobach ich zabezpieczenia. Przestrzeganie tajemnicy danych osobowych obowiązuje przez cały okres zatrudnienia u ADO, a także po ustaniu stosunku pracy lub odwołaniu z pełnionej funkcji;
   4) ochrony danych osobowych oraz środków przetwarzających dane osobowe przed nieuprawnionym dostępem, ujawnieniem, modyfikacją, zniszczeniem lub zniekształceniem;
   5) ścisłego przestrzegania zakresu nadanego upoważnienia do przetwarzania danych osobowych. Rozwiązanie stosunku pracy, odwołanie z pełnionej funkcji powoduje wygaśnięcie upoważnienia do przetwarzania danych osobowych;
   6) przestrzeganie procedur związanych z otwieraniem i zamykaniem pomieszczeń, w których przetwarzane są dane osobowe, a także z wejściem do tych obszarów osób nieupoważnionych;
   7) informowanie Administratora Danych lub Administratora Bezpieczeństwa Informacji o podejrzanych osobach.
4. W przypadku naruszenia przepisów lub zasad postępowania, osoba upoważniona do przetwarzania danych osobowych podlega odpowiedzialności służbowej i karnej. naruszenie zasad ochrony danych osobowych, a także sposobu ich zabezpieczenia, może skutkować postawieniem pracownikowi zarzutu popełnienia, jednego z przestępstw określonych w Rozdziale 8 Ustawy lub przestępstwa określonego w art. 266 Kodeksu Karnego.

5. Pracownicy przetwarzający dane osobowe, odpowiedzialni są za poinformowanie osób, których dane osobowe przetwarzają o:
   1) adresie siedziby GOPS w Książkach;
   2) celu zbierania danych;
   3) dobrowolności lub obowiązku podania danych, a jeżeli taki obowiązek istnieje, o jego podstawie prawnej;
   4) prawie wglądu do treści swoich danych oraz możliwości ich poprawienia.
6. W przypadku zbierania danych osobowych nie bezpośrednio od osoby, której one dotyczą, osobę tę należy dodatkowo poinformować o źródle danych oraz uprawnieniach wynikających z art. 32 ust. 1 pkt 7 i 8 Ustawy.

§ 8

Obszary przetwarzania danych osobowych

1. Obszar przetwarzania danych osobowych w Gminnym Ośrodku Pomocy Społecznej w Książkach obejmuje budynek, pomieszczenia i części pomieszczeń, w których przetwarzane są dane osobowe oraz miejsca, gdzie przechowuje się nośniki informacji zawierające dane osobowe.
2. Obszar przetwarzania danych osobowych określony jest w „Wykazie pomieszczeń, w których przetwarzane są dane osobowe", stanowiącym załącznik nr 3 do niniejszej polityki.
3. Budynki lub pomieszczenia, w których są przetwarzane dane osobowe winny być zamykane podczas nieobecności osób upoważnionych do przetwarzania danych osobowych w sposób ograniczający możliwość dostępu do nich osobom nieupoważnionym.

§ 9

Opis struktury zbiorów danych osobowych

1. Dane osobowe mogą być przetwarzane w zbiorach danych, przy zastosowaniu systemów informatycznych oraz zbiorów ewidencyjnych w postaci karotek, skorowidzów, wydruków, ksiąg i wykazów.
2. Zawartość pól informacyjnych występujących w systemach zastosowanych w celu przetwarzania danych osobowych musi być zgodna z przepisami prawa, które uprawniają lub zobowiązują Administratora Bezpieczeństwa Informacji do przetwarzania danych osobowych.
3. Administrator Systemów Informatycznych/Informatyk w oparciu o informacje uzyskane od Właścicieli zasobów danych osobowych, prowadzi – Ewidencję stosowanych systemów i programów (w tym licencji oprogramowania), zastosowanych do przetwarzania danych osobowych.
4. Opis struktury zbiorów danych osobowych przetwarzanych w systemach informatycznych prowadzi Administrator Systemów Informatycznych/Informatyk. Opis struktury zbiorów danych osobowych stanowi załącznik nr 4 do niniejszej Polityki.
5. Przepływ danych pomiędzy systemami zastosowanymi w celu przetwarzania danych osobowych może odbywać się w postaci przepływu jednokierunkowego lub przepływu dwukierunkowego.
6. Przepływ jednokierunkowy oznacza, że system informatyczny udostępnia dane ze zbioru (bazy) danych tylko w trybie „do odczytu".
7. Przepływ dwukierunkowy umożliwia upoważnionemu użytkownikowi korzystanie z danych w trybach do odczytu„ i „do zapisu", tj. umożliwia wprowadzanie nowych danych i modyfikację istniejących.

8. Przesyłanie danych pomiędzy systemami może odbywać się w sposób manualny, przy wykorzystaniu nośników zewnętrznych (np. płyta CD, DVD, dysk wymienny, PenDrive, itp.) lub w sposób półautomatyczny, przy wykorzystaniu funkcji eksportu/importu danych za pomocą teletransmisji (np. poprzez szyfrowaną sieć teleinformatyczną).

§ 10

Zarządzanie przetwarzaniem danych osobowych

1. Realizację zadań mających na celu zwiększenie skuteczności ochrony danych osobowych powinny zagwarantować następujące założenia:
   1) przeszkolenie pracowników dopuszczonych do przetwarzania danych w zakresie bezpieczeństwa danych osobowych;
   2) przypisanie użytkownikom określonych atrybutów pozwalających na ich identyfikację w systemach informatycznych (np. hasła, identyfikatory), umożliwiających im dostęp do danych osobowych – stosownie do zakresu upoważnienia i indywidualnych poziomów uprawnień;
   3) okresowe sprawdzanie przestrzegania przez użytkowników wdrożonych metod postępowania przy przetwarzaniu danych osobowych;
   4) podejmowanie niezbędnych działań, w celu likwidacji słabych ogniw w systemie ochrony danych osobowych;
   5) śledzenie osiągnięć w dziedzinie bezpieczeństwa fizycznego, bezpieczeństwa systemów informatycznych i w miarę możliwości organizacyjnych i techniczno – finansowych;
   6) wdrażanie nowych narzędzi i metod pracy oraz sposobów zarządzania, służących wzmocnieniu bezpieczeństwa przetwarzanych danych osobowych.
2. Na każdym etapie przetwarzania danych osobowych należy brać pod uwagę, w niezbędnym zakresie, integralność, poufność oraz rozliczalność dla przetwarzanych danych osobowych.
3. Administrator Danych powinien mieć pewność, że pracownicy oraz współpracownicy:
   1) są odpowiednio wprowadzani w swoje obowiązki i odpowiedzialności związane z ochroną danych osobowych i ich przetwarzaniem przed przyznaniem im dostępu do danych osobowych;
   2) otrzymali zalecenia określające wymagania w zakresie bezpieczeństwa danych osobowych związane z ich obowiązkami służbowymi;
   3) wypełniali zalecenia i warunki zatrudnienia, które uwzględniają zasady ochrony danych osobowych oraz właściwe metody pracy;
   4) w sposób ciągły utrzymywali odpowiednie umiejętności i kwalifikacje.
4. Za bieżącą, operacyjną ochronę danych osobowych odpowiada każda osoba, przetwarzająca te dane w zakresie zgodnym z zakresem upoważnienia, kompetencjami i rolą spowodowaną w procesie.

§11

Przetwarzanie danych osobowych

1. Pracownicy mają prawo do przetwarzania danych osobowych wyłącznie po uzyskaniu formalnego upoważnienia do przetwarzania danych osobowych, wystawionego przez ADO.
2. W tym celu ADO/ABI przed dopuszczeniem pracownika do pracy przy przetwarzaniu danych osobowych:

1) zapoznaje pracownika z przepisami dotyczącymi ochrony danych osobowych oraz uregulowaniami wewnętrznymi obowiązującymi w Gminnym Ośrodku Pomocy Społecznej w Książkach;

2) wystawia pracownikowi formalne upoważnienie do przetwarzania danych osobowych, zgodnie ze wzorem upoważnienia stanowiącym załącznik nr 5 do niniejszej Polityki;

3) przyjmuje od pracownika pisemne oświadczenie o zachowaniu poufności i tajemnicy służbowej, zgodnie ze wzorem oświadczenia stanowiącym załącznik nr 6 do niniejszej Polityki.

3. Osoby upoważnione do przetwarzania danych osobowych wpisane są do ewidencji. Ewidencja osób upoważnionych do przetwarzania danych osobowych powinna być prowadzona przez ABI, zgodnie ze wzorem stanowiącym załącznik nr 7 do niniejszej Polityki.
4. Ewidencja osób upoważnionych do przetwarzania danych osobowych winna być przechowywana w szafie zamykanej, do której dostęp ma ADO/ABI.

§12

Rejestr zbiorów danych osobowych

1. Pracownik jest zobowiązany zgłosić ABI zamiar utworzenia nowego zbioru danych osobowych wraz ze wskazaniem podstawy przetwarzania danych, uzasadnieniem celowości, zakresu i sposobu zbierania danych osobowych.
2. ABI przygotowuje projekt zgłoszenia zbioru danych osobowych do rejestracji GIODO, jeżeli takie zgłoszenie jest ustawowo wymagane.
3. ABI sprawdza opisane w zgłoszeniu rejestracyjnym warunki techniczne i organizacyjne dotyczące zabezpieczeń w systemie informatycznym. W przypadku niewystarczającego poziomu zabezpieczeń występuje z wnioskiem do ASI/Informatyka o podniesienie poziomu zabezpieczeń.
4. Sprawdzony przez ABI projekt zgłoszenia zbioru danych osobowych do rejestracji GIODO jest przedstawiany ADO do podpisu. Po akceptacji Administratora Danych Osobowych ABI zgłasza wniosek o rejestrację zbioru danych osobowych do GIODO i wyznacza Właściciela zasobów danych osobowych dla zarejestrowanego zbioru.
5. Z obowiązku rejestracji zbiorów danych osobowych do GIODO zwolnione są zbiory zawierające dane przetwarzane w zborach, które nie są prowadzone z wykorzystaniem systemów informatycznych, z wyjątkiem zbiorów zawierających dane, o których mowa w art. 27 ust. 1 ustawy.

§13

Udostępniania danych osobowych

1. Dane osobowe mogą być udostępniane podmiotom uprawnionym do ich otrzymania na mocy przepisów prawa.
2. Dane osobowe mogą być udostępniane w następujących przypadkach:
   1) na podstawie wniosku od podmiotu uprawnionego do otrzymywania danych osobowych na podstawie przepisów;
   2) na podstawie umowy z innym podmiotem, w ramach które istnieje konieczność udostępnienia danych;
   3) na podstawie wniosku osoby, które dane dotyczą.

3. Wniosek o udostępnienie danych osobowych musi być złożony wyłącznie w formie pisemnej. Powinien zawierać informacje umożliwiające wyszukanie żądanych danych osobowych w zbiorze oraz wskazywać ich zakres i przeznaczenie.
4. Udostępniając dane osobowe należy zaznaczyć, ze można je wykorzystać wyłącznie zgodnie z przeznaczeniem, dla którego zostały udostępnione.
5. Na pisemny wniosek pochodzący od osoby, której dane dotyczą, informacje o osobie powinny być udzielone w terminie 30 dni od daty złożenia wniosku.
6. Za przygotowanie danych osobowych do udostępnienia w zakresie wskazanym we wniosku jest odpowiedzialny Właściciel zasobów danych osobowych.
7. Odpowiedź na wniosek o udostępnienia danych osobowych przed wysłaniem jest akceptowana przez Właściciela zasobów danych osobowych oraz Administratora Bezpieczeństwa informacji, a następnie podpisywana przez Administratora Danych Osobowych.
8. Odmowa udostępnienia danych osobowych następuje gdy brak jest podstawy prawnej do udostępnienia tych danych.

§14

Powierzanie danych osobowych

1. Powierzenie przetwarzania danych osobowych występuje wówczas, gdy podmioty zewnętrzne współpracujące z Gminnym Ośrodkiem Pomocy Społecznej w Książkach mają dostęp do danych osobowych przetwarzanych w Gminnym Ośrodku Pomocy Społecznej w Książkach.
2. Powierzenie może mieć miejsce wyłącznie w trybie przewidzianym zapisami art. 31 Ustawy poprzez podpisanie stosownej pisemnej umowy powierzenia pomiędzy Administratorem Danych Osobowych a podmiotem, któremu powierzono przetwarzanie danych osobowych.

§15

Postępowanie w przypadku naruszenia bezpieczeństwa ochrony danych osobowych

1. Zasady postępowania w przypadku naruszenia bezpieczeństwa danych osobowych obowiązują wszystkie osoby biorące udział w procesie przetwarzania danych osobowych.
2. Naruszeniem zasad bezpieczeństwa danych osobowych jest każdy stwierdzony fakt nieuprawnionego ujawnienia danych osobowych, udostępnienia lub umożliwienia dostępu do nich osobom nieupoważnionym, zabrania danych przez osobę nieupoważnioną, uszkodzenia jakiegokolwiek elementu systemu informatycznego.
3. W przypadku stwierdzenia naruszenia zabezpieczenia systemu informatycznego lub zaistnienia sytuacji, które mogą wskazać na naruszenie bezpieczeństwa danych osobowych, każdy pracownik zatrudniony przy przetwarzaniu danych osobowych jest zobowiązany przerwać przetwarzanie danych osobowych i powiadomić o tym fakcie bezpośredniego przełożonego lub ABI i postępować zgodnie z podjętą decyzją.
4. Zgłoszenie naruszenia ochrony danych osobowych powinno zawierać:
   1) opisanie działania wskazującego na naruszenie ochrony danych osobowych;
   2) określenie sytuacji i czasu, w jakim stwierdzono naruszenie ochrony danych osobowych;
   3) wskazanie istotnych informacji mogących mieć wpływ na przyczynę naruszenia;
   4) określenie znanych danej osobie sposobów zabezpieczenia systemu oraz wszelkich kroków podjętych po ujawnieniu zdarzenia.

5. W przypadku naruszenia przepisów lub zasad postępowania, osoba upoważniona do przetwarzania danych osobowych podlega odpowiedzialności służbowej i karnej.

§16

Postanowienia końcowe

W sprawach nieuregulowanych w Polityce maja zastosowanie przepisy Ustawy z dnia 29 sierpnia 1997 r. o ochronie danych osobowych oraz przepisy wykonawcze tej ustawy.