Załącznik nr 1 do Zarządzenia nr 18/2015
Dyrektora PCPR w Zgierzu z dnia 22 lipca 2015 r.

POLITYKA BEZPIECZEŃSTWA INFORMACJI W ZAKRESIE PRZETWARZANIA DANYCH OSOBOWYCH W POWIATOWYM CENTRUM POMOCY RODZINIE

Spis treści

I. Podstawa prawna

§1.

Dokumenty: Polityka bezpieczeństwa informacji w zakresie przetwarzania danych osobowych oraz Instrukcja Zarządzania Systemem Informatycznym Powiatowego Centrum Pomocy Rodzinie w Zgierzu służą do przetwarzania danych osobowych i zostały opracowane na podstawie niniejszych aktów prawnych:

1) konstytucji Rzeczypospolitej Polskiej z dnia 2 kwietnia 1997 r.
2) ustawy z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (tekst jednolity Dz. U. 2014 r. poz. 1182 z późn. zm).
3) rozporządzenia Ministra Spraw Wewnętrznych i Administracji z dnia 29 kwietnia 2004r. w sprawie dokumentacji przetwarzania danych osobowych oraz warunków technicznych i organizacyjnych, jakimi powinny odpowiadać urządzenia i systemy informatyczne służące do przetwarzania danych osobowych (Dz. U. Nr 100, poz. 1024).
4) rozporządzenie Rady Ministrów z dnia 12 kwietnia 2012 r. w sprawie Krajowych Ram Interoperacyjności, minimalnych wymagań dla rejestrów publicznych i wymiany informacji w postaci elektronicznej oraz minimalnych wymagań dla systemów teleinformatycznych (Dz. U. 2012 r. poz. 526).
5) rozporządzenie Ministra Administracji i Cyfryzacji z dnia 11 maja 2015 r. w sprawie sposobu prowadzenia przez administratora bezpieczeństwa informacji rejestru zbiorów danych (Dz. U. 2015 r. poz. 719).
6) rozporządzenie Ministra Administracji i Cyfryzacji z dnia 11 maja 2015 r. w sprawie trybu i sposobu realizacji zadań w celu zapewnienia przestrzegania przepisów o ochronie danych osobowych przez administratora bezpieczeństwa informacji (Dz. U. 2015 r. poz. 745).

II. Postanowienia ogóle

§2.

1. Celem opracowania i wdrożenia polityki bezpieczeństwa jest określenie podstawowych zasad dotyczących bezpiecznego przetwarzania dokumentacji zawierających dane osobowe, zarówno w formie papierowej jak i elektronicznej, nie naruszając zasad określonych w ustawie o ochronie danych osobowych.

2. Polityka bezpieczeństwa została opracowana dla potrzeb Powiatowego Centrum Pomocy Rodzinie w Zgierzu i obowiązuje wszystkie osoby oraz firmy zewnętrzne, mające bezpośredni jak i pośredni dostęp do informacji zawierających dane osobowe, które są zbierane, przetwarzane i przechowywane w siedzibie PCPR w Zgierzu.

3. Dostęp do przetwarzania danych osobowych maja wyłącznie osoby, które posiadają upoważnienie wydane przez Administratora danych osobowych oraz zostały odpowiednio przeszkolone i poinformowane o sposobie przetwarzania danych osobowych. Są one zobowiązane do zachowania tajemnicy zarówno w kwestii danych osobowych jak i sposobach zabezpieczeń użytych do ich ochrony.

4. Niniejszy dokument ma na celu uświadomienie osobom pracującym z danymi osobowymi o odpowiedzialności i konsekwencjach nie przestrzegania zasad wynikających z ustawy o ochronie danych osobowych, które mogą prowadzić do utraty tych danych na rzecz osób nieuprawnionych.

5. Zastosowane w polityce bezpieczeństwa zabezpieczenia mają przede wszystkim zapewnić:
   1) ***poufność informacji*** – rozumianą jako zapewnienie, że tylko uprawnieni pracownicy mają dostęp do informacji;
   2) ***integralność informacji*** – rozumianą jako zapewnienie dokładności i kompletności informacji oraz metod jej przetwarzania;

3) ***dostępność informacji*** – rozumianą jako zapewnienie, że osoby upoważnione mają dostęp do informacji i związanych z nią zasobów wtedy, gdy jest to potrzebne;
4) ***zarządzanie ryzykiem*** – rozumiane jako proces identyfikowania, kontrolowania i minimalizowania lub eliminowania ryzyka dotyczącego bezpieczeństwa, które może dotyczyć systemów informacyjnych.

6. Ochrona danych osobowych w Powiatowym Centrum Pomocy Rodzinie w Zgierzu realizowana jest w oparciu o zabezpieczenia fizyczne – stosowanie narzędzi uniemożliwiającym dostęp do danych osobowych osobom nieuprawnionym, programowe – stosowanie autoryzacji użytkowników pracujących z danymi osobowymi oraz przez pożądane zachowanie użytkowników.

7. Do stosowania zasad określonych przez dokumenty polityki bezpieczeństwa zobowiązani są wszyscy użytkownicy, w tym pracownicy w rozumieniu Kodeksu pracy, a także konsultanci, stażyści oraz inne osoby mające dostęp do informacji podlegających ochronie.

8. W Powiatowym Centrum Pomocy Rodzinie w Zgierzu polityka bezpieczeństwa stosowana jest w szczególności do:
   1) danych osobowych przetwarzanych w systemie POMOST,
   2) danych osobowych przetwarzanych w systemie TYLDA,
   3) danych osobowych przetwarzanych w systemie PŁATNIK,
   4) danych osobowych przetwarzanych w systemie PŁACE Firmy ProLogika,
   5) danych osobowych przetwarzanych w systemie FK ARISCO,
   6) wszystkich informacji dotyczących danych pracowników PCPR w Zgierzu, w tym danych osobowych personelu i treści zawieranych umów o pracę,
   7) wszystkich danych zbieranych i przetwarzanych w procesie rekrutacji,
   8) informacji dotyczących zabezpieczenia danych osobowych, w tym w szczególności nazw kont i haseł w systemach przetwarzania danych osobowych,
   9) rejestru osób dopuszczonych do przetwarzania danych osobowych,
   10) innych dokumentów zawierających dane osobowe.

III. Definicje

§3.

Określenia użyte w dalszej części tego opracowania odpowiednio oznaczają:

1. ***Ustawa*** – ustawa z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (Dz. U. z 2014 r. poz. 1182).

2. ***Powiatowe Centrum Pomocy Rodzinie w Zgierzu*** – PCPR w Zgierzu

3. ***Generalnym Inspektorze Ochrony Danych Osobowych***, zwanym dalej „GIODO" – należy przez to rozumieć organ do spraw ochrony danych osobowych.

4. ***Dane osobowe*** – wszelkie informacje dotyczące zidentyfikowanej lub możliwej do zidentyfikowania osoby fizycznej zgodnie z art. 6 ustawy. Osobą do zidentyfikowania jest osoba, której tożsamość można określić bezpośrednio lub pośrednio, w szczególności przez powołanie się na numer identyfikacyjny, jeden lub kilka specyficznych czynników określających jej cechy. Do danych osobowych zalicza się więc nie tylko imię, nazwisko i adres, ale również przypisane jej numery, dane o cechach fizjologicznych, umysłowych, ekonomicznych, kulturowych i społecznych.

5. ***Zbiór danych osobowych*** – każdy zbiór posiadający strukturę o charakterze osobowym, dostępny według określonych kryteriów, niezależnie od tego, czy jest rozproszony czy też podzielony funkcjonalnie.

6. ***Dane wrażliwe*** – dane o pochodzeniu rasowym lub etnicznym, poglądach politycznych, przekonaniach religijnych lub filozoficznych, przynależności wyznaniowej, partyjnej lub związkowej, jak również danych o stanie zdrowia, kodzie genetycznym, nałogach lub życiu seksualnym oraz danych dotyczących

skazań, orzeczeń o ukaraniu i mandatów karnych, a także innych orzeczeń wydanych w postępowaniu sądowym lub administracyjnym.

7. ***Przetwarzanie danych osobowych*** – wszystkie czynności jakie będą wykonywane na zgromadzonych danych osobowych, między innymi: przetwarzanie, przechowywanie, przekazywanie, czy usuwanie.

8. ***Polityka bezpieczeństwa*** – zbiór jednoznacznych, spójnych zgodnych z obowiązującym prawem przepisów, zasad i reguł postępowania z dokumentacją papierową jak i elektroniczną zawierającą dane osobowe.

9. ***Administrator Danych Osobowych*** zwany nalej „**ADO**" – to organ, jednostka organizacyjna, podmiot lub osoba, o których mowa w art. 3 ustawy, decydująca o celach i środkach przetwarzania danych osobowych. Administratorem Danych Osobowych w Powiatowym Centrum Pomocy Rodzinie w Zgierzu jest Dyrektor jednostki.

10. ***Administrator Bezpieczeństwa Informacji*** zwany dalej „**ABI**" – osoba powołana przez ADO do nadzorowania i kontrolowania poprawności przetwarzania informacji, zawierających dane osobowe.

11. ***Administrator Systemu Informatycznego*** zwany dalej „**ASI**" – osoba odpowiedzialna za wdrażanie technicznych zabezpieczeń służących do ochrony zbieranych, przetwarzanych i przechowywanych danych osobowych.

12. ***System informatyczny*** – jest to zbiór powiązanych ze sobą elementów, którego funkcją jest przetwarzanie danych przy użyciu techniki komputerowej. System informatyczny stanowi zarówno sprzęt jak i oprogramowanie.

13. ***Użytkownik systemu*** – osoba posiadająca uprawnienia umożliwiające działanie w systemie informatycznym.

14. ***Osoba upoważniona*** – osoba posiadająca odpowiednie upoważnienie wydane przez ADO lub ABI, działającego w imieniu ADO do przetwarzania danych osobowych w systemie informatycznym.

15. ***Stacja robocza*** – komputer wchodzący w skład systemu informatycznego na którym osoba upoważniona może przetwarzać dane osobowe.

16. ***Zabezpieczenie systemu informatycznego*** – zespół narzędzi oraz odpowiednich konfiguracji poszczególnych elementów systemu informatycznego zabezpieczających go przed nieuprawnionym dostępem, dającym możliwość modyfikacji, zniszczenia lub pozyskania jakichkolwiek informacji zawierających dane osobowe.

IV. Rejestracja zbiorów danych

§4.

1. Obowiązek rejestracji zbiorów jest jednym z podstawowych obowiązków, jakie nakłada na ADO ustawa o ochronie danych osobowych.
2. Zgodnie z art. 40 ustawy ADO jest zobowiązany zgłosić zbiór danych osobowych do rejestracji, której dokonuje GIODO w celu przetwarzania tych danych, z wyjątkiem zbiorów które z mocy ustawy o ochronie danych osobowych nie podlegają obowiązkowi rejestracji.
3. Zgodnie z art. 43, ust. 1a ustawy o ochronie danych osobowych Administrator danych osobowych powołał ABI i zgłosił go Generalnemu Inspektorowi Danych Osobowych do rejestracji, w związku z czym ADO nie podlega obowiązkowi rejestracji do GIODO zbiorów danych osobowych wykorzystywanych w Powiatowym Centrum Pomocy Rodzinie w Zgierzu, z wyjątkiem zbiorów danych osobowych zawierających informacje o których mowa w art. 27 ust. 1 ustawy tj. zbiorów danych osobowych zawierających dane wrażliwe.
4. ABI prowadzi w PCPR w Zgierzu jawny rejestr zbiorów danych osobowych przetwarzanych przez administratora danych, z wyjątkiem zbiorów o których mowa w art. 43 ust. 1, zawierającego nazwy zbioru oraz informacje, o których mowa w art. 41 ust. 1 pkt 2-4a i 7
5. Administrator bezpieczeństwa informacji w ramach prowadzenia rejestru
   1) wpisuję zbiór danych do rejestru przed rozpoczęciem przetwarzania w zbiorze danych;
   2) aktualizuje informacje dotyczące zbioru danych w rejestrze – w przypadku zmiany informacji objętych wpisem;
   3) wykreśla zbiór danych z rejestru – w przypadku zaprzestania przetwarzania w nim danych osobowych;
   4) udostępnia rejestr do przeglądania.

V. Zakres Polityki bezpieczeństwa

§5.

1. W systemie informatycznym Powiatowego Centrum Pomocy Rodzinie w Zgierzu przetwarzane są informacje służące do wykonywania zadań z zakresu pomocy społecznej.
2. Dane osobowe zbierane są w celu:
   1) realizacji zadań określonych postanowieniami ustaw wymienionych w §2 Regulaminu Organizacyjnego Powiatowego Centrum Pomocy Rodzinie w Zgierzu i aktów wykonawczych wydanych do tych ustaw,
   2) przygotowywań sprawozdań finansowych,
   3) zatrudnienia, świadczenia usług na podstawie umów cywilno – prawnych.
3. Informacje te są przetwarzane i składowane zarówno w postaci papierowej (w kartotekach, zbiorach, wykazach, księgach i innych zbiorach ewidencyjnych) jak i elektronicznej przetwarzanej w systemach informatycznych, także w przypadku przetwarzania poza zbiorem danych.

§6.

Zakresy określone przez dokumenty Polityki Bezpieczeństwa Informacji mają zastosowanie do całego systemu informatycznego PCPR w Zgierzu, w szczególności do:

1) wszystkich istniejących, wdrażanych obecnie lub w przyszłości systemów informatycznych oraz papierowych, w których przetwarzane są informacje podlegające ochronie;
2) informacji będących własnością PCPR w Zgierzu, które zostały nagromadzone przez cały okres funkcjonowania podmiotu;
3) wszystkich lokalizacji – budynków i pomieszczeń, w których są lub będą przetwarzane informacje podlegające ochronie.

§7.

Informacje niejawne nie są objęte zakresem Polityki Bezpieczeństwa.

VI. Zadania i obowiązki ADO, ABI, ASI

§8.

1. Osobą odpowiedzialną za ochronę danych osobowych przetwarzanych w Powiatowym Centrum Pomocy Rodzinie w Zgierzu jest ADO. Zgodnie z ustawa jest nim Dyrektor PCPR w Zgierzu.
2. Do obowiązków ADO należy przede wszystkim:
   1) wydawanie upoważnień do przetwarzania danych osobowych,
   2) przetwarzanie danych zgodnie z prawem i wymogami ustawy,
   3) zabezpieczenie przetwarzanych danych osobowych przed ich ujawnieniem, przejęciem oraz usunięciem przez osoby do tego nieupoważnione,
   4) ochrona danych osobowych przed ich przypadkowym zmodyfikowaniem, upublicznieniem lub skasowaniem,
   5) decyzja o celach i środkach przetwarzania danych osobowych,
   6) inne czynności mające na celu ochronę i zabezpieczenie danych osobowych.

§9.

1. ADO do celów ochrony danych osobowych przetwarzanych w Powiatowym Centrum Pomocy Rodzinie w Zgierzu wyznacza ABI – którym jest Pan Adrian Oszajca.
2. Do obowiązków ABI należą przede wszystkim:
   1) przygotowanie i aktualizowanie Polityki Bezpieczeństwa i Instrukcję Zarządzania Systemem Informatycznym w zakresie przetwarzania danych osobowych zgodnie z wymogami ustawy oraz obowiązujących rozporządzeń Ministra Spraw Wewnętrznych i Administracji dotyczących dokumentacji przetwarzania danych osobowych oraz warunków technicznych i organizacyjnych, jakim powinny odpowiadać urządzenia i systemy informatyczne służące do przetwarzania danych osobowych;
   2) nadzoruje przestrzeganie zasad ochrony, przetwarzania danych osobowym zgodnie z wymogami zawartymi w Polityce Bezpieczeństwa oraz Instrukcji

Zarządzania Systemem Informatycznym w zakresie przetwarzania danych osobowych;

3) nadaje oraz odbiera uprawnienia dostępu do systemu informatycznego poszczególnym użytkownikom, którzy maja dostęp do przetwarzania danych osobowych;
4) prowadzi ewidencje osób upoważnionych do przetwarzania danych osobowych;
5) prowadzi publiczny rejestr zbiorów danych, w którym przetwarzane są dane osobowe oraz zgłasza rejestry zawierające informację szczególnie chronione w myśl art. 27 ust. 1 ustawy do GIODO;
6) prowadzi wykaz pomieszczeń w których przetwarzane są dane osobowe;
7) interweniuje w przypadku naruszenia zasad ochrony danych osobowych.

3. ABI ma prawo:
   1) wstępu do pomieszczeń, w których zlokalizowane są zbiory danych osobowych i przeprowadzenia niezbędnych badań lub innych czynności kontrolnych w celu oceny zgodności przetwarzania danych z ustawą;
   2) żądać od pracowników Powiatowego Centrum Pomocy Rodzinie w Zgierzu złożenia pisemnych lub ustnych wyjaśnień w przypadku podejrzenia pojawienia się nieprawidłowości w przetwarzaniu danych osobowych;
   3) żądać okazania dokumentów i wszelkich danych mających bezpośredni związek z zakresem kontroli;
   4) żądać udostępnienia do kontroli urządzeń, nośników oraz systemów informatycznych służących do przetwarzania danych osobowych.

§10.

1. ADO powierza obowiązek technicznego zabezpieczenia systemu informatycznego przed nieuprawnionym dostępem do danych osobowych Administratorowi Systemu Informatycznemu, którym w PCPR w Zgierzu jest Pan Rafał Kuczyński.
2. Do głównych zadania ASI należą:

1) konfiguracja zabezpieczeń systemu informatycznego przeciwdziałająca nieuprawnionym dostępom do danych osobowych osobom nieupoważnionym;
2) nadawanie/odbieranie praw dostępu do systemu informatycznego użytkownikom przetwarzającym dane osobowe z uwzględnieniem informacji przekazanych od ABI;
3) odpowiednie reagowania w przypadku wykrycia nieprawidłowości w przetwarzaniu danych osobowych polegające na powstrzymaniu dalszego nieprawidłowego procederu oraz niezwłoczne zgłoszenie zaistniałej sytuacji do ABI i Dyrektora jednostki;
4) prawidłowe, nadzorowane usuwanie/kasowanie informacji, zawierających dane osobowe z urządzeń przekazanych do likwidacji;
5) nadzorowanie i zabezpieczanie kopii bezpieczeństwa a w szczególności miejsca ich przechowywania, zawierających dane osobowe przed przejęciem przez osoby nieuprawnione.

§11.

Obowiązki użytkownika systemu informatycznego:

1. Ochrona danych do logowania do systemu informatycznego, w którym przetwarzane są dane osobowe przed osobami nieuprawnionymi oraz niezwłoczne zgłaszanie ich ASI w przypadku pojawienia się podejrzenia o ich przejęciu przez osoby trzecie.
2. Nieudostępnianie osobistych danych do logowania innym użytkownikom systemu informatycznego.
3. Blokowanie komputera po odejściu od stanowiska pracy.
4. Niepozostawianie danych zawierających dane osobowe bez opieki w przypadku odejścia od biurka.
5. Przetwarzanie danych osobowych w miejscach do tego wyznaczonych czyli wskazanych w rejestrze miejsc służących do przetwarzania danych osobowych.
6. Zabezpieczanie danych osobowych po zakończeniu ich przetwarzania, nie pozostawiania ich na stanowisku pracy bez opieki i nadzoru.

7. Zgłaszanie wszelkich podejrzeń i nieprawidłowości związanych z zabezpieczeniem użytkowanego komputera, będącego częścią systemu informatycznego, służącego do przetwarzania danych osobowych, mogących mieć wpływ na bezprawne działanie osób trzecich, dążące do utraty ochrony i bezpieczeństwa przetwarzanych danych osobowych.

VII. Upoważnienia do przetwarzania danych osobowych

§12.

Pracownicy Powiatowego Centrum Pomocy Rodzinie w Zgierzu w celu uzyskania dostępu do przetwarzania danych osobowych występują za pośrednictwem ABI do ADO z wnioskiem (**wg wzoru stanowiącego załącznik nr 2 do niniejszego regulaminu**) o wydanie upoważnienia dla osoby przetwarzającej dane osobowe

§13.

Niniejszy wniosek powinien zostać złożony przed rozpoczęciem pracy na danych osobowych przez osobę zatrudnioną. We wniosku należy wskazać nazwę zbiorów danych ze wskazaniem sposobu ich przetwarzania.

§14.

Po uzyskaniu opinii Administratora Bezpieczeństwa Informacji, Administrator Danych Osobowych wydaje upoważnienie do przetwarzania danych osobowych dla pracownika Powiatowego Centrum Pomocy Rodzinie w Zgierzu **wg wzoru stanowiącego załącznik nr 3** do niniejszego regulaminu.

VIII. Udostępnianie oraz powierzenie obowiązku przetwarzania danych osobowych

§15.

Najważniejsze przesłanki i zasady udostępniania danych:

1) nie jest istotne czy udostępnianie danych ma charakter odpłatny czy nie, aby czynność była uznana za udostępnianie;
2) nie ma znaczenia (ujmując problem technicznie) czy udostępnianie następuje w formie przekazu ustnego, pisemnego, za pomocą powszechnych środków przekazu lub poprzez sieć komputerową itd.;
3) udostępnianie danych osobowych osobom lub podmiotom uprawnionym do ich otrzymania odbywa się na mocy przepisów prawa;
4) dane osobowe z wyłączeniem danych wrażliwych mogą być udostępniane w oparciu o przepisy prawa, jeżeli osoba wnioskująca w sposób wiarygodny uzasadni potrzebę posiadania tych danych, a ich udostępnienie nie naruszy praw i wolności osób których dane dotyczą;
5) dane osobowe udostępnia się na pisemny, umotywowany wniosek, chyba że przepis innej ustawy stanowi inaczej. Wniosek powinien zawierać informacje umożliwiające wyszukanie w zbiorze żądanych danych osobowych oraz wskazać ich zakres i przeznaczenie;
6) udostępnione dane osobowe można wykorzystać wyłącznie zgodnie z przeznaczeniem, dla którego zostały udostępnione.

§16.

W przypadku konieczności przetwarzania danych osobowych przez odrębne podmioty świadczące usługi dla ADO może on powierzyć ich przetwarzanie, w drodze umowy zawartej na piśmie, pod następującymi warunkami:

1) pisemna umowa powinna być zawarta niezależnie od posiadanej umowy określającej relacje obu stron;
2) podmiot, któremu powierzono przetwarzanie danych, może przetwarzać je wyłącznie w zakresie i celu przewidzianych w umowie;

3) podmiot, któremu powierzono przetwarzanie danych, jest obowiązany przed rozpoczęciem przetwarzania danych podjąć środki zabezpieczające zbiór danych, o których mowa w art. 36-39 ustawy;
4) W zakresie przestrzegania tych przepisów podmiot ponosi odpowiedzialność jak administrator danych;
5) Odpowiedzialność za przestrzeganie przepisów ustawy o ochronie danych osobowych spoczywa na Administratorze danych osobowych, co nie wyłącza odpowiedzialności podmiotu, który zawarł umowę, za przetwarzanie danych niezgodne z tą umową.

IX. Środki organizacyjne i techniczne zastosowane do ochrony i nadzoru przetwarzanych danych osobowych

§17.

W celu stworzenia właściwych zabezpieczeń, które powinny bezpośrednio oddziaływać na procesy przetwarzania danych wprowadza się następujące środki organizacyjne:

1) przetwarzanie danych osobowych w Powiatowym Centrum Pomocy Rodzinie w Zgierzu może odbywać się wyłącznie w ramach wykonywania zadań służbowych, zakres uprawnień wynika z zakresu tych zadań;
2) do przetwarzania danych mogą być dopuszczone wyłącznie osoby posiadające stosowne upoważnienie;
3) unieważnienie upoważnienia następuje na piśmie, wg wzoru stanowiącego **załącznik nr 4** do niniejszej dokumentacji;
4) dostęp do budynków, pomieszczeń jak i do urządzeń przetwarzających dane osobowe powinny mieć wyłącznie osoby uprawnione do tego;
5) dane osobowe powinny być wyłącznie przetwarzane w budynkach, pomieszczeniach Powiatowego Centrum Pomocy Rodzinie w Zgierzu do tego przystosowanych i zabezpieczonych, przez osoby upoważnione przez Administratora danych osobowych – **wg załącznika nr 5** do niniejszego dokumentu;
6) zbiory danych osobowych (bazy danych) w których dokonuje się przetwarzania danych osobowych powinny być zabezpieczone przed nieuprawnionym dostępem i zewidencjonowane w rejestrze zbiorów danych osobowych, który prowadzi ABI **wg załącznika nr 6** do niniejszego dokumentu;
7) każdy pracownik Powiatowego Centrum Pomocy Rodzinie w Zgierzu co najmniej raz na dwa lata musi odbyć szkolenie z zakresu ochrony danych osobowych. Fakt uczestnictwa w szkoleniu pracownik potwierdza pisemnie na liście obecności uczestników szkolenia;

8) nowo przyjęty pracownik Powiatowego Centrum Pomocy Rodzinie w Zgierzu obowiązkowo odbywa szkolenie przed przystąpieniem do przetwarzania danych;
9) każdy upoważniony do przetwarzania danych osobowych w Powiatowym Centrum Pomocy Rodzinie w Zgierzu potwierdza pisemnie fakt zapoznania się z niniejszą dokumentacją i zrozumieniem wszystkich zasad bezpieczeństwa wg wzoru stanowiącego **załącznik nr 1** do niniejszej dokumentacji. Podpisany dokument jest dołączany do akt osobowych;
10) obszar przetwarzania danych osobowych określony w **załączniku nr 5** do niniejszego regulaminu zabezpiecza się przed dostępem osób nieuprawnionych na czas nieobecności w nim osób upoważnionych do przetwarzania danych osobowych;
11) przebywanie osób nieuprawnionych w w/w obszarze jest dopuszczalne za zgodą Administratora danych osobowych lub w obecności osoby upoważnionej do przetwarzania danych osobowych;
12) pomieszczenia stanowiące obszar przetwarzania danych powinny być zamykane na klucz;
13) monitory komputerów na których przetwarzane są dane osobowe ustawione są w sposób uniemożliwiający wgląd osobom postronnym w przetwarzane dane;
14) przed opuszczeniem pomieszczenia stanowiącego obszar przetwarzania danych należy zamknąć okna oraz usunąć z biurka wszystkie dokumenty i nośniki informacji oraz umieścić je w odpowiednich zamykanych szafach lub biurkach.

§18.

Zbiory danych osobowych przetwarzane w Powiatowym Centrum Pomocy Rodzinie w Zgierzu zabezpieczone są poprzez:

1. Środki ochrony fizycznej:
   1) zbiory danych osobowych przechowywane są w pomieszczeniach zabezpieczonych przed swobodnym dostępem;
   2) zbiory danych osobowych w formie papierowej przechowywane są w szafach zamykanych na klucz;

3) archiwalne zbiory danych osobowych przechowywane są szafie zamykanej na klucz, a dostęp do niego mają wyłącznie upoważnione osoby na podstawie wydanego upoważnienia przez Administratora Danych;
4) kopie bezpieczeństwa (kopie zapasowe) przechowuje się miejscach zabezpieczonych przed nieuprawnionym przejęciem, modyfikacją uszkodzeniem lub zniszczeniem;
5) kopie bezpieczeństwa (kopie zapasowe) zbiorów danych osobowych na nośnikach danych (dysk zewnętrzny) przechowywane są w zamkniętym na klucz szafach metalowych, a dostęp do niego mają wyłącznie upoważnione osoby na podstawie wydanego upoważnienia przez ADO;
6) pomieszczenia w których przetwarzane są zbiory danych osobowych zabezpieczone są przed skutkami pożaru za pomocą wolnostojącej gaśnicy;
7) dokumenty zawierające dane osobowe o ustaniu przydatności są niszczone w sposób mechaniczny za pomocą niszczarek dokumentów. Po zniszczeniu dokumentów spisuję się protokół zniszczenia.

2. Środki sprzętowe, infrastruktury informatycznej i telekomunikacyjnej stosowane w PCPR w Zgierzu:
   1) zbiory danych osobowych przetwarzane są przy użyciu komputerów stacjonarnych jak i przenośnych;
   2) bezwzględny zakaz podłączania prywatnych komputerów i innych urządzeń do infrastruktury teleinformatycznej w pomieszczeniach PCPR w Zgierzu;
   3) bezwzględny zakaz przenoszenia, wynoszenia danych na nośnikach zewnętrznych, zawierające dane osobowe poza obszar możliwości ich przetwarzania;
   4) dostęp do systemu operacyjnego, w którym przetwarzane są dane osobowe na prawach administratora posiada wyłącznie ASI. Dostęp zabezpieczony jest za pomocą procesu uwierzytelniania z wykorzystaniem identyfikatora oraz hasła;
   5) zastosowano środki ochrony przed szkodliwym oprogramowaniem i spamem – oprogramowanie antywirusowe;
   6) użyto system firewall stanowiący element programu antywirusowego do ochrony dostępu do sieci komputerowej;

7) dostęp do urządzeń aktywnych sieci LAN (np. przełączniki sieciowe, routery) ma wyłącznie ASI;
8) ruch między siecią LAN a WAN jest monitorowany;
9) dostęp do sieci LAN mają wyłącznie komputery, które uzyskały zgodę na prace w sieci teleinformatycznej wydaną przez „ABI" oraz „ASI".

3. Środki ochrony w ramach systemowych narzędzi programowych i baz danych stosowanych w PCPR w Zgierzu:
   1) dostęp do zbiorów danych osobowych wymaga uwierzytelnienia z wykorzystaniem spersonalizowanego, unikatowego identyfikatora użytkownika systemu informatycznego oraz hasła użytkownika;
   2) identyfikator użytkownika który utracił dostęp do danych osobowych nie może być przydzielony innej osobie;
   3) zastosowano systemowe środki pozwalające na określenie odpowiednich praw dostępu do zasobów informatycznych, w tym zbiorów danych osobowych dla poszczególnych użytkowników systemu Informatycznego;
   4) ASI sporządza okresowo (tygodniowo) kopie zapasowe baz danych osobowych gromadzonych na serwerze ze wszystkich wykorzystywanych systemów informatycznych, programów, żeby zabezpieczyć się przed utrata danych spowodowaną awarią sprzętu komputerowego itp.;
   5) należy zabezpieczyć komputery, serwery przed skutkami awarii bądź niestabilnego napięcia z sieci elektrycznej poprzez podłączenie każdego komputera, serwera do zasilacza UPS;
   6) zmiana haseł dostępowych ASI oraz użytkowników systemów informatycznych następuję przynajmniej raz na 30 dni;
   7) dane osobowe przechowywane na dyskach twardych komputerów lub innych nośnikach danych, w przypadku zgłoszenia do utylizacji musza zostać trwale usunięte.

§19.

Zasady dostępu do systemu informatycznego dla pracowników:

1) każdy użytkownik systemu loguje się za pomocą indywidualnego loginu i hasła, które zostały mu przydzielone przez ASI;

2) hasło musi spełniać określone kryteria aby było akceptowalne: min 8 znaków zawierających kombinację dużych, małych liter i cyfr oraz być zmieniane co 30 dni;
3) użytkownik jest zobowiązany stosować się do zasad bezpieczeństwa w posługiwaniu się loginem i hasłem do systemu;
4) w przypadku podejrzenia utraty poufności loginu i hasła użytkownik występuje do ASI o ustanowenie nowego hasła.

§20.

Zasady nadzoru nad oprogramowaniem zainstalowanym na komputerach stanowiącym własność PCPR w Zgierzu

1) nadzór nad oprogramowaniem zainstalowanym na komputerach będących własnością PCPR w Zgierzu pełni ABI za pośrednictwem ASI;
2) Administrator systemów informatycznych sporządza i aktualizuje karty komputerów;
3) użytkownik komputera który dokonuje odebrania komputera z oprogramowaniem weryfikuje prawdziwość danych zawartych w karcie komputera i potwierdza je własnoręcznym czytelnym podpisem z datą wykonania podpisu;
4) Administrator bezpieczeństwa informacji oraz Administrator systemów informatycznych dokonują okresowej kontroli danych zawartych w karcie komputera ze stanem faktycznym;
5) jeżeli w wyniku takiej wyrywkowej kontroli wyjdzie na jaw że użytkownik dokonał samowolnej instalacji jakiegokolwiek oprogramowania na które PCPR w Zgierzu nie posiada licencji, bądź nie spełnia wymogów licencyjnych, odpowiada za to bezpośrednio użytkownik komputera;
6) to użytkownik czuwa nad tym żeby zgodnie z procedurami wew. określonymi w dokumencie „*polityka bezpieczeństwa informacji w zakresie przetwarzania danych osobowych w PCPR w Zgierzu*” nie zostawiać komputera zalogowanego i to on odpowiada od momentu podpisania karty komputera, w której znajduje się jego oświadczenie o odpowiedzialności za

wszystkie zmiany w oprogramowaniu i sprzęcie niezgodne z zapisami w karcie komputera;

7) taka sama forma odpowiedzialności obowiązuje w wypadku kontroli przez organy upoważnione do kontroli legalności oprogramowania;
8) za oprogramowanie zewidencjonowane w kartach komputerów i za wszystkie licencje będące własnością PCPR w Zgierzu odpowiada Administrator danych osobowych, a Administrator bezpieczeństwa informacji nadzoruje zgodność z wymogami licencyjnymi oprogramowania użytkowanego i będącego własnością PCPR w Zgierzu.

§21.

Zasady nadzoru pod względem technicznym nad sprzętem komputerowym stanowiącym własność PCPR w Zgierzu

1) sprzęt komputerowy jest sprzętem nie wymagającej systematycznej okresowej kontroli stanu technicznego (nie stwarza zagrożenia dla użytkownika ani dla zainstalowanego w nim oprogramowania sam z siebie, jedynie na skutek działania czynników zewnętrznych, na przykład przepięcia w sieci elektrycznej), dlatego zrezygnowano z przeprowadzania systematycznych okresowych przeglądów takiego sprzętu. Stan ilościowy sprzętu oraz oprogramowania jest sprawdzany w ramach inwentaryzacji;
2) nadzór nad sprzętem technicznym sprawuje Administrator bezpieczeństwa informacji za pośrednictwem Administratora systemów informatycznych i to oni reagują na wszelkiego typu zgłoszenia od pracowników – użytkowników systemu informatycznego dotyczące nieprawidłowego działania sprzętu czy też oprogramowania, odnotowuje każdą naprawę i usterkę oraz jej usunięcie w karcie komputera;
3) po dokonaniu naprawy przedstawia się użytkownikowi do podpisu nową kartę komputera z naniesioną informacją na czym polegała naprawa i co zostało w wyniku jej wymienione.

§22.

Ochrona budynków oraz pomieszczeń gdzie przetwarzane są dane osobowe:

1) wszystkie pomieszczenia, w których przetwarzane są dane osobowe posiadają drzwi zabezpieczone zamkiem, zamykanym po zakończeniu pracy;
2) dokumentacja zawierająca dane osobowe w wersji papierowej przechowywana jest w specjalnych szafach zabezpieczonych zamkiem;
3) budynek zabezpieczony jest systemem alarmowym, obsługiwanym i zarządzanym przez firmę zewnętrzną oraz przez zarządcę budynku od którego PCPR w Zgierzu wynajmuje część pomieszczeń.

X. Procedury postepowania w przypadku naruszenia ochrony danych osobowych

§23.

Niniejsze procedury wew. stosuje się w przypadku, gdy stwierdzono naruszenie zabezpieczeń sprzętu informatycznego, sieci komputerowej, systemu alarmowego i zabezpieczenia pomieszczeń, w których przetwarzane są dane osobowe.

§24.

Za naruszenie ochrony danych osobowych uważa się w szczególności:

1) nieuprawniony dostęp lub próbę dostępu do danych osobowych lub pomieszczeń, w których się one znajdują,
2) naruszenie lub próby naruszenia integralności danych rozumiane jako wszelkie modyfikacje, zniszczenia lub próby ich dokonania przez osoby nieuprawnione lub uprawnione działające w złej wierze lub jako błąd w działaniu osoby uprawnionej (np. zmianę zawartości danych, utratę całości lub części danych),
3) naruszenie lub próby naruszenia integralności systemu,
4) zmianę lub utratę danych zapisanych na kopiach zapasowych,
5) naruszenie lub próby naruszenia poufności danych lub ich części,
6) nieuprawniony dostęp (sygnał o nielegalnym logowaniu lub inny objaw wskazujący na próbę lub działanie związane z nielegalnym dostępem do systemu),
7) udostępnienie osobom nieupoważnionym danych osobowych lub ich części,
8) zniszczenie, uszkodzenie lub wszelkie próby ingerencji nieuprawnionej w system informatyczny zmierzające do zakłócenia jego działania bądź pozyskania w sposób niedozwolony (lub w celach niezgodnych z przeznaczeniem) danych zawartych w systemie informatycznym lub kartotekach.

§25.

Osobami bezpośrednio odpowiedzialnymi za zgodną z prawem ochronę danych osobowych w PCPR w Zgierzu i ich zabezpieczeń są:

1) Administrator danych osobowych;
2) Administrator bezpieczeństwa informacji;
3) Administrator systemów Informatycznych;
4) pracownicy upoważnieni do przetwarzania danych osobowych w PCPR w Zgierzu.

§26.

1. Każdy pracownik PCPR w Zgierzu biorący udział w przetwarzaniu danych osobowych w systemie informatycznym jest odpowiedzialny za bezpieczeństwo tych danych. W szczególności osoba, która stwierdzi lub podejrzewa naruszenie zabezpieczenie ochrony danych osobowych w systemie informatycznym (lub przetwarzanych w inny sposób) powinna niezwłocznie poinformować o tym fakcie Administratora bezpieczeństwa informacji. W przypadku braku możliwości zawiadomienia ABI lub ASI niezwłocznie należy powiadomić bezpośredniego przełożonego.
2. Do czasu przybycia Administratora bezpieczeństwa informacji należy:
   1) niezwłocznie podjąć czynności niezbędne do powstrzymania niepożądanych skutków zaistniałego naruszenia, o ile istnieje taka możliwość, a następnie uwzględnić w działaniu również ustalenie przyczyn lub sprawców;
   2) zabezpieczyć dostęp do miejsca lub urządzenia przez osoby trzecie;
   3) wstrzymać pracę na komputerze na którym zaistniało naruszenie ochrony oraz nie uruchamiać bez koniecznej potrzeby komputerów i innych urządzeń, których funkcjonowanie w związku naruszeniem ochrony zostało wstrzymane;
   4) zaniechać dalszych planowanych przedsięwzięć, które wiążą się z zaistniałym naruszeniem i mogą utrudnić udokumentowanie i analizę zdarzenia;

5) nie zmieniać położenia przedmiotów, które pozwalają stwierdzić naruszenie ochrony lub odtworzyć jej okoliczności;
6) podjąć stosowne do zaistniałej sytuacji, inne niezbędne działania celem zapobieżenia dalszym zagrożeniom, które mogą skutkować utratą danych osobowych;
7) podjąć inne działania przewidziane w instrukcjach technicznych i technologicznych stosowanie do objawów i komunikatów towarzyszących naruszeniu;
8) wstępnie udokumentować zaistniałe naruszenie;
9) nie opuszczać bez uzasadnionej potrzeby miejsca zdarzenia do czasu przybycia Administratora bezpieczeństwa informacji lub osoby upoważnionej.

3. Po przybyciu na miejsce naruszenia lub ujawnienia ochrony danych osobowych Administrator bezpieczeństwa informacji lub osoba go zastępująca powinna:
1) zapoznać się z zaistniałą sytuacją i dokonać wyboru metody dalszego postępowania mając na uwadze ewentualne zagrożenia dla prawidłowości pracy;
2) zaprotokołować wszelkie informacje związane ze zdarzeniem;
3) wygenerować i wydrukować wszystkie możliwe dokumenty i raporty, które mogą pomóc w ustaleniu okoliczności zdarzenia;
4) przystąpić do zidentyfikowania rodzaju zaistniałego zdarzenia, zwłaszcza do określenia skali zniszczeń i metody dostępu do danych niepowołanych;
5) dokonać fizycznego odłączenia urządzeń i segmentów sieci, które mogły umożliwić dostęp do bazy danych osobie nie uprawnionej;
6) wylogować użytkownika podejrzanego o naruszenie zabezpieczenia ochrony danych;
7) dokonać zmiany hasła na konto Administratora bezpieczeństwa informacji i użytkownika, poprzez które uzyskano nielegalny dostęp w celu uniknięcia ponownej próby włamania;
8) zażądać dokładnej relacji z zaistniałego naruszenia od osoby powiadamiającej, jak również od każdej innej osoby, która może posiadać informacje związane z zaistniałym naruszeniem.

4. Administrator bezpieczeństwa informacji dokumentuje zaistniały przypadek naruszenia oraz sporządza raport, który powinien zawierać w szczególności:

1) wskazanie osoby powiadamiającej o naruszeniu oraz innych osób zaangażowanych w zdarzeniu;
2) określeniu czasu, miejsca naruszenia i powiadomienia;
3) określeniu okoliczności towarzyszących i rodzaju naruszenia;
4) wyszczególnienie wziętych faktycznie pod uwagę przesłanek do wyboru metody postępowania i opis podjętego działania;
5) wstępną ocenę przyczyn wystąpienia naruszenia;
6) ocenę przeprowadzonego postępowania wyjaśniającego i naprawczego.

5. Raport o którym mowa w pkt. 4 Administrator bezpieczeństwa informacji przekazuję niezwłocznie Administratorowi danych osobowych.
6. Administrator bezpieczeństwa informacji przystępuje do usuwania skutków incydentu i przywrócenia prawidłowego przebiegu procesu przetwarzania danych osobowych, w szczególności działania związane z usuwaniem skutków incydentu mogą obejmować:
   1) przeprowadzenie naprawy sprzętu informatycznego;
   2) rekonfigurację sprzętu informatycznego;
   3) wprowadzenie poprawek do oprogramowania;
   4) rekonfiguracje oprogramowania;
   5) odtworzenie danych z kopii awaryjnych;
   6) modyfikacje danych w celu odtworzenia ich integralności;
   7) inne naprawy urządzeń wchodzących w skład infrastruktury informatycznej wspomagającej lub zabezpieczających działanie systemu informatycznego.

XI. Postanowienia końcowe

§27.

1. Wobec osoby, która w przypadku naruszenia ochrony danych osobowych lub uzasadnionego domniemania takiego naruszenia nie podjęła działania określonego w niniejszym dokumencie, a w szczególności nie powiadomiła odpowiedniej osoby zgodnie z określonymi zadaniami, a także gdy nie zrealizowała stosownego działania dokumentującego ten przypadek, wszczyna się postępowanie dyscyplinarne.

2. Administrator bezpieczeństwa informacji zobowiązany jest prowadzić ewidencję osób, które zostały zapoznane z niniejszym dokumentem i zobowiązują się do stosowania zasad w nim zawartych.

3. Przypadki nieuzasadnionego zaniechania obowiązków wynikających z niniejszego dokumentu mogą być traktowane jako ciężkie naruszenie obowiązków pracowniczych, w szczególności przez osobę która wobec naruszenia ochrony danych osobowych lub uzasadnionego domniemania takiego naruszenia nie powiadomiła o tym Administratora bezpieczeństwa informacji.

4. Orzeczona kara dyscyplinarna wobec osoby uchylającej się od powiadomienia Administratora Bezpieczeństwa Informacji nie wyklucza odpowiedzialności karnej tej osoby zgodnie z ustawą z dnia 29 sierpnia 1997r. o ochronie danych osobowych (tekst jednolity Dz. U. z 2014 r. poz. 1182 ze zm.) oraz możliwości wniesienia wobec niej sprawy z powództwa cywilnego przez pracodawcę o zrekompensowanie poniesionych strat.

5. W sprawach nie uregulowanych niniejszym dokumentem mają zastosowanie przepisy ustawy z dnia 29 sierpnia 1997r. o ochronie danych osobowych (tekst jednolity Dz. U. z 2014 r. poz. 1182 ze zm.) rozporządzenia Ministra Spraw

Wewnętrznych i Administracji z dnia 29 kwietnia 2004r. 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).

§28.

1. W związku ze zmianami w zakresie ochrony danych osobowych oraz mając na uwadze zmiany przepisów w tym zakresie, ABI zobowiązuję się dokonywać każdorazowo do dnia 30 kwietnia każdego roku aktualizacji treści zawartej w niniejszej polityce bezpieczeństwa przetwarzania danych osobowych oraz instrukcji zarządzania systemem informatycznym.
2. Aktualizacja zapisów prowadzona będzie pod kątem zgodności stanu zapisanego ze stanem faktycznym, w szczególności danych zawartych w następujących dokumentach:
   1) wykazie budynków i pomieszczeń tworzących obszar, w którym przetwarzane są dane osobowe,
   2) rejestru zbiorów danych osobowych wraz ze wskazaniem programów zastosowanych do przetwarzania tych danych,
   3) ewidencji osób upoważnionych do przetwarzania danych osobowych w Powiatowym Centrum Pomocy Rodzinie w Zgierzu,
   4) określenie środków technicznych i organizacyjnych niezbędnych dla zapewnienia poufności, integralności i rozliczalności przetwarzanych danych,
   5) sposobu przepływu danych pomiędzy poszczególnymi systemami informatycznymi w sieci lokalnej (LAN).

XII. Załączniki do polityki bezpieczeństwa

Integralną część niniejszego dokumentu stanowią następując załączniki:

- **załącznik nr 1**: *„Oświadczenie o zachowaniu poufności i zapoznaniu się z przepisami o ochronie danych osobowych”.*
- **załącznik nr 2**: „ *Wniosek o wydanie upoważnienia do przetwarzania danych osobowych”.*
- **załącznik nr 3**: *„Upoważnienie do przetwarzania danych osobowych”.*
- **Załącznik nr 4**: *„Unieważnienie wydanego upoważnienia do przetwarzania danych osobowych”.*
- **załącznik nr 5**: „*Wykaz budynków, pomieszczeń lub części pomieszczeń tworzących obszar w którym przetwarzane są dane osobowe”.*
- **załącznik nr 6**: *„ Rejestr zbiorów danych osobowych wraz ze wskazaniem programów (aplikacji) zastosowanych do przetwarzania danych osobowych w PCPR w Zgierzu”.*
- **załącznik nr 7**: *„Ewidencja osób upoważnionych do przetwarzania danych osobowych w PCPR w Zgierzu”.*
- **załącznik nr 8:** *„Opis sposobu przepływu danych pomiędzy poszczególnymi systemami informatycznymi w sieci lokalnej PCPR w Zgierzu”.*
- **załącznik nr 9:** *„Oświadczenie informacyjne dla pracownika PCPR w Zgierzu”.*