POLITYKA BEZPIECZEŃSTWA

INFORMACJI

W ZAKRESIE PRZETWARZANIA DANYCH OSOBOWYCH

w

POWIATOWYM CENTRUM POMOCY RODZINIE w KRAPKOWICACH

KRAPKOWICE, 2015 r.

SPIS TREŚCI

I. POSTANOWIENIA OGÓLNE

§ 1

Celem Polityki Bezpieczeństwa danych osobowych, zwanej dalej Polityką Bezpieczeństwa, jest uzyskanie optymalnego i zgodnego z wymogami obowiązujących aktów prawnych w zakresie ochrony danych osobowych, sposobu przetwarzania w Powiatowym Centrum Pomocy Rodzinie w Krapkowicach grupy informacji zawierającej dane osobowe.

§ 2

Określenia użyte w Polityce Bezpieczeństwa oznaczają:

1. PCPR Powiatowe Centrum Pomocy Rodzinie w Krapkowicach,
2. dane osobowe wszelkie informacje dotyczące zidentyfikowanej lub możliwej do zidentyfikowania osoby fizycznej,
3. przetwarzanie danych osobowych gromadzenie, utrwalanie przechowywanie, opracowywanie, zmienianie, udostępnianie i usuwanie danych osobowych, zwłaszcza w systemach informatycznych,
4. użytkownik osoba upoważniona do przetwarzania danych osobowych,
5. administrator systemu osoba upoważniona do zarządzania systemem informatycznym,
6. system informatyczny system przetwarzania danych w PCPR Krapkowice wraz z zasobami ludzkimi, technicznymi oraz finansowymi, który dostarcza i rozprowadza informacje,
7. zabezpieczenie systemu informatycznego należy przez to rozumieć wdrożenie stosowanych środków administracyjnych, technicznych oraz ochrony przed modyfikacją, zniszczeniem, nieuprawnionym dostępem i ujawnieniem lub pozyskaniem danych osobowych a także ich utratą.

II. DEFINICJA BEZPIECZEŃSTWA INFORMACJI

§ 3.

1.Utrzymanie bezpieczeństwa przetwarzanych przez PCPR informacji rozumiane jest jako zapewnienie ich poufności, integralności i dostępności na odpowiednim poziomie. Miarą bezpieczeństwa jest wielkość ryzyka związanego z zasobem stanowiącym przedmiot niniejszej Polityki.

2.Poniżej opisane jest rozumienie wyżej wymienionych pojęć w odniesieniu do informacji i aplikacji:

1) Poufność informacji rozumiana jako zapewnienie, że tylko uprawnieni pracownicy mają dostęp do informacji,
2) Integralność informacji rozumiana jako zapewnienie dokładności i kompletności informacji oraz metod jej przetwarzania,
3) Dostępność informacji rozumiane 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.

3. Dodatkowo zarządzanie bezpieczeństwem informacji wiąże się z zapewnieniem:
1) Niezaprzeczalności odbioru rozumianej jako zdolność systemu do udowodnienia, że adresat informacji otrzymał ją w określonym miejscu i czasie,
2) Niezaprzeczalności nadania rozumianej jako zdolność systemu do udowodnienia, że nadawca informacji faktycznie ją nadał lub wprowadził do systemu w określonym miejscu i czasie,
3) Rozliczalności działań rozumianej, jako zapewnienie, że wszystkie działania istotne dla przetwarzania informacji zostały zarejestrowane w systemie i możliwym jest zidentyfikowanie użytkownika, który działania dokonał.

III. ZAKRES

§ 4.

1.W systemie informacyjnym PCPR przetwarzane są informacje służące do wykonywania zadań z zakresu pomocy społecznej, pieczy zastępczej, przeciwdziałania przemocy w rodzinie i rehabilitacji społecznej osób niepełnosprawnych.

2.Informacje te są przetwarzane i składowane zarówno w postaci manualnej jak i elektronicznej.

§ 5

Politykę Bezpieczeństwa stosuje się do:

1. danych osobowych przetwarzanych w systemie Pomost,
2. wszystkich informacji dotyczących danych pracowników PCPR, w tym danych osobowych personelu i treści zawieranych umów o pracę,
3. wszystkich danych kandydatów do pracy zbieranych na etapie rekrutacji,

4. informacji dotyczących zabezpieczenia danych osobowych, w tym w szczególności nazw kont i haseł w systemach przetwarzania danych osobowych,
5. rejestru osób dopuszczonych do przetwarzania danych osobowych,
6. innych dokumentów zawierających dane osobowe.

§ 6.

1. Zakresy określone przez dokumenty Polityki Bezpieczeństwa Informacji mają zastosowanie do całego systemu informacyjnego PCPR 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 lub klientów PCPR, o ile zostały przekazane na podstawie umów,
3) wszystkich lokalizacji pomieszczeń, w których są lub będą przetwarzane informacje podlegające ochronie,
4) wszystkich pracowników w rozumieniu przepisów Kodeksu Pracy, konsultantów, stażystów i innych osób mających dostęp do informacji podlegających ochronie.

2. Do stosowania zasad określonych przez dokumenty Polityki Bezpieczeństwa zobowiązani są wszyscy pracownicy w rozumieniu Kodeksu Pracy, konsultanci, stażyści oraz inne osoby mające dostęp do informacji podlegających ochronie.

§ 7.

Informacje niejawne nie są objęte zakresem niniejszej Polityki.

IV. STRUKTURA DOKUMENTÓW POLITYKI BEZPIECZEŃSTWA INFORMACJI

§ 8.

1.Dokumenty Polityki Bezpieczeństwa Informacji ustanawiają metody zarządzania oraz wymagania niezbędne do zapewnienia skutecznej i spójnej ochrony przetwarzanych informacji.

2.Zestaw dokumentów Polityki Bezpieczeństwa Informacji składa się z:

1) Niniejszego dokumentu Polityki Bezpieczeństwa Informacji,
2) Instrukcji zarządzania systemami informatycznymi w zakresie wymogów bezpieczeństwa przetwarzania danych osobowych, opisującej sposób zarządzania systemami przetwarzania danych osobowych w PCPR,

3) Instrukcji postępowania w sytuacji naruszenia ochrony danych osobowych, opisującej tryb postępowania w sytuacjach naruszenia zabezpieczenia zasobów danych osobowych, zaobserwowanych prób naruszenia tego zabezpieczenia, a także uzasadnionego podejrzenia o przygotowywanej próbie naruszenia.
4) Wykaz pomieszczeń tworzących obszar, w którym przetwarzane są dane osobowe.

V. DOSTĘP DO INFORMACJI

§ 9.

Wszystkie osoby, których rodzaj wykonywanej pracy będzie wiązał się z dostępem do danych osobowych, przed przystąpieniem do pracy, podlegają przeszkoleniu w zakresie obowiązujących przepisów prawa dotyczących ochrony danych osobowych oraz obowiązujących w PCPR zasad ochrony danych osobowych.

§ 10.

Zakres czynności dla osoby dopuszczonej do przetwarzania danych osobowych powinien określać zakres odpowiedzialności tej osoby za ochronę danych osobowych w stopniu odpowiednim do zadań tej osoby realizowanych przy przetwarzaniu tych danych.

§ 11.

Udostępnianie danych osobowych podmiotom upoważnionym do ich otrzymania, na podstawie przepisów prawa, powinno odbywać się wg określonych odrębnymi przepisami procedur postępowania.

VI. ZARZĄDZANIE DANYMI OSOBOWYMI

§ 12.

Administratorem danych osobowych PCPR jest Dyrektor Powiatowego Centrum Pomocy Rodzinie w Krapkowicach.

§ 13.

Za bezpieczeństwo danych osobowych PCPR, odpowiada Administrator danych osobowych – Dyrektor Powiatowego Centrum Pomocy Rodzinie w Krapkowicach.

§ 14.

1. Obowiązki wynikające z ustawy o ochronie danych osobowych Dyrektor Powiatowego Centrum Pomocy Rodzinie w Krapkowicach powierza Administratorowi Systemu Informatycznemu (ASI).

2. ASI odpowiada za realizację wymagań obowiązujących przepisów prawa, dotyczących ochrony danych osobowych.

3. ASI zobowiązany jest do zapoznania pracowników PCPR z treścią ustawy z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (Dz. U. z 2002 r. Nr 101, poz. 926, z późn. zm.), Polityką Bezpieczeństwa Informacji w zakresie przetwarzania danych osobowych, Instrukcją zarządzania systemami informatycznymi w zakresie wymogów bezpieczeństwa przetwarzania danych osobowych oraz Instrukcją postępowania w sytuacji naruszenia ochrony danych osobowych.

4. Zapoznanie się z dokumentami określonymi w ust. 3 pracownicy PCPR potwierdzają podpisem na „Indywidualnym zakresie czynności osoby zatrudnionej przy przetwarzaniu danych osobowych" (wzór w załączniku nr 3 do Instrukcji zarządzania systemami informatycznymi w zakresie wymogów bezpieczeństwa przetwarzania danych osobowych w PCPR) i przekazują Administratorowi Bezpieczeństwa Informacji.

§ 15.

Ochrona zasobów danych osobowych PCPR jako całości przed ich nieuprawnionym użyciem lub zniszczeniem jest jednym z podstawowych obowiązków pracowników PCPR.

VII. ZAKRESY ODPOWIEDZIALNOŚCI

§ 16.

Za bezpieczeństwo informacji odpowiedzialny jest każdy pracownik PCPR.

§ 17.

Administrator Systemu Informatycznego odpowiedzialny jest za:

1. bieżący monitoring i zapewnienie ciągłości działania systemu informatycznego oraz baz danych,
2. optymalizację wydajności systemu informatycznego, baz danych,
3. instalacje i konfiguracje sprzętu sieciowego i serwerowego,
4. instalacje i konfiguracje oprogramowania systemowego, sieciowego, oprogramowania bazodanowego,
5. konfigurację i administrację oprogramowaniem systemowym, sieciowym oraz bazodanowym zabezpieczającym dane chronione przed nieupoważnionym dostępem,
6. współpracę z dostawcami usług oraz sprzętu sieciowego i serwerowego oraz zapewnienie zapisów dotyczących ochrony danych osobowych,

7. zarządzanie kopiami awaryjnymi konfiguracji oprogramowania systemowego, sieciowego,
8. zarządzanie kopiami awaryjnymi danych w tym danych osobowych oraz zasobów umożliwiających ich przetwarzanie,
9. przeciwdziałanie próbom naruszenia bezpieczeństwa informacji,
10. przyznawanie na wniosek Administratora Danych ściśle określonych praw dostępu do informacji w danym systemie,
11. zarządzanie licencjami, procedurami ich dotyczącymi,
12. prowadzenie profilaktyki antywirusowej.

VIII. PRZETWARZANIE DANYCH OSOBOWYCH

§ 19.

Systemy informatyczne, służące do przetwarzania danych osobowych, muszą spełniać wymogi obowiązujących aktów prawnych regulujących zasady gromadzenia i przetwarzania danych osobowych.

§ 20.

Do tworzenia kopii bezpieczeństwa danych osobowych w postaci elektronicznej służą indywidualne systemy archiwizowania dla poszczególnych systemów przetwarzania.

§ 21.

Kopie bezpieczeństwa oraz dokumenty papierowe zawierające dane osobowe przechowuje się w warunkach uniemożliwiających dostęp do nich osobom nieuprawnionym.

IX. ARCHIWIZOWANIE INFORMACJI ZAWIERAJĄCYCH DANE OSOBOWE

§ 22.

Zasady archiwizacji i brakowania dokumentów reguluje Ustawa z dnia 14 lipca 1983r. o Narodowym Zasobie Archiwalnym i Archiwach (Dz. U. z 2011r. Nr 123, poz. 698 ze zm.).

Wykaz pomieszczeń tworzących w Powiatowym Centrum Pomocy Rodzinie w Krapkowicach obszar, w którym przetwarzane są dane osobowe:

1. Dyrektor – pok. nr 204 A
2. Zespół ds. pieczy zastępczej – pok. nr 201, 203
3. Księgowość, Stanowisko ds. Administracyjno-Kadrowych – pok. 204 B
4. Stanowisko ds. Osób Niepełnosprawnych – pok. nr 202