POLITYKA BEZPIECZEŃSTWA INFORMACJI
w Warszawskim Hospicjum Społecznym
wydana w dniu 2018.05.20
przez Zarząd Hospicjum

Spis treści:

I. Wykaz czynności danych osobowych w WHS.
II. Zakres danych osobowych przetwarzanych w WHS.
III. Wykaz budynków, pomieszczeń lub części pomieszczeń, w których przetwarzane są dane osobowe.
IV. Procedury nadawania i zmiany uprawnień do przetwarzania danych osobowych.
V. Odpowiedzialność.
VI. Rejestr użytkowników.

Celem Polityki Bezpieczeństwa Informacji jest zapewnienie ochrony DANYCH OSOBOWYCH przetwarzanych w celach określonych w art. 27 ust. 2 pkt. 7 Ustawy z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (t.j. Dz. U. Z 2002 r. Nr 101, poz. 926 z późn. zm.) ROZPORZĄDZENIE 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 (ogólne rozporządzenie o ochronie danych) przetwarzanych przez Warszawskie Hospicjum Społeczne przed wszelkiego rodzaju zagrożeniami, tak wewnętrznymi jak i zewnętrznymi, świadomymi lub nieświadomymi.

Polityka obejmuje wszystkich pracowników Warszawskiego Hospicjum Społecznego oraz dostawców, podmiotów współpracujących na podstawie umów cywilnoprawnych, mających jakikolwiek kontakt z danymi osobowymi objętymi ochroną.

Przetwarzanie danych osobowych w Warszawskim Hospicjum Społecznym odbywa się w wersji papierowej i za pomocą systemów informatycznych.

Administratorem danych w Warszawskim Hospicjum Społecznym jest Zarząd Stowarzyszenia.

Słowniki:

1. ADO - Administrator Danych Osobowych – należy przez to rozumieć Zarząd Warszawskiego Hospicjum Społecznego.

2. ASI – Administrator Systemu Informatycznego – osoba odpowiedzialna za funkcjonowanie systemu informatycznego WHS.

3. Dane osobowe – wszelkie informacje umożliwiające zidentyfikowanie osoby.

4. Identyfikator – należy przez to rozumieć elektroniczne, indywidualne oznaczenie pracowników w systemie informatycznym tzw. login.

5. Pracownik – należy przez to rozumieć osobę zatrudnioną w formie umowy o pracę lub umowy cywilnoprawnej.

6. Użytkownik systemu – należy przez to rozumieć osobę upoważnioną do przetwarzania danych osobowych w systemie informatycznym WHS. Użytkownikiem systemu może być pracownik WHS wykonujący pracę na podstawie umowy o pracę, umowy zlecenie lub innej umowy cywilnoprawnej lub upoważniony wolontariusz.

7. Ustawę – należy przez to rozumieć ustawę z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (t.j. Dz. U. Z 2002 r. Nr 101, poz. 926 z późn. zm.).

I. Wykaz czynności danych przetwarzanych w WHS

Wykaz czynności danych przetwarzanych wymienionym w załączniku nr 1 do niniejszej polityki bezpieczeństwa, będący jej integralną częścią. (Załącznik dostępny w siedzibie WHS)

II. Zakres danych osobowych przetwarzanych w WHS

W WHS. utworzono i wydzielono następujące zbiory danych osobowych:

A. Dane osobowe pracowników i zleceniobiorców, w których przetwarzane są następujące dane: imię i nazwisko, adres zamieszkania PESEL, wysokość wynagrodzenia, telefon kontaktowy.

B. Dane osobowe pracowników i zleceniobiorców dla ZUS, w których przetwarzane są następujące dane: imię i nazwisko, adres zamieszkania, PESEL, przynależność NFZ.

C. Dane osobowe Pacjentów których przetwarzane są następujące dane: imię i nazwisko, adres zamieszkania, telefon kontaktowy, PESEL, przynależność NFZ, historia choroby.

D. Dane osobowe Rodziny Pacjenta: imię i nazwisko, telefon kontaktowy.

E. Dane osobowe Wolontariuszy, których przetwarzane są następujące dane: imię i nazwisko, adres zamieszkania, PESEL, telefon kontaktowy.

F. Dane osobowe dostawców towarów, których przetwarzane są następujące dane: imię i nazwisko, adres firmy, NIP, telefon kontaktowy.

G. Dane osobowe darczyńców, których przetwarzane są następujące dane: imię i nazwisko, adres, nazwa firmy, NIP.

III. Wykaz budynków, pomieszczeń, w których przetwarzane są dane osobowe.

1. Przetwarzanie danych osobowych odbywa się w Warszawskim Hospicjum Społecznym Pl. Inwalidów 3, klatka VII, suterena

3. Dostęp do przetwarzania danych osobowych mają jedynie upoważnieni pracownicy i wolontariusze oraz ADO.

4. Zabrania się przebywania osób postronnych w pomieszczeniach, w których przetwarzane są dane osobowe bez obecności osób upoważnionych.

IV. Procedury nadawania i zmiany uprawnień do przetwarzania danych osobowych.

1. Każdy użytkownik przed przystąpieniem do przetwarzania danych osobowych musi zapoznać się z następującymi dokumentami:
a) Ustawą z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (tekst jednolity – Dz. U. z 2002 r. Nr 101 poz. 926 z późn. zm.),
b) ROZPORZĄDZENIEM 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 (ogólne rozporządzenie o ochronie danych).
c) Rozporządzeniem 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),
d) Niniejszą Polityką Bezpieczeństwa.

2. Zapoznanie się z powyższymi dokumentami użytkownik systemu potwierdza własnoręcznym podpisem na oświadczeniu, którego wzór stanowi Załącznik nr 3. (Załącznik dostępny w siedzibie WHS)

3. Przetwarzanie danych osobowych może dokonywać jedynie użytkownik systemu upoważnionym przez ADO. Wzór upoważnienia stanowi Załącznik nr 2. (Załącznik dostępny w siedzibie WHS). Wzór umowy powierzenia załącznik nr 4. (Załącznik dostępny w siedzibie WHS).

V. Odpowiedzialność

1. Użytkownik systemu ma prawo do wykonania tych czynności, do których został upoważniony.

2. Wszelkie przekroczenia lub jakiekolwiek próby przekroczenia przyznanych uprawnień, będą traktowane jako naruszenie podstawowych obowiązków pracowniczych.

3 W uzasadnionej sytuacji ADO może odebrać uprawnienia w sposób natychmiastowy. Z takiego postępowania ma on sporządzić notatkę służbową do wiadomości użytkownika systemu, którego sprawa dotyczy.

4. Hasło oraz uprawnienia użytkownika systemu, który je utracił, należy niezwłocznie wyrejestrować z systemu informatycznego. Wyrejestrowania z systemu dokonuje ASI.

5. Użytkownik systemu, zatrudniony przy przetwarzaniu danych osobowych, zobowiązany jest do zachowania ich poufności oraz dołożenia wszelkich starań, aby dane osobowe nie zostały przekazane osobom nieuprawnionym.

VI. Rejestr użytkowników

1. ADO jest zobowiązany do prowadzenia i ochrony rejestru użytkowników i ich uprawnień w systemie informatycznym.

2. Rejestr musi odzwierciedlać aktualny stan systemu w zakresie użytkowników i ich uprawnień.

3. Rejestr, którego wzór stanowi Załącznik nr 4 zawiera:
a) imię i nazwisko użytkownika
b) identyfikator użytkownika
c) zakres uprawnień
d) datę nadania uprawnień
e) datę odebrania uprawnień
f) przyczynę odebrania uprawnień
g) podpis ADO.