2019

Polityka Bezpieczeństwa Danych Osobowych

Zielona Terapia

ZIELONA TERAPIA
przestrzeń naturalnie kształtowana

Polityka Bezpieczeństwa Danych Osobowych

Postanowienia ogólne

1. Celem powstania niniejszej Polityki jest realizacja obowiązków wynikających z przepisów dotyczących ochrony danych osobowych, jak również spełnienie wymagań chroniących prywatność i godność osób, których dane osobowe są przetwarzane w przedsiębiorstwie Anna Szczepańska Zielona Terapia.
2. Przedmiotem Polityki jest określenie, opisanie i zawarcie, w tym i załączonych dokumentach, zastosowanych środków technicznych i organizacyjnych zapewniających ochronę przetwarzanych danych osobowych odpowiednią do zagrożeń oraz kategorii danych osobowych objętych ochroną, a w szczególności zabezpieczeń danych osobowych przed ich udostępnieniem osobom nieupoważnionym, zabraniem przez osobę nieuprawnioną, przetwarzaniem z naruszeniem ustawy oraz zmianą, utratą, uszkodzeniem lub zniszczeniem.
3. Polityka została opracowana z uwzględnieniem metod i środków ochrony danych, których skuteczność w czasie ich zastosowania jest powszechnie uznawana. Za priorytet uznano zagwarantowanie zgromadzonym danym osobowym, przez cały okres ich przetwarzania charakteru poufnego wraz z zachowaniem ich integralności i rozliczalności, ze szczególnym uwzględnieniem obowiązujących przepisów prawa dotyczących ochrony danych osobowych.

Podstawa prawna

4. Dane osobowe w przedsiębiorstwie Anna Szczepańska Zielona Terapia przetwarzane są z poszanowaniem obowiązujących w tym zakresie przepisów prawa, a w szczególności:
    1) 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 – dalej również jako „RODO")
    2) Przepisów ustawy z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (tj. Dz.U. z 2002 r., nr 101, poz. 926 z póź.zm.) oraz przepisów wykonawczych wydanych z upoważnienia tej ustawy, a w szczególności Rozporządzenia 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 do przetwarzania danych osobowych (Dz.U. nr 100, poz. 100 poz.1024);
    3) Przepisów art. 22 § 1 -5 ustawy z dnia 26 czerwca 1974 r. Kodeks pracy (tj. Dz.U. z 1998 r. nr 21, poz. 94 z póź. zm.) i przepisów wykonawczych wydanych z upoważnienia tej ustawy;
    4) Innych przepisów ustawy i rozporządzeń normujących przetwarzanie danych osobowych określonych kategorii.

5. Dane osobowe w przedsiębiorstwie Anna Szczepańska Zielona Terapia przetwarzane są w celu zawarcia i realizacji umów z klientami, a także wykonania ciążących na przedsiębiorstwie obowiązków prawnych, ustalenia i obrony oraz dochodzenia roszczeń, obsługi reklamacji i zgłoszeń, wsparcia technicznego, rozliczeń finansowych, w tym wystawienia dokumentów księgowych.
6. Przez użyte w dokumencie określenia rozumie się:

1) **Administrator Danych Osobowych** – Anna Szczepańska prowadzący działalność gospodarczą pod firmą Anna Szczepańska Zielona Terapia z siedzibą przy ul. Petrażyckiego 7e/1, 30-399 Kraków, wpisaną do Centralnej Ewidencji i Informacji o Działalności Gospodarczej (CEiDG), NIP: 6762089444, REGON: 121052061;
2) **dane osobowe** – informacje o zidentyfikowanej lub możliwej do zidentyfikowania osobie fizycznej („osobie, której dane dotyczą"); możliwa do zidentyfikowania osoba fizyczna to osoba, którą można bezpośrednio lub pośrednio zidentyfikować, w szczególności na podstawie identyfikatora takiego jak imię i nazwisko, numer identyfikacyjny, dane o lokalizacji, identyfikator internetowy lub jeden bądź kilka szczególnych czynników określających fizyczną, fizjologiczną, genetyczną, psychiczną, ekonomiczną, kulturową lub społeczną tożsamość osoby fizycznej;
3) **zbiór danych** – oznacza uporządkowany zestaw danych osobowych dostępnych według określonych kryteriów, niezależnie od tego, czy zestaw ten jest scentralizowany, zdecentralizowany czy rozproszony funkcjonalnie lub geograficznie;
4) **przetwarzanie danych osobowych** – oznacza operację lub zestaw operacji wykonywanych na danych osobowych lub zestawach danych osobowych w sposób zautomatyzowany lub niezautomatyzowany, 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;
5) **system informatyczny** - zespół współpracujących ze sobą urządzeń, programów, procedur przetwarzania informacji i narzędzi programowych zastosowanych w celu przetwarzania danych;
6) **zabezpieczenie danych osobowych** – wdrożenie i eksploatacja stosownych środków technicznych i organizacyjnych zapewniających ochronę danych przed ich nieuprawnionym przetwarzaniem.

Zakres stosowania dokumentu Polityki Bezpieczeństwa Danych Osobowych.

7. Polityka Bezpieczeństwa Danych Osobowych ma zastosowanie w stosunku do wszystkich postaci informacji zawierających dane osobowe: dokumentów papierowych, zapisów elektronicznych i innych, będących własnością lub administrowanych przez przedsiębiorstwo Anna Szczepańska Zielona Terapia i przetwarzanych w systemach informatycznych i tradycyjnych (papierowych) przedsiębiorstwa.

8. Polityka Bezpieczeństwa Danych Osobowych ma zastosowanie w stosunku do wszystkich pracowników i współpracowników przedsiębiorstwa Anna Szczepańska Zielona Terapia, jak również osób trzecich mających dostęp do danych osobowych w przedsiębiorstwie.

9. Ochrona danych osobowych wynikająca z Polityki Bezpieczeństwa Danych Osobowych jest realizowana na każdym etapie przetwarzania informacji.

Zasady dotyczące przetwarzania danych osobowych

10. Dane osobowe muszą być:

a) przetwarzane zgodnie z prawem, rzetelnie i w sposób przejrzysty dla osoby, której dane dotyczą („zgodność z prawem, rzetelność i przejrzystość");

b) zbierane w konkretnych, wyraźnych i prawnie uzasadnionych celach i nieprzetwarzane dalej w sposób niezgodny z tymi celami; dalsze przetwarzanie do celów archiwalnych w interesie publicznym, do celów badań naukowych lub historycznych lub do celów statystycznych nie jest uznawane w myśl art. 89 ust. 1 RODO za niezgodne z pierwotnymi celami („ograniczenie celu");

c) adekwatne, stosowne oraz ograniczone do tego, co niezbędne do celów, w których są przetwarzane („minimalizacja danych");

d) prawidłowe i w razie potrzeby uaktualniane; należy podjąć wszelkie rozsądne działania, aby dane osobowe, które są nieprawidłowe w świetle celów ich przetwarzania, zostały niezwłocznie usunięte lub sprostowane („prawidłowość");

e) przechowywane 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 RODO, 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 („ograniczenie przechowywania");

f) przetwarzane w sposób zapewniający odpowiednie bezpieczeństwo danych osobowych, w tym ochronę przed niedozwolonym lub niezgodnym z prawem przetwarzaniem oraz przypadkową utratą, zniszczeniem lub uszkodzeniem, za pomocą odpowiednich środków technicznych lub organizacyjnych („integralność i poufność").

Środki techniczne i organizacyjne niezbędne dla realizacji zasad przetwarzania danych osobowych

11. Za bezpieczeństwo informacji odpowiedzialni są wszyscy pracownicy i współpracownicy upoważnieni do przetwarzania danych osobowych. W szczególności odpowiadają oni za przestrzeganie zasad bezpieczeństwa wynikających z niniejszej Polityki oraz zgłaszanie incydentów i wykonywanie zaleceń Administratora Danych Osobowych.

12. Zarządzanie bezpieczeństwem danych osobowych jest procesem ciągłym.

13. We wszystkich umowach, które mogą dotyczyć przetwarzania danych w przedsiębiorstwie Anna Szczepańska Zielona Terapia, należy uwzględnić zapisy zobowiązujące drugą stronę do przestrzegania odpowiednich zapisów Polityki Bezpieczeństwa Informacji.

14. W przypadku konieczności odbierania zgody na przetwarzanie danych osobowych, należy zapewnić dobrowolność jej pozyskania oraz powiadomić o prawie do odwołania takiej zgody.

15. Przedsiębiorstwo Anna Szczepańska Zielona Terapia stosuje przy przetwarzaniu danych środki techniczne i organizacyjne zapewniające ochronę danych, określone w art. 32-36 RODO w szczególności, zapewnia zabezpieczenie integralności i poufności danych osobowych.

16. Do zapewnienia bezpieczeństwa danych i informacji zastosowano następujące środki organizacyjne:

a) dostęp do danych osobowych mogą mieć tylko i wyłącznie pracownicy/współpracownicy posiadający pisemne, imienne upoważnienia nadane przez Administratora danych;

b) każdy z pracowników/współpracowników powinien zachować szczególną ostrożność przy przenoszeniu wszelkich nośników z danymi;

c) należy chronić dane przed wszelkim dostępem do nich osób nieupoważnionych;

d) pomieszczenia, w których są przetwarzane dane osobowe, powinny być zamykane na klucz;

e) dostęp do kluczy posiadają tylko upoważnieni pracownicy/współpracownicy;

f) dostęp do pomieszczeń, w których są przetwarzane dane osobowe, mogą mieć tylko upoważnieni pracownicy/współpracownicy,

g) w przypadku pomieszczeń, do których dostęp mają również osoby nieupoważnione, mogą przebywać w tych pomieszczeniach tylko w obecności osób upoważnionych i tylko w czasie wymaganym na wykonanie niezbędnych czynności;

h) szafy, w których przechowywane są dane, powinny być zamykane na klucz;

i) klucze do tych szaf posiadają tylko upoważnieni pracownicy/współpracownicy;

j) szafy z danymi powinny być otwarte tylko na czas potrzebny na dostęp do danych, a następnie powinny być zamykane;

k) dane w formie papierowej mogą znajdować się na biurkach tylko na czas niezbędny na dokonanie czynności służbowych, a następnie muszą być chowane do szaf.

17. Do zapewnienia bezpieczeństwa danych i informacji zastosowano następujące środki techniczne:

a) dostęp do komputerów, na których są przetwarzane dane, mają tylko upoważnieni pracownicy/współpracownicy;

b) wszystkie komputery są zabezpieczone hasłami;

c) monitory komputerów, na których przetwarzane są dane, są tak ustawione, aby osoby nieupoważnione nie miały wglądu w dane;

d) na komputerach uruchomiona jest funkcja włączania blokady ekranu zabezpieczonej hasłem w chwili oddalenia się od sprzętu w obecności innych osób

e) w wypadku potrzeby wyniesienia komputera przenośnego (np. typu notebook) zawierającego dane osobowe lub inne informacje chronione, komputer taki musi być odpowiednio dodatkowo zabezpieczony, a dane zaszyfrowane;

f) nie należy udostępniać osobom nieupoważnionym tych komputerów;

g) w przypadku potrzeby przeniesienia danych osobowych pomiędzy komputerami należy dokonać tego z zachowaniem szczególnej ostrożności;

h) nośniki użyte do tego należy wyczyścić (skasować nieodwracalnie), aby nie zostały na nich dane osobowe;
i) w wypadku niemożliwości skasowania danych z nośnika (płyta CD-ROM) należy taką płytę zniszczyć fizycznie;
j) w przypadku wykorzystania do przenoszenia dysków dane należy kasować z tych dysków;
k) niezabezpieczonych danych osobowych nie należy przesyłać drogą elektroniczną;
l) sieć komputerowa jest zabezpieczona przed wszelkim dostępem z zewnątrz;
ł) domena internetowa jest zabezpieczona certyfikatem SSL;
m) błędne lub nieaktualne wydruki i wersje papierowe zawierające dane osobowe lub inne informacje chronione niszczone są za pomocą niszczarki lub w inny mechaniczny sposób uniemożliwiający powtórne ich odtworzenie.

Dostęp do informacji i danych osobowych

18. Przetwarzanie, w tym udostępnianie danych osobowych, jest prawnie dopuszczalne, jeżeli jest niezbędne do zrealizowania uprawnienia lub spełnienia obowiązku wynikającego z przepisu prawa.
19. Dane osobowe można wykorzystać wyłącznie zgodnie z przeznaczeniem, dla którego zostały udostępnione.
20. Podmiot występujący o udostępnienie informacji powinien wskazać podstawę prawną upoważniającą go do otrzymania tych danych albo uzasadnioną potrzebę żądania ich udostępnienia. Tylko w takiej sytuacji można dokonać oceny, czy w określonym przypadku udostępnienie danych jest prawnie dopuszczalne i czy nie będzie ono stanowić naruszenia zasad ochrony informacji.
21. Dane osobowe, dla których okres przetwarzania nie wynika z obowiązujących przepisów prawa i dla których nie jest możliwe określenie z góry tego okresu, są przetwarzane tak długo, jak długo istnieje jednocześnie podstawa prawna oraz cel dla ich przetwarzania.
22. Ustanie celu przetwarzania danych jest równoznaczne z koniecznością usunięcia danych osobowych.
23. Dane osobowe przetwarzane wyłącznie w oparciu o przesłankę zgody na przetwarzanie danych osobowych są usuwane zawsze niezwłocznie po wycofaniu takiej zgody.

Prawa osób , których dane są przetwarzane

24. Przedsiębiorstwo Anna Szczepańska Zielona Terapia gwarantuje osobom fizycznym, których dane osobowe są przetwarzane w związku z bieżącą działalnością, realizację uprawnień gwarantowanych im przez obowiązujące przepisy prawa.
25. W szczególności każdej osobie fizycznej, której dane osobowe są przetwarzane, przysługuje prawo do żądania od administratora dostępu do danych osobowych dotyczących osoby, której dane dotyczą, ich sprostowania, usunięcia lub ograniczenia przetwarzania lub prawo do wniesienia sprzeciwu wobec przetwarzania, a także o prawie do przenoszenia danych.

Postępowanie w sytuacji naruszenia ochrony danych

26. W sytuacji powzięcia informacji o naruszeniu lub podejrzeniu naruszenia ochrony danych osobowych należy postępować zgodnie z zasadami wynikającymi z art. 33 i 34 RODO.
27. W sytuacji stwierdzenia wystąpienia naruszenia ochrony danych osobowych oraz prawdopodobieństwa zaistnienia ryzyka naruszenia praw lub wolności osób fizycznych, informacja o naruszeniu powinna zostać zgłoszona do PUODO.
28. Zgłoszenie naruszenia Administrator danych osobowych przygotowuje w terminie 72 godzin po stwierdzeniu naruszenia, zgodnie z wymaganiami art. 33 RODO.
29. Zgłoszenie przekazywane jest do PUODO w formie elektronicznej za pomocą systemu informatycznego zgodnie z trybem określonym przez organ.
30. W sytuacji, gdy stwierdzone naruszenie ochrony danych osobowych może powodować wysokie ryzyko naruszenia praw lub wolności osób fizycznych, o naruszeniu należy zawiadomić wszystkie osoby, których dane dotyczą. Inspektor analizuje czy w odniesieniu do wymogów art. 34 ust. 3 RODO zawiadomienie osób, których dane dotyczą, będzie wymagane.
31. Wszystkie stwierdzone naruszenia są dokumentowane przez Administratora danych osobowych.

Postanowienia końcowe

32. Polityka jest dokumentem wewnętrznym i nie może być udostępniania osobom nieupoważnionym w żadnej formie.
33. W sprawach nieuregulowanych w niniejszej Polityce mają zastosowanie przepisy RODO oraz UODO.
34. Pracownicy i współpracownicy przedsiębiorstwa Anna Szczepańska Zielona Terapia zobowiązani są do bezwzględnego stosowania zasad określonych w Polityce.

Załączniki:

1. Wzór dokumentu upoważnienia do przetwarzania danych osobowych,
2. Rejestr czynności przetwarzania danych osobowych,
3. Ewidencja naruszeń w obszarze ochrony danych osobowych,
4. Wzór raportu o naruszeniu danych osobowych