POLITYKA BEZPIECZEŃSTWA INFORMACJI OBOWIĄZUJĄCA W GABINECIE LOGOPEDYCZNYM ANNY CHRAPEK OD DNIA 19 MARCA 2024 R.

Celem niniejszej *Polityki Bezpieczeństwa Informacji* jest uzyskanie optymalnego i zgodnego z wymogami obowiązujących aktów prawnych w zakresie ochrony danych osobowych (w szczególności z Rozporządzeniem Parlamentu Europejskiego i Rady (UE) 2016/679 z 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 (dalej: RODO) oraz ustawą o ochronie danych osobowych z dnia 10 maja 2018 r. (Dz.U.2018.1669)) sposobu przetwarzania danych osobowych w gabinecie logopedycznym prowadzonym przez Annę Chrapek, prowadzącą jednoosobową działalność gospodarczą pod firmą ALBERO Anna Chrapek, Zembrzyce 579, 34-210 Zembrzyce, NIP 5521514709, REGON 387364357.

Spis treści:

I. Definicje

1. **Administrator Danych Osobowych –** Anna Chrapek, prowadzącą jednoosobową działalność gospodarczą pod firmą ALBERO Anna Chrapek, Zembrzyce 579, 34-210 Zembrzyce, NIP 5521514709, REGON 387364357.

2. **Dane osobowe** – wszelkie informacje dotyczące zidentyfikowanej lub możliwej do zidentyfikowania osoby fizycznej.

3. **Identyfikator Użytkownika (Login)** – ciąg znaków literowych, cyfrowych lub innych jednoznacznie identyfikujący osobę upoważnioną do przetwarzania danych osobowych w systemie informatycznym (Użytkownika) w razie Przetwarzania danych osobowych w takim systemie.

4. Pracownik – osoba fizyczna zatrudniona u Administratora Danych Osobowych na podstawie umowy o pracę lub umowy cywilnoprawnej.

5. **Przetwarzanie danych** – operacja lub zestaw operacji wykonywanych na danych osobowych lub zestawach danych osobowych w sposób zautomatyzowany lub niezautomatyzowany, taka 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.

6. **System informatyczny** – zespół współpracujących ze sobą urządzeń, programów, procedur przetwarzania informacji i narzędzi programowych zastosowanych w celu przetwarzania danych.

7. **Użytkownik** – osoba upoważniona przez Administratora Danych Osobowych do Przetwarzania danych osobowych.

8. **Zbiór danych** – każdy uporządkowany zestaw danych o charakterze osobowym, dostępny według określonych kryteriów.

II. Postanowienia ogólne

1. Polityka Bezpieczeństwa Informacji reguluje zasady przetwarzania wszystkich danych osobowych w gabinecie logopedycznym Anny Chrapek, niezależnie od formy ich przetwarzania oraz od tego, czy dane są lub mogą być przetwarzane w zbiorach danych.

2. Polityka Bezpieczeństwa Informacji jest przechowywana w wersji elektronicznej oraz w wersji papierowej (minimum jeden egzemplarz) w siedzibie Administratora Danych Osobowych.

3. Polityka Bezpieczeństwa Informacji jest udostępniana do wglądu:

a) osobom posiadającym upoważnienie do przetwarzania danych osobowych - w każdej chwili na ich wniosek,

b) osobom, którym ma zostać nadane upoważnienie do przetwarzania danych osobowych, celem

umożliwienia im zapoznania się z jej treścią.

4. Dla skutecznej realizacji Polityki Administrator Danych Osobowych zapewnia:

a) odpowiednie do zagrożeń i kategorii danych objętych ochroną środki techniczne i rozwiązania organizacyjne mającej na celu zapobiegać występowaniu incydentów z zakresu ochrony danych osobowych,

b) kontrolę i nadzór nad Przetwarzaniem danych osobowych,

c) monitorowanie zastosowanych środków ochrony.

5. Administrator Danych Osobowych zapewnia, że czynności wykonywane w związku z przetwarzaniem i zabezpieczeniem danych osobowych są zgodne z niniejszą Polityką Bezpieczeństwa Informacji oraz odpowiednimi przepisami prawa.

III. Dane osobowe przetwarzane przez Administratora Danych Osobowych

1. Dane osobowe przetwarzane przez Administratora Danych Osobowych gromadzone są w zbiorach danych.

2. Administrator Danych Osobowych w ramach swojej działalności przetwarza dane osobowe przede wszystkim w następujących zbiorach danych:

a) klienci,

b) kontrahenci.

3. Administrator Danych Osobowych nie podejmuje czynności przetwarzania, które mogłyby się wiązać z poważnym prawdopodobieństwem wystąpienia wysokiego ryzyka dla praw i wolności osób. W przypadku planowania takiego działania Administrator wykona czynności określone w art. 35 i nast. RODO.

4. W przypadku planowania nowych czynności przetwarzania Administrator Danych Osobowych dokonuje analizy ich skutków dla ochrony danych osobowych oraz uwzględnia kwestie ochrony danych w fazie ich projektowania.

4. Administrator Danych Osobowych prowadzi rejestr czynności przetwarzania (wzór rejestru czynności przetwarzania stanowi **Załącznik nr 1** do niniejszej Polityki Bezpieczeństwa Informacji).

IV. Obowiązki i odpowiedzialność w zakresie zarządzania bezpieczeństwem

1. Wszyscy Użytkownicy w gabinecie logopedycznym Anny Chrapek zobowiązani są do przetwarzania danych osobowych zgodnie z obowiązującymi przepisami i zgodnie z ustaloną przez Administratora Danych Polityką Bezpieczeństwa Informacji, Instrukcją Zarządzania Systemem Informatycznym, a także innymi dokumentami wewnętrznymi i procedurami związanymi z

Przetwarzaniem danych osobowych obowiązującymi w gabinecie logopedycznym Anny Chrapek.

2. Wszystkie dane osobowe w gabinecie logopedycznym Anny Chrapek są przetwarzane z poszanowaniem zasad przetwarzania przewidzianych przez przepisy prawa:

a) w każdym wypadku występuje chociaż jedna z przewidzianych przepisami prawa podstaw dla przetwarzania danych osobowych,

b) dane osobowe zbierane są w konkretnych, wyraźnych i prawnie uzasadnionych celach i nieprzetwarzane dalej w sposób niezgodny z tymi celami,

c) dane osobowe są przetwarzane jedynie w takim zakresie, jaki jest niezbędny dla osiągnięcia celu przetwarzania danych,

d) dane osobowe są przetwarzane rzetelnie i w sposób przejrzysty,

e) dane osobowe są prawidłowe i w razie potrzeby uaktualniane,

f) czas przechowywania danych osobowych jest ograniczony do okresu ich przydatności do celów, do których zostały zebrane, a po tym okresie są one anonimizowane bądź usuwane,

g) wobec osoby, której dane dotyczą, wykonywany jest obowiązek informacyjny zgodnie z treścią art. 13 i 14 RODO,

h) dane osobowe są zabezpieczone przed naruszeniami zasad ich ochrony.

3. Za naruszenie lub próbę naruszenia zasad przetwarzania i ochrony danych osobowych uważa się w szczególności:

a) naruszenie bezpieczeństwa Systemów informatycznych, w których przetwarzane są dane osobowe, w razie ich przetwarzania w takich systemach,

b) udostępnianie lub umożliwienie udostępniania danych osobowych osobom lub podmiotom do tego nieupoważnionym,

c) niedopełnienie obowiązku zachowania w tajemnicy danych osobowych oraz sposobów ich zabezpieczenia,

d) przetwarzanie danych osobowych niezgodnie z założonym zakresem i celem ich zbierania,

e) spowodowanie uszkodzenia, utraty, niekontrolowanej zmiany lub nieuprawnione kopiowanie danych osobowych,

f) naruszenie praw osób, których dane osobowe są przetwarzane.

4. W przypadku stwierdzenia okoliczności naruszenia zasad ochrony danych osobowych Użytkownik zobowiązany jest do podjęcia wszystkich niezbędnych kroków, mających na celu ograniczenie skutków naruszenia i do niezwłocznego powiadomienia Administratora Danych Osobowych.

5. Do obowiązków Administratora Danych Osobowych w zakresie zatrudniania, zakończenia lub zmiany warunków zatrudnienia pracowników należy dopilnowanie, by:

a) pracownicy byli odpowiednio przygotowani do wykonywania swoich obowiązków z zakresu

ochrony danych osobowych,

b) każdy z przetwarzających dane osobowe pracowników był pisemnie upoważniony do przetwarzania danych osobowych (wzór upoważnienia stanowi **Załącznik nr 2** do niniejszej Polityki Bezpieczeństwa Informacji),

c) każdy pracownik zobowiązał się do zachowania danych osobowych przetwarzanych w gabinecie logopedycznym Anny Chrapek w tajemnicy (wzór oświadczenia i zobowiązania osoby przetwarzającej dane osobowe do zachowania tajemnicy stanowi **Załącznik nr 3** do niniejszej Polityki Bezpieczeństwa).

6. Obowiązki dotyczące pracowników, o których mowa w ust. 5, mają odpowiednie zastosowanie również odnośnie innych Użytkowników.

7. Użytkownicy zobowiązani są do:

a) ścisłego przestrzegania zakresu nadanego upoważnieniem,

b) przetwarzania i ochrony danych osobowych zgodnie z przepisami prawa powszechnie obowiązującego, niniejszą Polityką Bezpieczeństwa Informacji oraz Instrukcją Zarządzania Systemem Informatycznym,

c) zachowania w tajemnicy danych osobowych oraz sposobów ich zabezpieczenia,

d) zgłaszania incydentów związanych z naruszeniem bezpieczeństwa danych oraz niewłaściwym funkcjonowaniem systemu Administratorowi Danych Osobowych lub wyznaczonym i upoważnionym do tego przez niego osobom.

8. Obowiązki, o których mowa w ust. 7 lit. b-d, odnoszą się odpowiednio do pracowników, którzy z jakichkolwiek względów nie zostali przez Administratora Danych Osobowych upoważnieni do przetwarzania danych osobowych.

V. Obszar przetwarzania danych osobowych

Obszar, w którym przetwarzane są dane osobowe obejmuje:

a) lokal, w którym znajduje się siedziba gabinetu logopedycznego Anny Chrapek pod adresem Zembrzyce 579, 34-210 Zembrzyce,

b) serwery należące do Administratora Danych Osobowych lub przez się wynajmowane, niezależnie od miejsca ich usytuowania,

VI. Określenie środków technicznych i organizacyjnych niezbędnych dla zapewnienia poufności, integralności i rozliczalności przetwarzanych danych

1. Administrator Danych zapewnia zastosowanie środków technicznych i organizacyjnych

niezbędnych dla zapewnienia poufności, integralności, rozliczalności i ciągłości Przetwarzanych danych.

2. Zastosowane środki ochrony (techniczne i organizacyjne) powinny być adekwatne do stwierdzonego poziomu ryzyka dla poszczególnych systemów, rodzajów zbiorów i kategorii danych. Środki te obejmują przede wszystkim:

a) ograniczenie dostępu do pomieszczeń, w których przetwarzane są dane osobowe, jedynie do osób odpowiednio upoważnionych; inne osoby mogą przebywać w pomieszczeniach wykorzystywanych do przetwarzania danych jedynie w towarzystwie osoby upoważnionej lub Administratora Danych Osobowych.

b) zamykanie pomieszczeń tworzących obszar Przetwarzania danych osobowych określony w pkt V lit. a na czas nieobecności pracowników i innych osób upoważnionych, w sposób uniemożliwiający dostęp do nich osobom trzecim,

c) wykorzystanie zamykanych na klucz lub szyfr szafek do zabezpieczenia dokumentów zawierających dane osobowe,

d) wykorzystanie niszczarki do skutecznego usuwania dokumentów zawierających dane osobowe, niepotrzebnych do dalszej pracy i niepodlegających przechowywaniu na podstawie przepisów prawa,

e) wprowadzenie polityki czystego biurka i czystego ekranu, w ramach której każdy pracownik i inna osoba upoważniona zobowiązany jest do:

- przechowywania na biurku tylko tych dokumentów, które są mu niezbędne do pracy w danym momencie,
- unikania przechowywania na biurku dokumentów niepotrzebnych do bieżących zadań,
- po zakończeniu pracy z dokumentami zawierającymi dane osobowe odłożenia ich do szuflady lub szafy zamykanej na klucz,
- ustawiania ekranu monitorów komputerów w sposób uniemożliwiający osobom postronnym zapoznania się z wyświetlającymi się na nim treściami, a – w razie potrzeby – stosowania filtra prywatyzującego,
- przy każdy opuszczaniu stanowiska pracy wprowadzenie systemu komputera w stan uśpienia lub wyłączenie go, tak, aby przy kolejnym logowaniu konieczne było wpisanie hasła,
- nie umieszczania na biurku napojów w pojemnikach grożących wylaniem oraz nie spożywanie posiłków nad dokumentami oraz sprzętem komputerowym.

e) wykonywanie kopii zapasowych (awaryjnych) danych osobowych,

f) ochronę sprzętu komputerowego wykorzystywanego przez Administratora Danych Osobowych przed złośliwym oprogramowaniem poprzez:

- korzystanie z aktualnego programu antywirusowego,
- okresowe aktualizacje systemu operacyjnego oraz zainstalowanego na komputerach oprogramowania.

g) zabezpieczenie dostępu do urządzeń gabinetu logopedycznego Anny Chrapek przy pomocy haseł dostępu,

h) zakaz wykorzystywania komputerów gabinetu logopedycznego Anny Chrapek przez pracowników do celów prywatnych,

i) zakaz podłączania do komputerów prywatnych nośników danych,

j) opracowanie i – w miarę potrzeby – aktualizację niniejszej Polityki Bezpieczeństwa Informacji oraz Instrukcji Zarządzania Systemami Informatycznymi,

k) udostępnianie danych osobowych drogą elektroniczną jedynie w postaci zaszyfrowanej lub zabezpieczonej hasłem.

VII. Naruszenia zasad ochrony danych osobowych

1. W przypadku stwierdzenia naruszenia ochrony danych osobowych Administrator Danych Osobowych dokonuje oceny, czy zaistniałe naruszenie mogło powodować ryzyko naruszenia praw lub wolności osób fizycznych.
2. W każdej sytuacji, w której zaistniałe naruszenie mogło powodować ryzyko naruszenia praw lub wolności osób fizycznych, Administrator Danych Osobowych zgłasza fakt naruszenia zasad ochrony danych organowi nadzorczemu bez zbędnej zwłoki – jeżeli to wykonalne, nie później niż w terminie 72 godzin po stwierdzeniu naruszenia (wzór zgłoszenia określa **Załącznik nr 4** do niniejszej Polityki Bezpieczeństwa Informacji; Administrator Danych Osobowych może również skorzystać ze wzoru zamieszczonego na stronie Urzędu Ochrony Danych Osobowych).
3. Jeżeli ryzyko naruszenia praw i wolności jest wysokie, Administrator zawiadamia o incydencie także osobę, której dane dotyczą (wzór zawiadomienia określa **Załącznik nr 5** do niniejszej Polityki Bezpieczeństwa Informacji).

VIII. Powierzenie przetwarzania danych osobowych

Administrator Danych Osobowych może powierzyć przetwarzanie danych osobowych innemu podmiotowi wyłącznie w drodze umowy zawartej w formie pisemnej, zgodnie z wymogami wskazanymi dla takich umów w art. 28 RODO.

IX. Postanowienia końcowe

1. Za niedopełnienie obowiązków wynikających z niniejszego dokumentu pracownik ponosi

odpowiedzialność na podstawie Kodeksu pracy oraz przepisów o ochronie danych osobowych, zaś pozostali Użytkownicy – na podstawie przepisów o ochronie danych osobowych i Kodeksu cywilnego.

2. Integralną część niniejszej Polityki Bezpieczeństwa Informacji stanowią następujące załączniki:

Załączniki:

1. Wzór rejestru czynności przetwarzania danych osobowych.
2. Wzór upoważnienia do przetwarzania danych osobowych.
3. Wzór oświadczenia i zobowiązania osoby przetwarzającej dane osobowe.
4. Wzór zgłoszenia naruszenia zasad ochrony danych do organu nadzorczego.
5. Wzór zawiadomienia o incydencie.