**Polityka bezpieczeństwa przetwarzania danych osobowych**

Niniejsza polityka opisuje reguły i zasady ochrony danych osobowych przetwarzanych w ramach działalności gospodarczej prowadzonej przez Gabinet dietetyczny DIET-COACHING Patrycja Sankowska, Wałcz ul. Dąbrowskiego 7, NIP 765 163 05 62 e-mail: patrycja@dietetyk-medyczny@gmail.com, tel. 535 513 446

## Rozdział I
## Postanowienia ogólne

### § 1

Celem niniejszej polityki jest uzyskanie optymalnego i zgodnego z wymogami obowiązujących aktów prawnych sposobu przetwarzania informacji zawierających dane osobowe, w tym zapewnienie ochrony danych osobowych przed wszelakiego rodzaju zagrożeniami, tak wewnętrznymi jak i zewnętrznymi, świadomymi lub nieświadomymi.

### § 2

Niniejsza polityka została wdrożona w związku z treścią art. 24 ust. 2 RODO jako dowód dołożenia należytej staranności w zakresie ochrony danych osobowych.

### § 3

Ochrona danych osobowych realizowana jest poprzez zabezpieczenia fizyczne, organizacyjne, oprogramowanie systemowe, aplikacje oraz samych użytkowników.

### § 4

Obok niniejszej polityki opracowano i wdrożono instrukcję zarządzania systemami informatycznymi służącymi do przetwarzania danych osobowych. Określa ona sposób zarządzania systemami informatycznymi służącymi do przetwarzania danych osobowych, ze szczególnym uwzględnieniem zapewnienia ich bezpieczeństwa.

### § 5

1. Utrzymanie bezpieczeństwa przetwarzanych danych osobowych rozumiane jest jako zapewnienie ich poufności, integralności, rozliczalności oraz dostępności na odpowiednim poziomie. Miarą bezpieczeństwa jest wielkość ryzyka związanego z ochroną danych osobowych.
2. Zastosowane zabezpieczenia mają służyć osiągnięciu powyższych celów i zapewnić:
   **1)** poufność danych – rozumianą jako właściwość zapewniającą, że dane nie są udostępniane nieupoważnionym osobom,
   **2)** integralność danych – rozumianą jako właściwość zapewniającą, że dane osobowe nie zostały zmienione lub zniszczone w sposób nieautoryzowany

**3)** rozliczalność danych – rozumianą jako właściwość zapewniającą, że działania osoby mogą być przypisane w sposób jednoznaczny tylko tej osobie

**4)** integralność systemu – rozumianą jako nienaruszalność systemu, niemożność jakiejkolwiek manipulacji, zarówno zamierzonej, jak i przypadkowej

**5)** dostępność informacji – rozumianą jako zapewnienie, że osoby upoważnione mają dostęp do informacji i związanych z nią zasobów wtedy, gdy jest to potrzebne

**6)** zarządzanie ryzykiem – rozumiane jako proces identyfikowania, kontrolowania i minimalizowania lub eliminowania ryzyka dotyczącego bezpieczeństwa, które może dotyczyć systemów informacyjnych służących do przetwarzania danych osobowych.

**§ 6**

Administratorem danych osobowych jest Gabinet dietetyczny DIET-COACHING Patrycja Sankowska, Wałcz ul. Dąbrowskiego 7, NIP 765 163 05 62 e-mail: patrycja@dietetyk-medyczny@gmail.com, tel. 535 513 446

**1.** Administrator danych osobowych nie wyznaczył inspektora ochrony danych osobowych świadomie, stwierdzając, że nie ciąży na nim taki obowiązek na podstawie art. 37 RODO.

**2.** Administrator danych osobowych nie wyznaczył administratora systemów informatycznych i wszelkie jego obowiązki wykonuje samodzielnie.

## Rozdział II
## Zakres stosowania

**§ 7**

Polityka bezpieczeństwa zawiera informacje dotyczące wprowadzonych zabezpieczeń technicznych i organizacyjnych zapewniających ochronę przetwarzanych danych osobowych.

**§ 8**

Politykę bezpieczeństwa stosuje się w szczególności do:

1) danych osobowych przetwarzanych w formie papierowej,
2) danych osobowych przetwarzanych w systemach informatycznych,
3) informacji dotyczących zabezpieczenia danych osobowych, w tym w szczególności nazw kont i haseł w systemach przetwarzania danych osobowych,
4) rejestru osób dopuszczonych do przetwarzania danych osobowych,
5) innych dokumentów zawierających dane osobowe.

**§ 9**

**1.** Zakresy ochrony danych osobowych określone przez niniejszą politykę mają zastosowanie do systemów informatycznych, w których są przetwarzane dane osobowe, a w szczególności do:

1) wszystkich istniejących, wdrażanych obecnie lub w przyszłości systemów informatycznych, w których przetwarzane są dane osobowe podlegające ochronie,
2) wszystkich lokalizacji – budynków i pomieszczeń, w których są lub będą przetwarzane informacje podlegające ochronie,
3) wszystkich pracowników, zleceniobiorców, wykonawców umów o dzieło, wykonawców umów o świadczenie usług, praktykantów, stażystów i innych osób mających dostęp do informacji podlegających ochronie.

**2.** Do stosowania zasad określonych przez Politykę bezpieczeństwa zobowiązani są wszyscy pracownicy, zleceniobiorcy, wykonawcy umów o dzieło, wykonawcy umów o świadczenie usług, praktykanci, stażyści i inne osoby mające dostęp do informacji podlegających ochronie.

**3.** Polityka bezpieczeństwa nie dotyczy podmiotów zewnętrznych, które przetwarzają dane osobowe powierzone im do przetwarzania przez administratora danych osobowych na podstawie stosownych umów powierzenia. Podmioty te stosują własne procedury i środki bezpieczeństwa związane z ochroną danych osobowych wymagane przez przepisy prawa, do czego zobowiązały się w ramach zawartych umów powierzenia przetwarzania danych osobowych.

## Rozdział III
## Opis działalności administratora danych osobowych, obszar przetwarzania danych osobowych i sprzęt wykorzystywany do przetwarzania danych osobowych

**§ 10**

1. Administrator danych osobowych prowadzi działalność gospodarczą, w związku z czym dochodzi do przetwarzania danych osobowych.
2. Dane osobowe przetwarzane są zarówno w formie elektronicznej, jak i papierowej.

**§ 11**

1. Dane osobowe przetwarzane są w obrębie siedziby administratora danych osobowych. Siedziba znajduje się pod następującym adresem: Wałcz ul. Dąbrowskiego 7. Siedziba znajduje się w wynajmowanym lokalu użytkowym o powierzchni 20 $m^2$. W lokalu znajduje się alarm przeciwwłamaniowy.
2. Dane osobowe w formie papierowej przechowywane są w obrębie siedziby administratora danych osobowych.

3. Dane osobowe w formie elektronicznej przetwarzane są w obrębie siedziby administratora danych osobowych, ale mogą być przetwarzane z dowolnego miejsca i w dowolnym czasie, ponieważ przetwarzanie odbywa się z wykorzystaniem komputerów oraz innych urządzeń przenośnych. Ponadto, przetwarzanie odbywa się w ramach systemów informatycznych, instalowanych lokalnie na komputerach oraz takich, do których dostęp następuje on-line, a systemy te nie są zainstalowane lokalnie na komputerach.
4. Ponieważ administrator danych osobowych powierza przetwarzanie danych osobowych podmiotom trzecim, do przetwarzania danych osobowych dochodzi również w innych lokalizacjach, ale w tym zakresie czynności przetwarzania dokonuje podmiot trzeci lub ewentualnie podmioty do tego przez niego upoważnione. Administrator danych osobowych nie ma szczegółowej wiedzy na temat lokalizacji, w obrębie których dochodzi do przetwarzania danych przez podmioty, którym powierzył przetwarzanie danych osobowych, ale podmioty te zobowiązały się do stosowania odpowiednich środków ochrony i bezpieczeństwa danych osobowych wymaganych przez przepisy prawa.
5. Odpowiednie środki ochrony danych osobowych zostały wdrożone w lokalizacji, o której mowa w ust. 1 powyżej oraz na urządzeniach wykorzystywanych do przetwarzania danych osobowych. Jeżeli chodzi o podmioty, którym administrator powierzył przetwarzanie danych osobowych, oświadczyły one, że wdrożyły odpowiednie środki ochrony i bezpieczeństwa danych osobowych wymagane przez przepisy prawa i zobowiązały się je utrzymywać przez okres powierzenia przetwarzania danych.

**§ 12**

**1.** Dane osobowe przetwarzane są przy wykorzystaniu komputerów przenośnych oraz smartfonów.

**2.** Przetwarzanie danych przy wykorzystaniu wskazanych powyżej urządzeń polega na tym, że następuje z nich logowanie do systemów, w ramach których przetwarzane są dane osobowe. Dostęp do komputera i smartfonów jest chroniony hasłem. Dane są również przechowywane na dyskach komputerów.

## Rozdział IV
## Środki techniczne i organizacyjne zabezpieczenia danych

**§ 13**

**1.** W celu zapewnienia odpowiedniego poziomu ochrony danych osobowych wprowadzono zabezpieczenia organizacyjne i techniczne.

**2.** Zabezpieczenia organizacyjne:

**1)** sporządzono i wdrożono politykę ochrony danych osobowych,

**2)** sporządzono i wdrożono instrukcję zarządzania systemami informatycznymi,

**3)** do przetwarzania danych osobowych zostały dopuszczone wyłącznie osoby posiadające upoważnienia nadane przez administratora danych osobowych,

4) osoby zatrudnione przy przetwarzaniu danych zostały zaznajomione z przepisami dotyczącymi ochrony danych osobowych oraz w zakresie zabezpieczeń systemu informatycznego,

5) osoby zatrudnione przy przetwarzaniu danych osobowych obowiązane zostały do zachowania ich w tajemnicy,

6) dane osobowe przetwarzane są w warunkach zabezpieczających dane przed dostępem osób nieupoważnionych,

7) dane osobowe w formie papierowej przechowywane są w zamkniętej, niemetalowej szafce;

8) dokumenty zawierające dane osobowe są po ustaniu przydatności niszczone z wykorzystaniem niszczarek,

9) lokalizacja, w której przechowywane są zbiory danych osobowych w formie papierowej zabezpieczona jest na wypadek pożaru poprzez wyposażenie pomieszczenia w gaśnice,

10) monitory komputerów, na których przetwarzane są dane osobowe ustawione są w sposób uniemożliwiający wgląd osobom postronnym w przetwarzane dane.

11) kopie zapasowe/archiwalne zbioru danych osobowych przechowywane są w zamkniętej niemetalowej szafce.

**3.** Zabezpieczenia techniczne:

1) zastosowano środki ochrony przed szkodliwym oprogramowaniem,

2) zastosowano uwierzytelnienie z wykorzystaniem identyfikatora użytkownika oraz hasła przy dostępie do zbioru danych,

3) zastosowano uwierzytelnienie z wykorzystaniem identyfikatora użytkownika oraz hasła przy starcie systemu operacyjnego komputera,

4) zastosowano systemowe środki pozwalające na określenie odpowiednich praw dostępu do zasobów informatycznych,

5) zastosowano środki umożliwiające określenie praw dostępu do wskazanego zakresu danych w ramach przetwarzanego zbioru danych osobowych,

6) zastosowano mechanizm automatycznego wylogowania użytkownika po określonym czasie braku aktywności.

**4.** Wskazane powyżej środki techniczne i organizacyjne zabezpieczenia danych dotyczą wyłącznie środków wdrożonych bezpośrednio przez administratora danych osobowych. W zakresie, w jakim administrator danych osobowych powierzył przetwarzanie danych osobowych innym podmiotom, podmioty te zobowiązały się utrzymywać odpowiednie środki ochrony danych osobowych wymagane przez przepisy prawa.

## Rozdział V
## Zadania administratora danych osobowych i administratora systemu informatycznego

**§ 14**

1. Do najważniejszych obowiązków administratora danych osobowych należy:
   1) organizacja bezpieczeństwa i ochrony danych osobowych zgodnie z wymogami obowiązujących przepisów prawa,
   2) zapewnienie przetwarzania danych zgodnie z uregulowaniami niniejszej polityki,
   3) wydawanie i anulowanie upoważnień do przetwarzania danych osobowych,
   4) prowadzenie ewidencji osób upoważnionych do przetwarzania danych osobowych,
   5) prowadzenie postępowania wyjaśniającego w przypadku naruszenia ochrony danych osobowych i zgłoszenie faktu naruszenia organowi nadzorczemu oraz zawiadomienie o tym osobę, której dane dotyczą,
   6) nadzór nad bezpieczeństwem danych osobowych,
   7) inicjowanie i podejmowanie przedsięwzięć w zakresie doskonalenia ochrony danych osobowych,
   8) przeprowadzanie szkoleń użytkowników zgodnie z ust. 2, 3, 4, 5 poniżej.
2. Każdy użytkownik, za wyjątkiem administratora danych osobowych, przed dopuszczeniem do pracy z systemem informatycznym przetwarzającym dane osobowe lub zbiorami danych osobowych w wersji papierowej winien być poddany przeszkoleniu w zakresie ochrony danych osobowych w zbiorach elektronicznych i papierowych.
3. Zakres szkolenia powinien obejmować zaznajomienie użytkownika z obowiązującymi przepisami prawa w zakresie ochrony danych osobowych oraz z instrukcjami obowiązującymi u administratora danych osobowych.

**§ 15**

**1.** Administratorem systemu informatycznego jest osoba określona przez administratora danych osobowych. Powołanie administratora systemu informatycznego dokonywane jest w formie pisemnej. Jeżeli administrator systemu informatycznego nie zostanie powołany, jego zadania wykonuje administrator danych osobowych.

**2.** Administrator systemu informatycznego odpowiedzialny jest za:
   1) bieżący monitoring i zapewnienie ciągłości działania komputerów i innych urządzeń wykorzystywanych do przetwarzania danych osobowych oraz systemów operacyjnych,
   2) optymalizację wydajności komputerów i innych urządzeń wykorzystywanych do przetwarzania danych osobowych oraz systemów operacyjnych,
   3) instalację i konfiguracje sprzętu sieciowego i serwerowego,
   4) instalację i konfigurację oprogramowania systemowego, sieciowego,
   5) konfigurację i administrowanie oprogramowaniem systemowym, sieciowym oraz zabezpieczającym dane chronione przed nieupoważnionym dostępem,
   6) nadzór nad zapewnieniem awaryjnego zasilania komputerów oraz innych urządzeń mających wpływ na bezpieczeństwo przetwarzania danych,

7) współpracę z dostawcami usług oraz sprzętu sieciowego i serwerowego,

8) zarządzanie kopiami awaryjnymi konfiguracji oprogramowania systemowego, sieciowego,

9) zarządzanie kopiami awaryjnymi danych osobowych oraz zasobów umożliwiających ich przetwarzanie,

10) przeciwdziałanie próbom naruszenia bezpieczeństwa informacji,

11) przyznawanie na wniosek administratora danych osobowych ściśle określonych praw dostępu do informacji w danym systemie,

12) wnioskowanie do administratora danych osobowych w sprawie zmian lub usprawnienia procedur bezpieczeństwa i standardów zabezpieczeń,

13) zarządzanie licencjami, procedurami ich dotyczącymi,

14) prowadzenie profilaktyki antywirusowej.

**3.** Praca administratora systemu informatycznego jest nadzorowana przez administratora danych osobowych, chyba, że administrator danych osobowych nie powołał administratora systemu informatycznego – wtedy jego zadania realizuje samodzielnie administrator danych osobowych.

## Rozdział VI
## Zgłaszanie i zawiadamianie o naruszeniu ochrony danych osobowych

### § 16

**1.** Każde naruszenie ochrony danych osobowych powinno być niezwłocznie zgłaszane przez użytkowników administratorowi danych osobowych. Szczegóły w zakresie postępowania w związku ze stwierdzonym naruszeniem ochrony danych osobowych przy korzystaniu z systemów informatycznych opisane zostały w Instrukcji zarządzania systemami informatycznymi służącymi do przetwarzania danych osobowych.

**2.** Administrator danych osobowych dokumentuje wszelkie naruszenia ochrony danych osobowych, w tym okoliczności naruszenia, jego skutki oraz podjęte środki zaradcze. Dokumentacja odbywa się z wykorzystaniem zestawienia incydentów naruszenia ochrony danych osobowych.

**3.** W przypadku naruszenia ochrony danych osobowych, na administratorze danych osobowych ciąży obowiązek zgłoszenia tego faktu do organu nadzorczego zgodnie z postanowieniami art. 33 RODO oraz zawiadomienia osoby, której dane dotyczą, zgodnie z postanowieniami art. 34 RODO.

## Rozdział VII
## Postanowienia końcowe

### § 17

1. Administrator danych osobowych ma obowiązek zapoznać z treścią niniejszej polityki każdego użytkownika.
2. Użytkownicy zobowiązani są do stosowania przy przetwarzaniu danych osobowych postanowień zawartych w niniejszej polityce.