

Polityka bezpieczeństwa  
danych osobowych przetwarzanych w ramach Programy BIOSfera BIODERMA

**Polityka bezpieczeństwa**  
danych osobowych przetwarzanych w ramach Programu  
BIOSfera BIODERMA

## I. CZĘŚĆ OGÓLNA

### 1. Podstawa prawna:

- a) Ustawa z dnia 29 sierpnia 1997 r. o ochronie danych osobowych. (tekst jednolity: Dz. U. 2002 r. Nr 101 poz. 926, ze zm.),
- b) Rozporządzenie 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. Nr. 100, poz. 1024).

### 2. Definicje:

- dane osobowe - są to wszelkie informacje dotyczące zidentyfikowanej lub możliwej do zidentyfikowania osoby fizycznej. Osoba możliwa do zidentyfikowania jest osoba, której tożsamość można określić bezpośrednio lub pośrednio, w szczególności przez powołanie się na numer identyfikacyjny (np. PESEL, NIP) albo jeden lub kilka specyficznych czynników określających jej cechy fizyczne, fizjologiczne, umysłowe, ekonomiczne, kulturowe lub społeczne (zgodnie z art.6 ust.1 i ust.2 ustawy z dnia 29 sierpnia 1997 r. o ochronie danych osobowych, Dz. U. 2002/101/926 - tekst jednolity z późniejszymi zm.).
- zbiór danych - to każdy posiadający strukturę zestaw danych o charakterze osobowym, dostępny według określonych kryteriów;
- system informatyczny - to zespół współpracujących ze sobą urządzeń, programów, procedur przetwarzania informacji i narzędzi programowych, a w szczególności stanowisk roboczych (pojedynczych komputerów) zastosowanych w celu przetwarzania danych;
- administratorzy danych osobowych - rozumie się przez to dyrektora firmy lub osobę uprawnioną przez dyrektora firmy do przetwarzania danych osobowych
- administrator systemu –osoba lub osoby upoważnione przez administratora danych osobowych do administrowania i zarządzania systemem
- identyfikator użytkownika (login) - ciąg znaków literowych, cyfrowych lub innych jednoznacznie identyfikujący osobę upoważnioną do przetwarzania danych osobowych w systemie informatycznym;
- hasło - to ciąg znaków literowych, cyfrowych lub innych, znany jedynie osobie uprawnionej do pracy w systemie informatycznym;
- publiczna sieć telekomunikacyjna – to sieć telekomunikacyjna wykorzystywana głównie do świadczenia publicznie dostępnych usług telekomunikacyjnych;
- administrator dostępu do Internetu - osoba przygotowująca i wdrażająca koncepcję podłączenia sieci lokalnej do sieci internet, administrująca serwerem i innymi urządzeniami wykorzystanymi w realizacji dostępu do sieci internet w firmie;
- administrator bezpieczeństwa informacji – osoba lub osoby upoważnione i odpowiedzialne za przestrzeganie ustawy o ochronie danych osobowych.
- przetwarzanie danych - to wszelkie operacje wykonywane na danych i ich zbiorach, a w szczególności zbieranie, utrwalanie, przechowywanie, opracowywanie, zmienianie, udostępnianie i usuwanie.

### 3. Celem polityki bezpieczeństwa danych osobowych jest:

- zapewnienie ochrony danych osobowych,
- przeciwdziałanie realnym i identyfikowalnym zagrożeniom bezpieczeństwa danych osobowych,
- wdrożenie i realizacja określonych procedur przetwarzania, przechowywania i udostępniania danych osobowych,

4. Na politykę bezpieczeństwa danych osobowych składają się:
  - identyfikowanie i analizowanie zagrożeń oraz ocena ryzyka ich wystąpienia, stosowanie odpowiednich zabezpieczeń danych osobowych przed zidentyfikowanymi i potencjalnymi zagrożeniami,
  - monitorowanie wdrażania i działania systemu zabezpieczeń,
  - prowadzenie dokumentacji dotyczącej ewidencji systemów i istotnych czynności administracyjnych wykonywanych w systemach informatycznych oraz innych czynności związanych z obsługą zasobów informacyjnych i informatycznych zawierających dane osobowe, w szczególności prowadzenie ewidencji osób upoważnionych do przetwarzania danych osobowych.
  - określenie sposobów reakcji w przypadku naruszenia polityki bezpieczeństwa.
5. Deklaracja kierownictwa
  - Dyrektor Generalna NAOS Poland Sp. Z o.o. angażuje się w rozwój i wdrożenie systemu bezpieczeństwa danych osobowych posiadanych przez NAOS Poland Sp. Z o.o., oraz deklaruje pracę nad stałym doskonaleniem niniejszej polityki.
  - Ponadto ustanowiono niniejszą politykę, której znajomość stanowi obowiązek każdego pracownika NAOS Poland Sp. Z o.o.
  - W celu zapewnienia bezpieczeństwa przetwarzanych danych wymaga się, aby wszyscy jego użytkownicy byli świadomi konieczności ochrony wykorzystywanych zasobów. Konsekwencja nie stosowania przez pracownika środków bezpieczeństwa określonych w instrukcjach wewnętrznych może być zniszczenie części lub całości systemów informatycznych, utrata poufności, autentyczności, straty finansowe, jak również utrata wizerunku.
  - Pracownicy są odpowiedzialni za bezpieczeństwo danych, do których mają dostęp. W szczególności w systemach informatycznych odpowiadają oni za poprawne wprowadzanie informacji do tych systemów oraz za użycie, zniszczenie lub uszkodzenie sprzętu oraz znajdujących się na nim danych i oprogramowania.

## II. CZĘŚĆ SZCZEGÓŁOWA

1. Wykaz pomieszczeń tworzących obszar, w którym przetwarzane są dane osobowe:
  - Biuro
2. Kopie zapasowe zbiorów danych będą przechowywane w Biurze, w szafce zamykanej na klucz.
3. Wykaz zbiorów danych osobowych:
  - Program BIOSfera – rejestracja. Do przetwarzania danych osobowych zawartych w tym zbiorze służy program BIOSfera BIODERMA stworzony na zlecenie firmy NAOS Poland SP. Z o.o. oraz serwis SalesMANAGO. Przetwarzanie odbywać się będzie na komputerze osoby upoważnionej do przetwarzania danych osobowych.
4. Opis struktury zbiorów:
  - BIOSfera societe – rejestracja: załącznik nr 1 do Polityki Bezpieczeństwa
  - BIOSfera societe – dane konta: załącznik nr 2 do Polityki Bezpieczeństwa
  - BIOSfera pharmacien – rejestracja: załącznik nr 3 do Polityki Bezpieczeństwa
  - BIOSfera pharmacien – dane konta: załącznik nr 4 do Polityki Bezpieczeństwa
  - PharmaGame– rejestracja: załącznik nr 5 do Polityki Bezpieczeństwa
  - PharmaGame– dane konta: załącznik nr 6 do Polityki Bezpieczeństwa

## 5. Sposób przepływu danych pomiędzy systemami

- Dane osobowe zgłaszane poprzez stronę internetową [www.klub-biosfera.pl](http://www.klub-biosfera.pl) lub [www.pharmagame.pl](http://www.pharmagame.pl). Użytkownik wypełnia formularz rejestracyjny na stronie [www.klub-biosfera.pl](http://www.klub-biosfera.pl) lub [www.pharmagame.pl](http://www.pharmagame.pl). Po akceptacji wysłania informacji, dane podane przez użytkownika są przesłane do bazy danych na serwerze należącym do firmy Poliman i zapisane w bazie mySQL oraz przesłane jest potwierdzenie na adres mailowy Bioderma, do którego dostęp mają upoważnione osoby. Dane są przechowywane w tej bazie oraz importowane do serwisu Sales Manago, gdzie podlegają przetwarzaniu i są wykorzystywane do komunikacji mailowej i smsowej.

## 6. Określenie środków technicznych i organizacyjnych niezbędnych dla zapewnienia poufności, integralności i rozliczalności danych:

- Pomieszczenia w obszarze bezpieczeństwa są zamykane w sposób uniemożliwiający dostęp do nich osób nieuprawnionych.
- Klucze do pomieszczeń posiadają tylko osoby zatrudnione w firmie na podstawie stosunku pracy.
- Przebywanie w pomieszczeniach w obszarze bezpieczeństwa osób nieuprawnionych do dostępu do danych osobowych jest dopuszczalne tylko w obecności osoby upoważnionej do dostępu do tych danych.
- Prace związane z zarządzaniem systemami informatycznymi mogą wykonywać jedynie wyznaczeni administratorzy tych systemów lub upoważnieni przez dyrektora firmy inni pracownicy w obecności administratora systemu.
- Każda osoba dopuszczona do pracy przy przetwarzaniu danych osobowych:
  - potwierdza własnoręcznym podpisem znajomość ustawy o ochronie danych osobowych; zarządzenie określające politykę bezpieczeństwa oraz instrukcję określającą sposób postępowania w przypadku naruszenia bezpieczeństwa,
  - posiada własny unikalny identyfikator (login i hasło) umożliwiający do zalogowania się do stacji roboczej (komputera), na którym będą przetwarzane dane osobowe,
    - Do pracy z systemami informatycznymi dopuszczani są jedynie osoby upoważnione posiadające indywidualny identyfikator użytkownika i osobiste hasło.
    - Administrator systemu zmienia główne hasła do systemów informatycznych najdalej co 30 dni.
    - Zabrania się zapisywania i przechowywania identyfikatorów i haseł w miejscach ogólnie dostępnych.
    - Każda osoba przetwarzająca dane ponosi odpowiedzialność wynikającą z zakresu jego czynności, w szczególności za zniszczenie, nieprawidłową modyfikację, udostępnienie danych osobom trzecim, prawidłowe konstruowanie i terminową zmianę haseł.
    - Zarejestrowania i wyrejestrowania użytkowników systemów informatycznych służących do przetwarzania danych osobowych dokonują administratorzy tych systemów po akceptacji formalnej administratora bezpieczeństwa informacji.
    - Administrator systemu prowadzi ewidencję nadanych indywidualnych identyfikatorów użytkowników zawierającą nazwę użytkownika, jego identyfikator, datę nadania oraz datę wycofania.
    - Administrator systemu prowadzi dziennik systemu zawierający informacje o pracy systemu i wykonywanych w nim informatycznych istotnych czynnościach administracyjnych.
    - Administrator systemu wykonuje kopie awaryjne w cyklu dwutygodniowym i przechowuje w zamkniętej szafie na klucz. Kopie są przechowywane przez okres odpowiadający rodzajowi kopii.
    - Administrator systemu przeprowadza okresowe kontrole zasobów informatycznych, nie rzadziej niż raz na tydzień, programami antywirusowymi. W przypadku wykrycia

Polityka bezpieczeństwa danych osobowych przetwarzanych w ramach Programy BIOSfera BIODERMA wirusa powiadamia administratora bezpieczeństwa informacji i usuwa wirusa posiadanym programem.

- Zewnętrzne nośniki danych są przed ich użyciem sprawdzane programem antywirusowym.
- Wgrywanie jakiegokolwiek oprogramowania do systemów informatycznych, na których przetwarzane są dane osobowe, jest możliwe tylko przez administratora systemu lub za jego wiedzą i po akceptacji formalnej administratora bezpieczeństwa informacji.
- Zasoby informacyjne oraz nośniki z danymi podlegają szczególnej ochronie przed kradzieżą, modyfikacją zawartości, podglądnięciem i kopiowaniem.
- Zasoby informacyjne, w szczególności wydruki zawierające dane osobowe oraz nośniki z danymi, przechowywane są w warunkach uniemożliwiających dostęp do nich osobom niepowołanym. O ile jest to niezbędne do bieżącej pracy lub wykonywania zleconego zadania, dopuszcza się ich przechowywanie w szafkach biurowych znajdujących się w strefie bezpieczeństwa.
- Zasoby informacyjne, w szczególności wydruki, które zawierają dane osobowe i są przeznaczone do usunięcia należy zniszczyć za pomocą niszczarki dokumentów.
- Przeznaczone do naprawy urządzenia lub nośniki danych zawierające dane osobowe pozbawia się przed naprawą danych osobowych albo naprawia się je pod nadzorem administratora systemu lub osoby upoważnionej przez dyrektora firmy.
- Zawierające dane osobowe urządzenia lub nośniki danych przeznaczone do przekazania odbiorcy nieuprawnionemu do otrzymania danych osobowych przed przekazaniem pozbawia się zapisu tych danych w sposób uniemożliwiający ich odtworzenie.
- Przeznaczone do likwidacji urządzenia lub nośniki danych zawierające dane osobowe, administrator systemu w obecności administratora bezpieczeństwa informacji pozbawia wcześniej zapisu tych danych w sposób uniemożliwiający ich odtworzenie, a gdy nie jest to możliwe, uszkadza się w sposób uniemożliwiający ich odtworzenie. Fakt dokonania likwidacji potwierdza się protokołem.

#### 7. Sposoby reakcji w przypadku naruszenia polityki bezpieczeństwa:

- Administrator bezpieczeństwa nadzoruje przestrzeganie polityki bezpieczeństwa.
- W przypadku stwierdzenia naruszenia przestrzegania polityki bezpieczeństwa administrator bezpieczeństwa niezwłocznie powiadamia o tym fakcie administratora systemu i dyrektora firmy, oraz podejmuje kroki do przywrócenia stanu pierwotnego zgodnego z przyjętą polityką bezpieczeństwa.

Załącznik nr 1 do Polityki Bezpieczeństwa: formularz rejestracyjny do BIOSfera societé



POZNAJ SFERĘ WYJĄTKOWYCH MOŻLIWOŚCI

- ✓ Dostęp do **wiedzy** o skórze i jej problemach
- ✓ **Rabaty i promocje**, a za każde 5 produktów Bioderma, 1 produkt w prezencie



- ✓ **BIOSfera élité** - jeszcze więcej korzyści i promocji!

ZALOGUJ SIĘ PRZEZ FACEBOOK

Nie publikujemy niczego bez Twojej zgody

lub

ZAREJESTRUJ SIĘ

MĘŻCZYZNA  KOBIETA

Wyrażam zgodę na przetwarzanie podanych danych osobowych przez NAOS Poland Sp. z o.o. z siedzibą w Krakowie 30-703, ul. Dekerta 24 dla celów marketingowych. Podanie danych osobowych jest dobrowolne. Mam prawo dostępu do treści swoich danych osobowych i prawo do ich poprawiania.

Wyrażam zgodę na otrzymanie od NAOS Poland Sp. z o.o. informacji handlowej za pomocą środków komunikacji elektronicznej.

Bioderma BIOSfera polityka prywatności

ZAREJESTRUJ SIĘ

Załącznik nr 2 do Polityki Bezpieczeństwa - dane konta BIOSfera societé:




**39**

AKTYWNOŚĆ

WIEDZA

DEKETA

ROZUMIEM

IDENTYT

**PROFIL**

[en.sungrow@bioderma.com](mailto:en.sungrow@bioderma.com)

**Imię** \_\_\_\_\_ ✓

**Surno** \_\_\_\_\_ ✓

**DATA URODZENIA** 29/12/1971 ✓

**SEX**  K  M ✓

**DATA WYBRANIA**  ✓

**PROFIL DOKUMENT**  SI  SI  SI ✓

**SKŁÓCZKA**  ✓

Zapisz

100%

TWOJA PRACA  
JEST WARTOŚCIOWA

PRACUJ, UŚMIECHAJ SIĘ

UŁOŻYMY DLA CIĘ PROFIL  
 Z DOSTĘPNYMI WARIANTAMI DLA TWOJEGO TYPU SKÓRY  
 I PRACUJ, UŚMIECHAJ SIĘ

**TWÓJ TYPI SKÓRY**

**WYBRANA SKÓRA**



PRACUJ, UŚMIECHAJ SIĘ  
 WARTOŚCIOWO  
 WARTOŚCIOWO  
 WARTOŚCIOWO

PRZECIĄGNIJ WYBRANY TYPI SKÓRY, MAX 3.

WYBRANA SKÓRA	WYBRANA SKÓRA	WYBRANA SKÓRA
SI	SI	SI
SI	SI	SI
SI	SI	SI

\*Wybór skłócy jest dobrowolny i nie ma wpływu na dostępną ofertę.  
 \*\*Wybór skłócy jest dobrowolny i nie ma wpływu na dostępną ofertę.

**JAK WOLISZ SPĘDZAĆ SWÓJ WOLNY CZAS?**

w domu w rodzinie / z dziećmi

w pracy / w szkole / w instytucjach

w klubie / w grupie

w domu, w rodzinie / z dziećmi

w klubie / w grupie / w instytucjach

inne

na samodzielnym / w klubie / w grupie

w pracy / w szkole / w instytucjach

**ADRES DO KORESPONDENCJI**

Imię i nazwisko / Nazwa \_\_\_\_\_ ✓

Ulica / Adres \_\_\_\_\_ ✓

00-0000 \_\_\_\_\_ ✓

00-0000 \_\_\_\_\_ ✓

00-0000 \_\_\_\_\_ ✓

00-0000 \_\_\_\_\_ ✓

Polityka bezpieczeństwa  
danych osobowych przetwarzanych w ramach Programu BIOsfera BIODERMA  
Załącznik nr 3 do Polityki Bezpieczeństwa – rejestracja do Programu BIOsfera farmacji:

## BIOsfera) farmacji

### FORMULARZ REJESTRACYJNY

**Apteka**

Dolnośląskie

Bielawa

APTEKA CENTRUM ZDROWIA ul. Wolności Bielawa

Numer licencji apteki

Numer ID KAMSOFIT

Zarejestruj mnie także do Pharmagame

**Dane uczestnika programu**

Imię

Nazwisko

Email

Informujemy, że dane osobowe Uczestników będą przetwarzane w celu przeprowadzenia Programu BIOsfera farmacji. Administratorem danych osobowych jest NAOS Poland Sp. z o.o., z siedzibą w Krakowie 30-703, ul. Dekerta 24. Podanie danych jest dobrowolne, ale niezbędne do wzięcia udziału w Programie. Uczestnikowi przysługuje prawo dostępu do treści jego danych osobowych i prawo ich poprawiania.

- Zgłaszam swój udział w organizowanym przez NAOS Poland Programie BIOsfera farmacji i akceptuję zasady oraz regulamin Programu.
- Wyrażam zgodę na przetwarzanie podanych danych osobowych przez NAOS Poland Sp. z o.o., z siedzibą w Krakowie 30-703, ul. Dekerta 24 dla celów marketingowych. Podanie danych osobowych jest dobrowolne. Mam prawo dostępu do treści swoich danych osobowych i prawo do ich poprawiania.
- Wyrażam zgodę na otrzymywanie od NAOS Poland Sp. z o.o. informacji handlowej za pomocą środków komunikacji elektronicznej.

**ZAREJESTRUJ SIĘ**

Po wypełnieniu formularza na Pani/Pana adres e-mail zostanie przesłany link aktywacyjny, login i hasło.

Załącznik nr 4 do Polityki Bezpieczeństwa – dane konta BIOsfera farmacji:



Załącznik nr 5 do Polityki Bezpieczeństwa– rejestracja do Programu PharmaGame:

**FORMULARZ REJESTRACYJNY**

**Apteka**

Działalność

Bielszwa

APTEKA CENTRUM ZDROWIA ul. Wolności Bielszwa

Numer identyfikacji apteki

Zarejestruj mnie także do Pharmacieum

**Dane uczestnika programu**

Imię

Nazwisko

Adres e-mail

Informujemy, że dane osobowe Uczestników będą przetwarzane w celu przeprowadzenia Programu PharmaGame. Administratorem danych osobowych jest NAOS Poland Sp. z o.o., z siedzibą w Krakowie 30-703, ul. Dekerta 24. Podanie danych jest dobrowolne, ale niezbędne do wzięcia udziału w Programie. Uczestnikowi przysługuje prawo dostępu do treści jego danych osobowych i prawo ich poprawienia.

Zgadzam się wziąć udział w organizowanym przez NAOS Poland turnieju PharmaGame i akceptuję zasady oraz regulamin gry.

Wyrażam zgodę na otrzymanie od NAOS Poland Sp. z o.o. informacji handlowej za pomocą środków komunikacji elektronicznej.

Wyrażam zgodę na przetwarzanie podanych danych osobowych przez NAOS Poland Sp. z o.o., z siedzibą w Krakowie 30-703, ul. Dekerta 24 dla celów marketingowych. Podanie danych osobowych jest dobrowolne. Mam prawo dostępu do treści swoich danych osobowych i prawo do ich poprawienia.

**ZAREJESTRUJ SIĘ**

Po wypełnieniu formularza na Poczcie/E-mail zostanie przesyłany link aktywacyjny login i hasło.

Załącznik nr 6 do Polityki Bezpieczeństwa– dane konta PharmaGame:

**MÓJ PROFIL**

Ewelina

biodermatest

506184540

Imię i nazwisko, firma

Dekerta

24

Nr lokalu

30-307

Kraków

**ZAPISZ**