Polityka bezpieczeństwa

danych osobowych przetwarzanych w ramach Programu

BIOsfera BIODERMA

LABORATOIRE DERMATOLOGIQUE BIODERMA
NAOS Poland Sp. z o.o.; ul. Dekerta 24; 30-703 Kraków; Tel: (+48) 12 292 00 60; Tel/Fax: (+48) 12 626 31 09, www.bioderma.pl

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,

LABORATOIRE DERMATOLOGIQUE BIODERMA
NAOS Poland Sp. z o.o.; ul. Dekerta 24; 30-703 Kraków; Tel: (+48) 12 292 00 60; Tel/Fax: (+48) 12 626 31 09, www.bioderma.pl

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 maja 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

LABORATOIRE DERMATOLOGIQUE BIODERMA
NAOS Poland Sp. z o.o.; ul. Dekerta 24; 30-703 Kraków; Tel: (+48) 12 292 00 60; Tel/Fax: (+48) 12 626 31 09, www.bioderma.pl

5. Sposób przepływu danych pomiędzy systemami

- Dane osobowe zgłaszane poprzez stronę internetową www.klub-biosfera.pl lub www.pharmagame.pl. Użytkownik wypełnia formularz rejestracyjny na stronie www.klub-biosfera.pl lub 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 zamykanej 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

LABORATOIRE DERMATOLOGIQUE BIODERMA
NAOS Poland Sp. z o.o.; ul. Dekerta 24; 30-703 Kraków; Tel: (+48) 12 292 00 60; Tel/Fax: (+48) 12 626 31 09, www.bioderma.pl

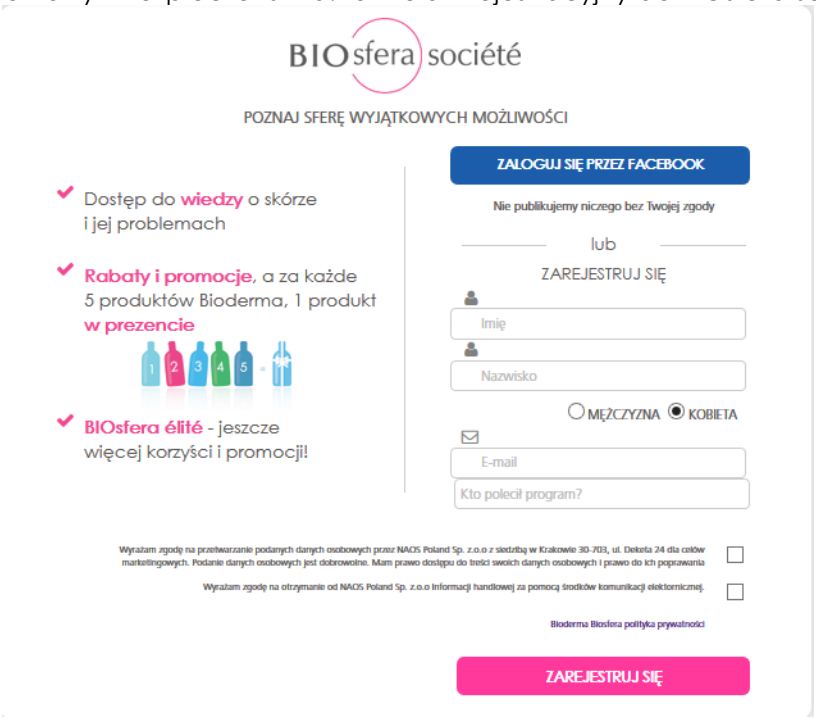
wirusa powiadamia administratora bezpieczeństwa informacji i usuwa wirusa posiadanym programem.

- 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, przechowuje się 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.

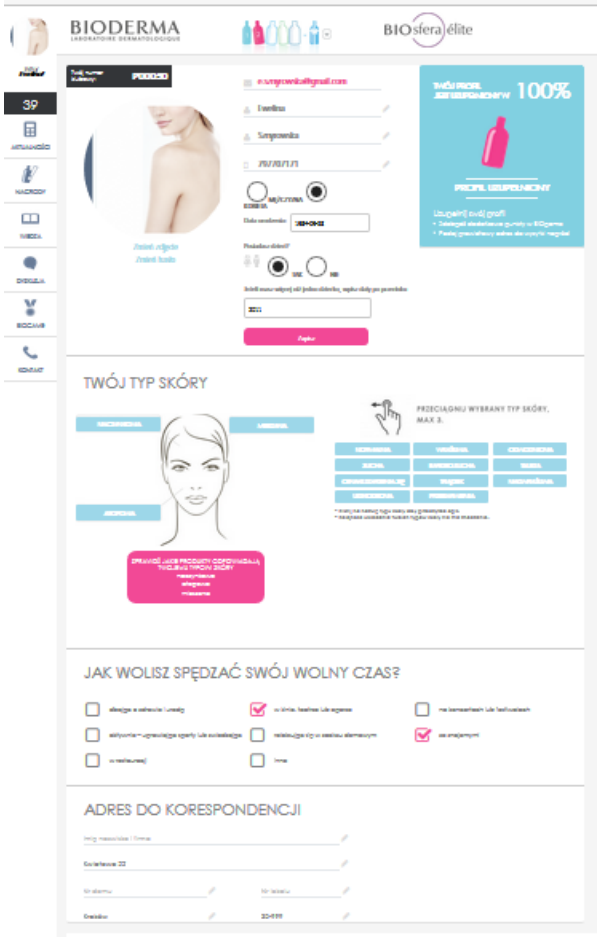
7. Sposoby reakcji w przypadku naruszenia polityki bezpieczeństwa:
   - Administrator bezpieczeństwa nadzoruje przestrzeganie polityki bezpieczeństwa.
   - W przypadku stwierdzenia naruszenia przestrzegania polityki bezpieczeństwa administrator bezpieczeństwa niezwłocznie powiadamia o tym fakcie administratora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

LABORATOIRE DERMATOLOGIQUE BIODERMA
NAOS Poland Sp. z o.o.; ul. Dekerta 24; 30-703 Kraków; Tel: (+48) 12 292 00 60; Tel/Fax: (+48) 12 626 31 09, www.bioderma.pl

Załącznik nr 1 do Polityki Bezpieczeństwa: formularz rejestracyjny do BIOsfera societe

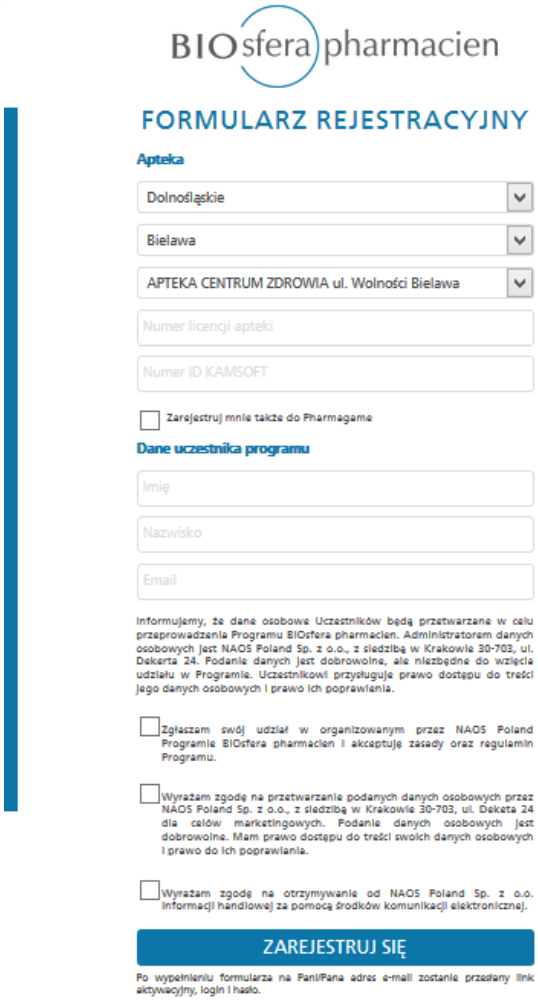


Załącznik nr 2 do Polityki Bezpieczeństwa - dane konta BIOsfera societe:

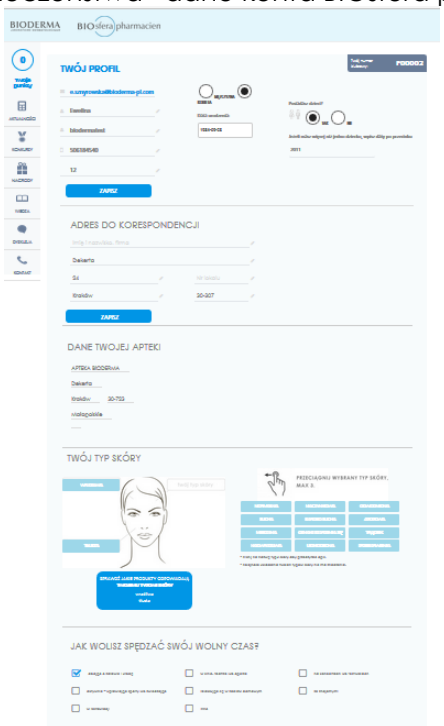


LABORATOIRE DERMATOLOGIQUE BIODERMA
NAOS Poland Sp. z o.o.; ul. Dekerta 24; 30-703 Kraków; Tel: (+48) 12 292 00 60; Tel/Fax: (+48) 12 626 31 09, www.bioderma.pl

Załącznik nr 3 do Polityki Bezpieczeństwa – rejestracja do Programu BIOsfera pharmacien:

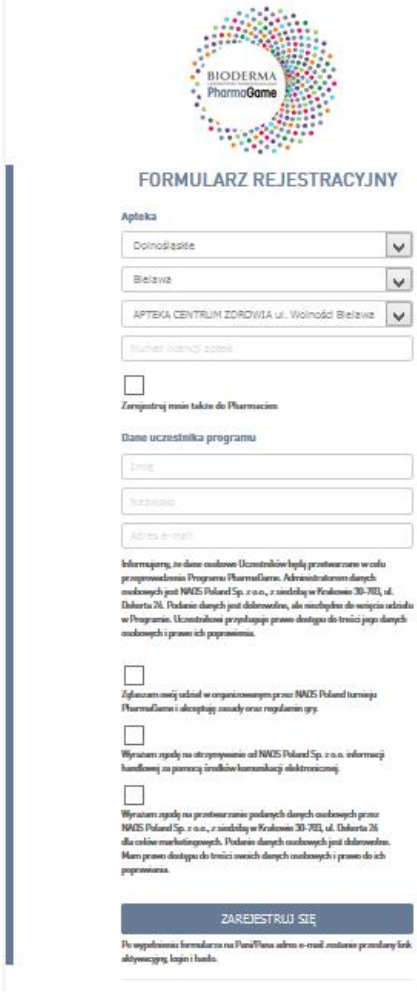


Załącznik nr 4 do Polityki Bezpieczeństwa– dane konta BIOsfera pharmacien:



LABORATOIRE DERMATOLOGIQUE BIODERMA
NAOS Poland Sp. z o.o.; ul. Dekerta 24; 30-703 Kraków; Tel: (+48) 12 292 00 60; Tel/Fax: (+48) 12 626 31 09, www.bioderma.pl

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



Załącznik nr 6 do Polityki Bezpieczeństwa– dane konta PharmaGame:

LABORATOIRE DERMATOLOGIQUE BIODERMA
NAOS Poland Sp. z o.o.; ul. Dekerta 24; 30-703 Kraków; Tel: (+48) 12 292 00 60; Tel/Fax: (+48) 12 626 31 09, www.bioderma.pl