Eyelid Sp. z o.o.
Łysakówek 83a, 39-305 Borowa
NIP 8172211684 REG. 525916920

Polityka Ochrony Danych Osobowych

EYELID SPÓŁKA Z OGRANICZONĄ ODPOWIEDZIALNOŚCIĄ
KRS: 0001048715
NIP: 8172211684
REGON: 525916920
adres siedziby: Łysakówek 83A, 39-305 Borowa
RPWDL: 000000265784
wersja: 1.1
data przyjęcia: 01.03.2024
data wejścia w życie: 01.03.2024

Niniejsza Polityka Ochrony Danych Osobowych określa zasady przetwarzania danych osobowych przez **EYELID SPÓŁKĘ Z OGRANICZONĄ ODPOWIEDZIALNOŚCIĄ** z siedzibą w Łysakówku, wpisaną do rejestru przedsiębiorców KRS pod numerem 0001048715, NIP 8172211684, REGON 525916920, prowadzącą działalność leczniczą jako podmiot wpisany do rejestru podmiotów wykonujących działalność leczniczą pod numerem 000000265784. Polityka uwzględnia specyfikę podmiotu wykonującego działalność leczniczą, w tym działalność Centrum Okulistycznego Eyelid w Mielcu przy ul. Solskiego 1, oraz wytyczne wynikające z zatwierdzonego przez Prezesa UODO Kodeksu postępowania dla sektora ochrony zdrowia.

§ 1. Cel i zakres polityki

1. Celem Polityki jest zapewnienie zgodnego z prawem, rzetelnego i bezpiecznego przetwarzania danych osobowych przez EYELID SPÓŁKĘ Z OGRANICZONĄ ODPOWIEDZIALNOŚCIĄ, zwaną dalej „Spółką" albo „Administratorem".
2. Polityka ma zastosowanie do wszystkich procesów przetwarzania danych osobowych realizowanych przez Spółkę, niezależnie od formy ich utrwalenia, w szczególności w systemach informatycznych, Elektronicznej Dokumentacji Medycznej, poczcie elektronicznej, dokumentacji papierowej, rejestrach, formularzach i nośnikach danych.
3. Polityka obejmuje dane osobowe pacjentów, przedstawicieli ustawowych pacjentów, osób upoważnionych przez pacjentów, personelu medycznego, pracowników, współpracowników, kandydatów do pracy, kontrahentów oraz innych osób, których dane są przetwarzane przez Spółkę.
4. Polityka dotyczy przetwarzania danych osobowych w siedzibie Spółki, jednostkach organizacyjnych i miejscach wykonywania działalności leczniczej ujawnionych w dokumentacji organizacyjnej i rejestrowej Spółki, w tym w Centrum Okulistycznym Eyelid w Mielcu.
5. Polityka stanowi dokument nadrzędny wobec procedur szczegółowych dotyczących ochrony danych osobowych obowiązujących u Administratora.

§ 2. Dane Administratora i definicje

1. Administratorem danych osobowych jest **EYELID SPÓŁKA Z OGRANICZONĄ ODPOWIEDZIALNOŚCIĄ** z siedzibą: Łysakówek 83A, 39-305 Borowa, wpisana do rejestru przedsiębiorców KRS pod numerem 0001048715, NIP 8172211684, REGON 525916920, RPWDL 000000265784.

2. Na potrzeby niniejszej Polityki przyjmuje się następujące definicje:

- **RODO** – rozporządzenie Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r.;
- **Administrator** – EYELID SPÓŁKA Z OGRANICZONĄ ODPOWIEDZIALNOŚCIĄ;
- **Dane osobowe** – wszelkie informacje o zidentyfikowanej lub możliwej do zidentyfikowania osobie fizycznej;
- **Dane szczególnej kategorii** – w szczególności dane dotyczące zdrowia, podlegające wzmożonej ochronie;
- **Przetwarzanie** – operacja lub zestaw operacji wykonywanych na danych osobowych, niezależnie od sposobu ich wykonywania;
- **IOD** – Inspektor Ochrony Danych, o ile został wyznaczony przez Administratora zgodnie z obowiązującymi przepisami;
- **Upoważniona osoba** – osoba dopuszczona do przetwarzania danych osobowych przez Administratora w granicach nadanego zakresu dostępu;
- **Incydent / naruszenie ochrony danych** – naruszenie bezpieczeństwa prowadzące do przypadkowego lub niezgodnego z prawem zniszczenia, utracenia, zmodyfikowania, nieuprawnionego ujawnienia lub nieuprawnionego dostępu do danych osobowych;
- **Dokumentacja medyczna** – dokumentacja prowadzona zgodnie z przepisami dotyczącymi praw pacjenta i dokumentacji medycznej.

§ 3. Zasady ogólne przetwarzania danych

1. Spółka przetwarza dane osobowe zgodnie z zasadami określonymi w art. 5 RODO, tj. zgodnie z prawem, rzetelnie i w sposób przejrzysty, w konkretnych i prawnie uzasadnionych celach, w zakresie adekwatnym i niezbędnym, z zachowaniem prawidłowości, ograniczenia przechowywania, integralności, poufności i rozliczalności.
2. Dane osobowe są przetwarzane wyłącznie wtedy, gdy istnieje odpowiednia podstawa prawna, w szczególności obowiązek prawny, wykonanie umowy, realizacja świadczeń zdrowotnych, uzasadniony interes Administratora albo zgoda osoby, której dane dotyczą, jeżeli jest wymagana.
3. Dane dotyczące zdrowia pacjentów są przetwarzane przede wszystkim w związku z udzielaniem świadczeń zdrowotnych, prowadzeniem dokumentacji medycznej, zapewnieniem opieki zdrowotnej i realizacją obowiązków wynikających z przepisów prawa.
4. Administrator wdraża odpowiednie środki techniczne i organizacyjne w celu ochrony danych osobowych, z uwzględnieniem charakteru, zakresu, kontekstu i celów przetwarzania oraz ryzyka naruszenia praw lub wolności osób fizycznych.

§ 4. Role i odpowiedzialności

1. Zarząd Spółki odpowiada za zapewnienie zgodności procesów przetwarzania danych z przepisami prawa oraz za organizację systemu ochrony danych osobowych.
2. Kierownicy komórek organizacyjnych, osoby odpowiedzialne za procesy oraz przełożeni odpowiadają za wdrożenie Polityki w obszarach im podległych oraz za dopuszczanie do danych wyłącznie osób uprawnionych.
3. Osoby przetwarzające dane osobowe są zobowiązane do:

- zachowania poufności;
- przestrzegania przepisów prawa, niniejszej Polityki i procedur szczegółowych;
- przetwarzania danych wyłącznie w granicach posiadanych uprawnień;
- niezwłocznego zgłaszania incydentów i nieprawidłowości.

4. Administrator wyznaczył Inspektora Ochrony Danych. IOD wykonuje zadania określone w art. 39 RODO, w szczególności monitoruje przestrzeganie przepisów o ochronie danych, doradza Administratorowi i personelowi oraz współpracuje z Prezesem UODO.

§ 5. Kategorie danych i główne obszary przetwarzania

1. W działalności Spółki przetwarzane są w szczególności następujące kategorie danych:

- dane identyfikacyjne i kontaktowe pacjentów;
- dane dotyczące zdrowia, wyników badań, rozpoznań, zaleceń i leczenia;
- dane przedstawicieli ustawowych i osób upoważnionych;
- dane personelu medycznego, pracowników i współpracowników;
- dane kontrahentów i osób reprezentujących kontrahentów;
- dane kandydatów do pracy;
- dane utrwalone w systemach informatycznych, rejestrach, dokumentach i korespondencji.

2. Główne procesy przetwarzania obejmują w szczególności:

- rejestrację pacjentów i umawianie wizyt;
- udzielanie ambulatoryjnych świadczeń zdrowotnych, w tym świadczeń okulistycznych;
- prowadzenie, przechowywanie i udostępnianie dokumentacji medycznej;
- rozliczenia z NFZ, ubezpieczycielami i pacjentami;
- prowadzenie kadr, płac i rozliczeń cywilnoprawnych;
- obsługę dostawców, kontrahentów i usług pomocniczych;
- zapewnienie bezpieczeństwa organizacyjnego i informatycznego.

3. Szczegółowy wykaz procesów przetwarzania jest prowadzony w rejestrze czynności przetwarzania.

§ 6. Podstawy prawne przetwarzania

1. Dane osobowe są przetwarzane na podstawach wynikających z RODO oraz przepisów szczególnych.
2. W odniesieniu do pacjentów podstawę przetwarzania stanowi w szczególności realizacja obowiązków prawnych ciążących na Administratorze oraz przetwarzanie niezbędne do celów profilaktyki zdrowotnej, diagnozy medycznej, zapewnienia opieki zdrowotnej lub leczenia oraz zarządzania systemami i usługami opieki zdrowotnej.
3. W odniesieniu do pracowników, współpracowników i kandydatów do pracy podstawą przetwarzania może być obowiązek prawny, wykonanie umowy, działania przed zawarciem umowy lub zgoda, jeśli jest wymagana.

4. W odniesieniu do kontrahentów i osób reprezentujących kontrahentów podstawą przetwarzania może być wykonanie umowy, obowiązek prawny lub prawnie uzasadniony interes Administratora.
5. Jeżeli przetwarzanie wymaga zgody, zgoda musi być dobrowolna, konkretna, świadoma i jednoznaczna, a jej udzielenie oraz cofnięcie powinny być odpowiednio odnotowane.

§ 7. Zasady dostępu i upoważnień

1. Dostęp do danych osobowych mają wyłącznie osoby posiadające odpowiednie upoważnienie lub wynikające z zakresu obowiązków uprawnienie do przetwarzania danych.
2. Zakres dostępu do danych musi być zgodny z zasadą minimalizacji i zasadą „need to know", tj. ograniczony do informacji niezbędnych do wykonania konkretnych zadań.
3. Każdej osobie dopuszczonej do przetwarzania danych nadaje się uprawnienia odpowiednie do jej roli organizacyjnej i zakresu obowiązków.
4. Administrator prowadzi ewidencję nadanych, zmienionych i odebranych uprawnień oraz rejestr upoważnień do przetwarzania danych osobowych.
5. Dostępy do systemów teleinformatycznych, w tym EDM, powinny być indywidualne, zabezpieczone hasłem i nadawane imiennie.
6. W razie ustania współpracy, zmiany stanowiska albo utraty potrzeby dostępu uprawnienia podlegają niezwłocznemu ograniczeniu albo cofnięciu.

§ 8. Obowiązek poufności

1. Osoby dopuszczone do przetwarzania danych osobowych są zobowiązane do zachowania poufności zarówno w okresie zatrudnienia lub współpracy, jak i po jej ustaniu.
2. Obowiązek poufności obejmuje w szczególności dane pacjentów, informacje o stanie zdrowia, dane personelu, informacje organizacyjne, techniczne i handlowe uzyskane w związku z wykonywaniem obowiązków.
3. Administrator zapewnia odbieranie od personelu stosownych oświadczeń o poufności, jeżeli wymaga tego charakter współpracy lub organizacja procesu.

§ 9. Środki techniczne i organizacyjne

1. Administrator stosuje środki bezpieczeństwa odpowiednie do zidentyfikowanych ryzyk, w szczególności:

- kontrolę dostępu do pomieszczeń, dokumentów i systemów;
- zamykane szafy lub pomieszczenia dla dokumentacji papierowej;
- indywidualne konta użytkowników;
- politykę haseł i okresowej zmiany haseł;
- kopie zapasowe i procedury odtworzeniowe;
- aktualizacje systemów i zabezpieczeń;
- ochronę antywirusową i firewall;
- zasady bezpiecznej pracy z pocztą elektroniczną i urządzeniami mobilnymi.

2. Dane papierowe i elektroniczne są chronione przed przypadkowym zniszczeniem, utratą, nieuprawnionym dostępem, zmianą i ujawnieniem.

3. W obszarach, w których dochodzi do bezpośredniej obsługi pacjentów, Administrator dąży do organizacji pracy ograniczającej ryzyko nieuprawnionego ujawnienia danych, w szczególności poprzez odpowiednią organizację rejestracji, dostęp do gabinetów i obieg dokumentów.
4. W przypadku korzystania z rozwiązań chmurowych, systemów zewnętrznych lub usług wsparcia technicznego Administrator zapewnia odpowiednie zabezpieczenia umowne i organizacyjne.

§ 10. Udostępnianie danych i powierzanie przetwarzania

1. Dane osobowe mogą być udostępniane wyłącznie podmiotom uprawnionym na podstawie przepisów prawa albo innym podmiotom, jeżeli istnieje ku temu odpowiednia podstawa prawna.
2. Dane pacjentów mogą być udostępniane wyłącznie zgodnie z przepisami regulującymi prawa pacjenta, dokumentację medyczną i ochronę danych osobowych.
3. Jeżeli Administrator korzysta z usług podmiotów przetwarzających, zawiera z nimi umowy powierzenia przetwarzania danych osobowych zgodne z art. 28 RODO.
4. Podmiot przetwarzający może przetwarzać dane wyłącznie na udokumentowane polecenie Administratora, w zakresie wynikającym z umowy powierzenia.
5. Udostępnienie danych, przekazanie dokumentacji lub zapewnienie zdalnego dostępu do systemów wymaga zachowania zasad bezpieczeństwa i odpowiedniej autoryzacji.

§ 11. Informowanie osób, których dane dotyczą

1. Administrator realizuje obowiązki informacyjne wobec osób, których dane dotyczą, zgodnie z art. 13 i 14 RODO.
2. Klauzule informacyjne powinny być dostosowane do kategorii osób, których dane dotyczą, w szczególności pacjentów, pracowników, współpracowników, kandydatów do pracy i kontrahentów.
3. Klauzule informacyjne powinny być udostępniane w sposób zapewniający osobom realną możliwość zapoznania się z ich treścią, np. w rejestracji, w dokumentach papierowych, na stronie internetowej lub w korespondencji elektronicznej.

§ 12. Realizacja praw osób, których dane dotyczą

1. Administrator zapewnia obsługę żądań osób, których dane dotyczą, w zakresie wynikającym z RODO, z uwzględnieniem ograniczeń wynikających z przepisów szczególnych, zwłaszcza dotyczących dokumentacji medycznej.
2. Żądania dotyczące dostępu do danych, sprostowania, ograniczenia przetwarzania, przenoszenia danych, sprzeciwu lub cofnięcia zgody są obsługiwane według procedury wewnętrznej.
3. Każde żądanie powinno zostać zarejestrowane i rozpatrzone bez zbędnej zwłoki, nie później niż w terminach określonych przez RODO, chyba że przepisy szczególne stanowią inaczej.
4. W przypadku żądań dotyczących dokumentacji medycznej należy równolegle stosować przepisy regulujące dostęp do dokumentacji medycznej.

§ 13. Retencja danych

1. Dane osobowe są przechowywane przez okres nie dłuższy, niż jest to niezbędne do realizacji celów przetwarzania, z uwzględnieniem przepisów prawa, obowiązków archiwizacyjnych, terminów przedawnienia oraz potrzeb dowodowych.
2. Okresy przechowywania dla poszczególnych kategorii danych określają przepisy szczególne albo wewnętrzna polityka retencji.
3. Dane po upływie okresu przechowywania podlegają usunięciu, anonimizacji albo zniszczeniu w sposób bezpieczny i udokumentowany, o ile ich dalsze przechowywanie nie wynika z przepisów prawa.
4. Dokumentacja medyczna jest przechowywana przez okresy wynikające z przepisów szczególnych.

§ 14. Naruszenia ochrony danych osobowych

1. Każda osoba, która stwierdzi lub podejrzewa naruszenie ochrony danych osobowych, jest zobowiązana niezwłocznie zgłosić ten fakt przełożonemu, osobie odpowiedzialnej za ochronę danych albo IOD, jeżeli został wyznaczony.
2. Każde zgłoszenie incydentu podlega analizie pod kątem charakteru zdarzenia, kategorii danych, liczby osób, skutków i ryzyka dla praw lub wolności osób fizycznych.
3. W przypadku stwierdzenia naruszenia ochrony danych Administrator podejmuje działania ograniczające skutki zdarzenia, dokumentuje incydent oraz dokonuje oceny, czy istnieje obowiązek zgłoszenia naruszenia do Prezesa UODO w terminie 72 godzin i zawiadomienia osoby, której dane dotyczą.
4. Administrator prowadzi rejestr naruszeń ochrony danych osobowych.

§ 15. Szkolenia i podnoszenie świadomości

1. Osoby dopuszczone do przetwarzania danych osobowych powinny być zapoznane z niniejszą Polityką oraz przeszkolone adekwatnie do zakresu swoich obowiązków.
2. Szkolenia powinny obejmować w szczególności:

- zasady poufności;
- obsługę dokumentacji medycznej i danych pacjentów;
- bezpieczne korzystanie z systemów IT;
- rozpoznawanie incydentów i reagowanie na nie;
- zagrożenia związane z pocztą elektroniczną, socjotechniką i urządzeniami mobilnymi.

3. Administrator dokumentuje przeprowadzane szkolenia oraz zapoznanie personelu z obowiązującą dokumentacją.

§ 16. Dokumentacja systemu ochrony danych

1. W ramach systemu ochrony danych osobowych Administrator prowadzi i aktualizuje w szczególności:

- rejestr czynności przetwarzania;
- klauzule informacyjne;

- umowy powierzenia;
- upoważnienia i rejestr upoważnień;
- procedurę obsługi incydentów i rejestr naruszeń;
- analizę ryzyka;
- dokument wyznaczenia IOD i potwierdzenie zgłoszenia do UODO, jeśli dotyczy.

2. Dokumentacja, o której mowa w ust. 1, powinna być utrzymywana w aktualnym stanie i podlegać przeglądowi po każdej istotnej zmianie organizacyjnej, prawnej albo technologicznej.

§ 17. Audyt i przegląd polityki

1. Polityka podlega okresowemu przeglądowi, nie rzadziej niż raz na 12 miesięcy, a także każdorazowo w przypadku:

- istotnej zmiany przepisów prawa;
- zmiany struktury organizacyjnej Spółki;
- wdrożenia nowych systemów lub usług;
- stwierdzenia incydentu lub nieprawidłowości wymagających zmiany zabezpieczeń

PREZES ZARZĄDU
EYEL[illegible] Sp. z o.o.

Jaromir Ziomek